No. 21-2763

IN THE UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

TYLER CAMERON GUTTERMAN, DALE NELSON,
HUNTER JOHNSON, *and* BRIAN HILTUNEN,

Plaintiffs-Appellants,

v.

INDIANA UNIVERSITY, BLOOMINGTON; *and* PAMELA S. WHITTEN,
in her official capacity as President of Indiana University,

Defendants-Appellees.

On Appeal from the United States District Court
for the Southern District of Indiana
No. 1:20-cv-02801
Honorable Jane Magnus-Stinson

APPELLANTS' REPLY BRIEF

Jeffrey M. Schwab
Reilly Stephens
Liberty Justice Center
141 W. Jackson Blvd.
Suite 1065
Chicago, Illinois 60604
Phone: 312-637-2280
jschwab@libertyjusticecenter.org
rstephens@libertyjusticecenter.org

Attorneys for Plaintiffs-Appellants

TABLE OF CONTENTS

TABLE OF AUTHORITIES

INTRODUCTION

Defendants Indiana University and University President Pamela Whitten make several missteps in their response brief. To begin with, their brief proceeds on a misconception: that the search at issue covered only Plaintiffs' use of their CrimsonCards at the exterior door of their dorm building. In fact, as pleaded in the Complaint, the access records at issue collected much more, including their access to the interior common areas of their dorms and their personal bedrooms. Defendants' repeated insistence that the card agreement allows them to do what they will with the data likewise has a core defect: as written, their own policies do to not provide them the authority they claim. Moreover, the standardless search of this kind of metadata threatens to endanger the student privacy that Defendants claim in their brief they consider of the utmost importance. Nor do Defendants' sundry other arguments support the decision below.

This Court should reverse the district court, and find that Plaintiffs have a reasonable expectation of privacy in the data generated by the ID cards the University requires them to use, and hold that Defendants' search of that data was an unreasonable invasion of that expectation of privacy.

ARGUMENT

I. This Court should reverse the decision below and find that the tracking of Plaintiffs' movements was an unreasonable search.

A. Plaintiffs have a Fourth Amendment privacy interest in their swipe data.

Defendants argue that all that is at issue is the swipes at the front door of the building, claiming that "there are simply no allegations which support any inference

that IU searched or entered Appellants' dorm rooms," Resp. Br. at 12, and that "[t]he data generated, therefore, only reveals that a student entered the IU building or facility." *Id.* at 19. But this is simply not the case. As pleaded in the Complaint, the data at issue recorded Plaintiffs' "access not only students' dorm buildings, but their individual bedrooms — as well as access elevators and dorm building common areas," and the University used that data "to check the alibis of several students" "by comparing their 'swipe' data to their testimony as to their whereabouts at the time of the incident." ¶¶ 18, 22 (S.A. 24–25). At the motion to dismiss stage, Plaintiffs are entitled to their reasonable factual claims as pleaded—and indeed, Defendants cite nothing for the proposition that the access of the swipe data was limited to the front door of this case. The reasonable factual inference drawn from Plaintiffs' allegations is that the University accessed data beyond simply the exterior door of the dorm buildings, and that the data included ID swipes at elevators, interior doors, and personal dorm rooms.

Defendants make much of the fact that they never *physically* entered the dorms or dorm rooms, and submit that this means there is no protection for the interior of the building because there was no trespass, and therefore the tracking of interior movements is irrelevant since "the protection afforded a home's curtilage applies only under a traditional trespass analysis." Resp. Br. at 12 n.2. This is wrong for several reasons.

First, since the tracking included the *dorm room*, the Fourth Amendment's protection of the home is implicated even if other aspects of the building were not.

Second, courts around the country, including this Court, have repeatedly held that students have an expectation of privacy in the common areas of their living spaces. *Reardon v. Wroan*, 811 F.2d 1025, 1030 (7th Cir. 1987) (recognizing an expectation of privacy in the common areas of a fraternity house); *State v. Houvener*, 186 P.3d 370, 375 (Wash. App. 2008) (recognizing an expectation of privacy in dorm building common areas); *see also People v. Killebrew*, 256 N.W.2d 581, 583 (Mich. App. 1977) (recognizing an expectation of privacy in the common areas of a multi-unit building). Third, the lack of a physical trespass does not mean that there is no protection for curtilage. Even where there is no physical trespass, intrusions into the privacy of the curtilage are still subject to the analysis of the reasonable expectation of privacy. *See, e.g., Florida v. Riley*, 488 U.S. 445, 449 (1989) (applying *Katz* to the curtilage where there was no physical trespass). Defendants' cites to *Jones* and *Jardines* are essentially backwards. "The Katz reasonable-expectations test 'has been added to, not substituted for,' the traditional property-based understanding of the Fourth Amendment." *Florida v. Jardines*, 569 U.S. 1, 11 (2013) (quoting *United States v. Jones*, 565 U.S. 400, 409 (2012)).

Defendants next argue that since the card agreement specifies the card is the property of the University, the data generated by the card is institutional data of the University, it can do with the data as it pleases, and Plaintiffs were on notice that the University would use the data in this way. Resp. Br. at 14–15, 17. But there was no such notice—indeed, the terms by which students accepted the cards were the opposite.

First, the 'ownership' status of the cards is irrelevant. If a property owner enters into a contract to transfer possession of their property to someone else, their continued access or use of the property is subject to the terms of the contract—the formal "ownership" arrangement simply brings the analysis back around to the contract's terms.

Second, the terms of the Card Agreement and related university policies do not provide notice that swipe data would be used for anything like this sort of purpose. Defendants make much of the portion of the data policy that allows access "for all legitimate university purposes." Resp. Br. at 14–15. But Defendants' reliance on this provision of policy simply ignores other University policies that specify what "legitimate university purposes" the cards are to be used for. Indiana University policy UA-13 states that the ID Card exists "to verify their [students', employees', other's] identity and manage their access to University services and facilities. The ID card will be used to verify the identity of the bearer of the card in University facilities when such identification is needed to be present at those facilities or on University grounds." Resp. Br. at 5. The policy states that the card's "intended use" is to be "an electronic identification, validation, and authentication credential for authorized access to services and facilities." *Id.*

The policy does not entitle the University to access, use, or release CrimsonCard swipe data. Such use of swipe data to check past entries to University buildings to check the alibis of students during an investigation does not comport with the intended purpose of the card—to contemporaneously verify the identity and manage

access to University services and facilities of by cardholders. Verification, validation, and authentication are all contemporaneous needs to permit access to a building—to "swipe in" in modern parlance. There is, of course, no question that Plaintiffs are and were who they say they are, and that Plaintiffs accessed University buildings they were entitled to enter using their ID Card. The use of this information to investigate Plaintiffs was therefore a *violation* of the terms of the card agreement, and Plaintiffs could not be on notice of a violation of the terms they agreed to.

Nor does the use here of swipe data fit within the policy's "safety and security exception." That exception is strictly limited to "[i]dentification information collected for production" of the card; it says nothing about ongoing access to students' individual, personal movements on campus. *Id.* If anything, the fact that the terms included a "safety and security exception" specific to a different circumstance shows that the terms do not cover this circumstance.

B. Using Plaintiffs' swipe data to track their movements was unreasonable.

Defendants assert that their actions were reasonable because "the Government only conducts a 'search' for purposes of the Fourth Amendment where it tracks movements in private locations that could not otherwise be obtained by visual observation." Resp. Br. at 16. Yet the facts of this case are that the University did in fact track movements in private locations that could not otherwise be obtained by visual inspection. Defendants claim that "anyone (e.g., other students, RAs, investigators from IU's Office of Student Conduct, or police officers) could have visually observed them enter (or exit) their residence halls." *Id.* But the data at issue

was not limited to the exterior doors that might have been viewed by a stakeout across the street. Rather, the search included the interior of the dorm buildings, including Plaintiffs' personal bedrooms—things that would not be seen by "neighbors, law enforcement, or others passing by." *Id.* Therefore, the data accessed here "reveal[ed] a critical fact about the interior of the premises that the Government is extremely interested in knowing." *United States v. Karo*, 468 U.S. 705, 715 (1984).

Defendants invoke this Court's recent decision in *United States v. Tuggle*, 4 F.4th 505, 509–10 (7th Cir. 2021). Resp. Br. at 18. As stated in Appellants' Opening Brief, *Tuggle* is a case about tracking public activity in a *single location*. Opening Br. at 20. Defendants find this analogous since "as Appellants allege, the CrimsonCard is needed only to access an IU building or facility, including one's dorm." Resp. Br. at 19. First, this is not true: Plaintiffs' Complaint alleges that the CrimsonCard is used for all manner of activities, including off-campus payments. *See* ¶¶ 17, 22–24 (S.A. 25–26). Second, the fact that the swipe data "only reveals that a student *entered* the IU building or facility," Resp. Br. at 19 (emphasis in original), does not by itself render the search unintrusive. Defendants' hypothetical here imagines swipe data showing "a student entered his or her residence hall at 10:00 p.m. on Friday evening and, again, at 10:00 a.m. on Saturday morning." *Id.* n.5. But the record need not be so sparse: the swipe data could just as easily show the student entering at one point in the night, then reentering at another an hour later, and that the student accessed an elevator at his bedroom door at another point without exiting the building.

Each of these could mean a number of different things—perhaps they went downstairs for a pizza delivery, or just for some fresh air, or perhaps they're engaged in illegal drug transactions. But when pieced together they begin to tell a story, and even more so, whereas here, the information from multiple students is cross referenced against each other, to show that they were together on a given night, and moved between each other's rooms or buildings. Metadata such as this can be easily "aggregated in a manner that enables the government to ascertain, more or less at will, [an individual's] political and religious beliefs, sexual habits, and so on." *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring). Technological tracking of movements tells the story "not simply of where we go, but by easy inference, of our associations—political, religious, amicable and amorous, to name only a few—and of the pattern of our professional and avocational pursuits." *People v. Weaver*, 909 N.E.2d 1195, 1199–200 (N.Y. 2009). And the idea that the data accessed here does not tell an investigator anything useful is belied by the simple fact that the University itself accessed the data believing it would learn useful information about Plaintiffs' whereabouts.

For this reason, Defendants' invocation of the third-party business records doctrine of *Smith v. Maryland*, 442 U.S. 735, 737 (1979) and *United States v. Miller*, 425 U.S. 435 (1976) is inappropriate. *See* Resp. Br. at 15, 19. As set forth in Appellants' Opening Brief, this Court should follow the Supreme Court in *Carpenter v. United States*, 138 S. Ct. 2206, 2212 (2018), and decline to apply the "third party" doctrine to this kind of modern technology. Opening Br. at 18–19. The doctrine—developed in the analog era for limited sorts of information such as phone numbers

is a poor fit for the digital age. *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring). Even before *Carpenter,* the Supreme Court had previously recognized that the traditionally broad "search incident to arrest" exemption should not be extended to the search of an arrestee's cell phone, because just as GPS tracking could provide more information than an old-fashioned tail, a person's cell phone now contains far more personal information than the purses and wallets of prior Fourth Amendment cases. *Riley v. California*, 134 S. Ct. 2473, 2489 (2014). *Carpenter* declined to overrule *Smith*, but also declined to extend the third-party business records doctrine to modern technology. 138 S. Ct. at 2219.

Defendants contend that the *Carpenter* scenario is "vastly different from the allegations in [Plaintiffs'] Complaint, that the University retained only a few months of data and used it for the limited purpose of checking their whereabouts at the time of the [hazing] incident.'" (quoting Dkt. 1 at 6, ¶ 18). First, Plaintiffs did not know at the time of pleading how long the University kept the data, only that it was accessed several months later and therefore kept at least that long—that is the reference to "several months" in ¶ 18. For all Plaintiffs knew at the time of pleading, the University may keep CrimsonCard data for years, and therefore Plaintiffs pleaded that the data "could potentially be stored indefinitely, investigators need not determine that there is probable cause before tracking it — historical records could be consulted for anyone who falls under suspicion." S.A. 26. Second, even several months is enough—the data in *Carpenter* covered approximately four to five months, for instance, and one of the Court orders returned only two days' worth. 138 S. Ct. at

2212 ("The first order sought 152 days of cell-site records from MetroPCS, which produced records spanning 127 days. The second order requested seven days of CSLI from Sprint, which produced two days of records . . .").

Defendants fall back on the claim that the swipe records at issue are "institutional data," because the Card Agreement says the Card is the University's property and therefore they are entitled to do with it as they please. Resp. Br. at 14, 21. But this can only be taken so far. First, as explained *supra*, use of the data in this manner is inconsistent with the University policies in question. Second, assuming the card is their property, that does not mean they can use it in any manner they prefer, any more than the fact that the dorm building is owned by the University means they could put spy cameras in the showers. The government still must operate subject to constitutional constraints. *Medlock v. Trs. of Ind. Univ.*, 738 F.3d 867, 871 (7th Cir. 2013) ("Indiana University is a public university, owned by the State of Indiana, and the student inspectors and university police are university employees and therefore state actors . . . so they can be sued under section 1983 for violating the Fourth Amendment."). And when the Government is acting as landlord, it cannot leverage that status to void the rights of those who live in government-run housing. *See Pratt v. Chi. Hous. Auth.*, 848 F. Supp. 792, 793 (N.D. Ill. 1994) (search of public housing projects).

Defendants attempt to analogize the situation here to cases from other circuits about magnetic swipe data, citing cases from the Fifth, Sixth, and Eighth Circuits. Resp. Br. at 22–23 (citing *United States v. Turner*, 839 F.3d 429, 436 (5th Cir. 2016);

United States v. Bah, 794 F.3d 617, 630-31 (6th Cir. 2015); *United States v. Briere de L'Isle*, 825 F.3d 426, 431 (8th Cir. 2016)). But they conflate the information on the magnetic strip on the card with the information generated by the card *swipes*, which are two different things. These three cases are about government searches of the magnetic strip on the card, which contained an account number or similar information used to process transactions. *See, e.g., Turner,* 839 F.3d at 431–32 ("A subsequent scan of the gift cards revealed that at least forty-three were altered, meaning the numbers encoded in the card did not match the numbers printed on the card"). The CrimsonCards include a magnetic strip as well, but this case is about the data generated by *swiping* the cards, not the authorizing information on the magnetic strip.

Defendants assert that the swipe data is different than the cell phone location data in *Carpenter* because it only generates a single data point at each swipe. Resp. Br. at 23–24. But the University did not access a single swipe, it accessed all the swipes over several periods of time and pieced them together to generate inferences about Plaintiffs' movements—exactly what Plaintiffs argue metadata can be used for. It is true that there are things this data does not capture, like "when a door is unlocked or left ajar," but that does not mean it fails to capture substantial information. And it is simply not true that the data "cannot reveal how long a student stayed in their room" and "does not reveal where Appellants went once they were inside." Resp. Br. at 24. In fact, the data reveals both of these pieces of information: since it tracks the use of interior doors, elevators, and other common spaces, as well

as bedrooms, it can tell the University where within the building Plaintiffs went, whether to their room, or to a different floor where a friend lived, and whether they left their room to return later. It can even provide an inference as to "when they went to sleep," *id.*, as the last card swipe at their bedroom is most likely to represent when they retired for the evening.

Nor is it the case that one cannot draw inferences as to "purpose or intent of a student's access to an IU building or facility." Resp. Br. at 24. Defendants rely on this Court's recent decision in *United States v. Soybel*, 13 F.4th 584, 593 (7th Cir. 2021), where IP-address information was analogized to the pen register in *Smith*. But there are several differences between the data here and the IP information in *Soybel*. First, the search in *Soybel* was conducted pursuant to a pen register act, and it was reasonable enough for this Court to find that a pen register in that instance was governed by the explicit approval of pen registers in *Smith,* since in the specific context of pen registers "technological differences don't necessarily beget constitutional ones." *Id.* at 591. Second, the IP information was inherently limited: "[t]he data the government would collect might show, for instance, that an internet user connected to a Google IP address. But it could not reveal the specific Google website accessed (i.e., YouTube or Gmail), let alone what the user was doing within that website." *Id.* at 588. The data therefore could not even necessarily show *which website* he was visiting, much less for what purpose—to watch a YouTube video, or to access Google's cloud storage, or just to use the google search engine to look for some completely unrelated non-Google website. Moreover, without outside context, it is

impossible to know that this was even Soybel's IP address in the first place. The CrimsonCard data is fundamentally different: it is explicitly attached to each Plaintiffs' identity in the system, and when they swipe it, the University knows exactly where they are, whether at a dorm room, or the library, or the student health clinic, or cutting class at an off-campus restaurant.

Defendants' citation to *Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182 (N.D. Cal. 2020), likewise falls short. To begin with, *Heeger* isn't a Fourth Amendment case at all; it's a class action against a private company for alleged privacy violations. In any case, the court in *Heeger* found that IP information was "apples and oranges" as compared with the cell phone location information in *Carpenter*. *Id.* at 1189. Plaintiffs agree: the shear fact that Facebook would incidentally know the IP address of the cell phone that connected to Facebook did not mean that Facebook was tracking the locations of the Plaintiffs, since the IP address of the cell phone would only identify the cell phone*, not its location*—an IP address reveals far less information that the CrimsonCard data.

It is to some extent true that "Appellants have multiple options to either limit generating swipe data or avoid it altogether," Resp. Br. at 27, in that they could choose certain places to use cash instead of the CrimsonCard, but they did not have a choice *as to the data accessed in this case*—IU requires freshmen to live on campus, they had no choice but to live in the dorms that would subject them to tracking.[1]

[1] "New, first-year, undergraduate students at Indiana University Bloomington are required to live on campus . . . Any student who violates the residency policy by living off-campus in Bloomington may be subject to immediate administrative withdrawal from the university and/or required to pay all room and board fees and charges for the semester(s) in which the

Moreover, this choice rings hollow when, as explained *supra*, Plaintiffs had no notice that this sort of abuse of their CrimsonCard data was possible, and so therefore were not aware that such a choice was necessary.

In a footnote, Defendants claim that the hypothetical at pages 19–20 of Appellants' Opening Brief "must be disregarded" as it "has no basis in fact" and was not "alleged in Appellants' complaint." Resp. Br. at 24–25, n.8. Plaintiffs were not aware that hypotheticals needed to be actual facts, nor that it was necessary to plead a hypothetical. But as it happens, Plaintiffs *did* plead the substantive point made by the hypothetical: that there are serious privacy concerns with this sort of data.[2]

Plaintiffs do not believe this case falls under the administrative search doctrine. However, if it does, Plaintiffs are entitled to pre-compliance review. Opening Br. at 13–14. Defendants' argument about *Patel* is simply a return to the same argument that the cards, and therefore the data, is the property of the University. Resp. Br. at 28-9. Yet they cite nothing for the proposition that "IU's search of its own records similarly does not require pre-compliance review." *Id.* Defendants analogize this to the possibility of the hotel owner in *Patel* searching his own records. But, as explained *supra*, the government, as a state actor, is subject to constitutional constraints above and beyond the everyday business owner. Likewise, Defendants' discussion of

violation(s) occurred." Indiana University Residential Programs and Services, *On-campus housing requirement*, https://housing.indiana.edu/housing/residency/index.html.

[2] "The privacy concerns in this sort of data are significant: IU officials could use this kind of swipe-card data to determine who attended the meetings of a disfavored political organization, or who is seeking medical services, or even who a student is romantically involved with. And since it could potentially be stored indefinitely, investigators need not determine that there is probable cause before tracking it — historical records could be consulted for anyone who falls under suspicion." (S.A. 26).

Medlock, Resp. Br. at 30–31, fails to distinguish the salient facts: *Medlock* was not a disciplinary proceeding, it was a basic health and safety check. *See* Opening Br. at 8–10. Nor does the attempt to analogize the health and safety purpose of the University's hazing investigation work: the RA health and safety checks contemplated by *Medlock* are the health and safety of the dorm facility—preventing fire hazards, toxic mold, etc.—not an open-ended interest in identifying disciplinary infractions.

Finally, the fact that, as it happens, the search at issue did not discover that Plaintiffs were guilty of anything does not absolve the Fourth Amendment violation. Privacy violations are an inherent injury—if one learned that a secret camera had been placed in one's home, it would be no great comfort to learn that the camera happened not to photograph anything criminal. *See, e.g., In re Facebook, Inc.*, 402 F. Supp. 3d 767, 777 (N.D. Cal. 2019) ("the law has long recognized that a privacy invasion is itself the kind of injury that can be redressed in federal court, even if the invasion does not lead to some secondary economic injury like identity theft."). Defendants insist that Plaintiffs were not the target of the investigation, but that is entirely contingent: had the investigation turned up wrongdoing by Plaintiffs, Defendants cannot seriously contend that there would have been no consequences. The fact that Plaintiffs are upstanding members of the University community should not undermine their right against unreasonable searches.

CONCLUSION

For the forgoing reasons, the decision below should be reversed.

Dated: January 13, 2021

/s/ Jeffrey M. Schwab
Jeffrey M. Schwab
Reilly Stephens
Liberty Justice Center
141 W. Jackson Blvd.
Suite 1065
Chicago, Illinois 60604
Phone: 312-637-2280
Fax: 312-263-7702
jschwab@libertyjusticecenter.org
rstephens@libertyjusticecenter.org

Attorneys for Plaintiffs-Appellants

CERTIFICATE OF COMPLIANCE

I certify that this brief conforms to the type-volume limitations imposed by Fed. R. App. P. 32 and Circuit Rule 32 for a brief produced using the following font: Proportional Century Schoolbook Font 12 pt body text, 11 pt for footnotes. Microsoft Word for Mac was used. The length of this brief was 4,085 words.

/s/ Jeffrey M. Schwab
Jeffrey M. Schwab

CERTIFICATE OF SERVICE

I hereby certify that on January 13, 2021, I electronically filed the foregoing Appellants' Reply Brief with the Clerk of the Court for the United States Court of Appeals for the Seventh Circuit by using the CM/ECF system. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

/s/ Jeffrey M. Schwab
Jeffrey M. Schwab