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' BRIEF AND SHORT APPENDIX

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

Attorney for Plaintiffs-Appellants

DISCLOSURE STATEMENT

1. The full name of every party the undersigned attorney represents in the case: Plaintiffs-Appellants Tyler Cameron Gutterman, Dale Nelson, Hunter Johnson, and Brian Hiltunen.

2. The name of all law firms whose partners or associates have appeared on behalf of the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this Court: the Liberty Justice Center; Anita Yvonne Milanovich of Milanovich Law, PLLC, served as local counsel in the district court in this case, but is not counsel to this appeal.

3. If the party or amicus is a corporation: not applicable.

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

Counsel for Plaintiffs-Appellants

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Treatises

JURISDICTIONAL STATEMENT

The District Court had jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under the Fourth Amendment to the United States Constitution and, therefore, presents a federal question, and had jurisdiction under 28 U.S.C. § 1343 because relief is sought under 42 U.S.C. § 1983. On September 24, 2021, Appellants filed a timely Notice of Appeal from the District Court's September 1, 2021 Judgment, Short Appendix ("S.A.") 20—Granting Appellees' Motion to Dismiss—issued in accordance with the court's September 1, 2021 Order. S.A. 1. This Court has jurisdiction pursuant to 28 U.S.C. § 1291.

STATEMENT OF ISSUE PRESENTED FOR REVIEW

Students living in university housing enjoy the protection of the Fourth Amendment against unreasonable searches. In this case, the University used records taken from Student IDs that it issued to all students to track Appellants movements, including when they accessed their dorm building and dorm rooms. Does the University's tracking of Appellants' movements, including their access to the university housing in which they live, as part of a formal University disciplinary investigation constitute an unreasonable search under the Fourth Amendment?

STATEMENT OF THE CASE

Appellants are undergraduate students at Indiana University, Bloomington. S.A. 3. As a condition of their attendance at the University, all students, including Plaintiffs, are required to carry an official, University-issued Student ID Card, known as a "CrimsonCard," which facilitates their access to university buildings and

services. *Id*. For example, a CrimsonCard is necessary to access dorm buildings and, in some cases, dorm rooms. S.A. 6. A CrimsonCard is also necessary for students to check out library books, print materials on university printers, and to get meals at university dining halls. *Id*. And these ID Cards are used to access academic buildings, parking garages, parking meters, and to purchase sodas and snacks from university vending machines, to pay for the use of laundry machines, to pay for food and drinks at university cafeterias, and all manner of sundry other daily activities. *Id*. This swipe data even allows students to make purchases off campus, at local restaurants and businesses that allow purchases using a student account. *Id*. But these ID Cards do more than just allow students to access university buildings or services, and purchase things on and off-campus. Importantly, for purposes of this case, these ID cards also record every time the student "swipes" the card. S.A. 3. Further, the university maintains records of this swipe data, which it uses as part of official investigations. S.A. 6. Those records reveal not only *where* students go, but *when*—which buildings, parking garages, or parking meters they access and when they access them, which university printers they use and when, where and when they check out library books, and where and when they have meals at university dining halls or cafeterias. Further, these records even record where and when students purchase things off campus with their CrimsonCard. S.A. 6.

The University allows access to this data to "all eligible employees and designated appointees of the university for all legitimate university purposes." S.A. 6 (quoting the University's Management of Institutional Data policy (DM–01)). The University

does not provide the subject of a search of swipe data the opportunity to obtain precompliance review before a neutral decisionmaker. *Id.*

As freshmen in the Fall of 2018, Plaintiffs took part in many of the University's activities and traditions, including pledging for the campus fraternity Beta Theta Pi ("Beta" or "the fraternity.") S.A. 3. During this Fall 2018 semester, the University investigated the fraternity regarding an alleged hazing incident. S.A. 6. As part of this investigation, the University used the swipe data it had tracked to compare with Plaintiffs' testimony as to their whereabouts at the time the alleged hazing occurred. S.A. 6–7. In particular, the swipe data was used to track Plaintiffs' movements into and out of their dorms. S.A. 21. There was never any allegation the Plaintiffs sponsored or organized the alleged hazing; indeed, they were pledges to the fraternity at the time. S.A. 7.

Indiana University policy UA-13 states that the ID Card exists "to verify their [students, employees, others] 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." S.A. 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*. Nothing in the CrimsonCard Terms and Conditions or the University's Policy Manual permits using the data to track students. *See* S.A. 3-6.

Procedural History

Appellants filed this case on October 29, 2020. Counts I of the Complaint alleges that the tracking of Appellants movements violated Plaintiffs' Fourth Amendment Rights. S.A. 30. Count II alleged that, even if the search at issue were subject to the administrative search doctrine, the lack of precompliance review meant that accessing the data still violated the Fourth Amendment. S.A. 31. Count III of the Complaint alleges that the University's use of swipe data represented a breach of contract by violating the University's own policies. S.A. 32. The Appellees filed a Motion to Dismiss on February 16, 2021. S.A. 7.

Appellees' Motion to Dismiss asserted that they were protected by sovereign immunity. S.A. 8. On the merits, it argued that there was no search, and if there was a Fourth Amendment search, that it was reasonable, and that Appellants' breach of contract claim failed as well. S.A. 10–11. On September 1, 2021, the District Court issued its opinion and judgment. S.A. 1, 20. The court held that while some of the claims were subject to sovereign immunity, Appellants' claims for prospective relief against President Whitten were not. S.A. 10. As to the Fourth Amendment claim, the court below assumed, without deciding, that the complaint alleged a Fourth Amendment search. S.A. 14. However, the court found that the search in question did not violate the Fourth Amendment because it was reasonable. S.A. 16. After dismissing the Fourth Amendment claims with prejudice, the court declined jurisdiction on the state law breach of contract claim, and therefore dismissed it

without prejudice. S.A. 17. On September 24, 2021, Appellants filed their Notice of Appeal with this Court. *See* Dkt. 1 at 1.

SUMMARY OF ARGUMENT

Citizens do not waive their Fourth Amendment rights simply because the government is acting as their landlord. Had Appellants been living in an apartment building off campus, the search at issue in this case would have required adherence to Fourth Amendment process. The answer should not be different simply because Appellants lived in housing operated by the University. The district court's conclusion to the contrary should be reversed. It is in conflict with the consistent holding of courts around the country that students living on campus should not have substantially different rights than those living on campus.

The core of the Fourth Amendment is the privacy of one's home, and it is precisely the special protection for the home that this case implicates. Appellants' swipe data tracked their movement into and out of their homes, as well as within them—the cards track access to the dorm building, elevators, hallways, communal lounges, personal bedrooms, even when students go to the bathroom. The University invaded the privacy of their homes by not only tracking their movements, but by employing that tracking in an official investigation into Appellants' conduct (to see if it could convict them of the administrative equivalent of perjury), in violation of the Fourth Amendment.

And while the search in this case intruded into the privacy of Appellants' living arrangements, the data at issue is not so limited. It tracks students all across, and

also off, campus. The decision below would permit tracking of any of these movements, without any standard, or review, or oversight. This court should decline to license such ubiquitous government surveillance.

STANDARD OF REVIEW

This Court reviews an order granting a motion to dismiss under Fed. R. Civ. P. 12(b)(6) de novo, construing the complaint in the light most favorable to the plaintiffs, "accepting as true all well-pleaded facts alleged, and drawing all possible inferences in [the plaintiffs'] favor." *Tamayo v. Blagojevich*, 526 F.3d 1074, 1081 (7th Cir. 2008). Dismissal under Rule 12(b)(6) is proper only where the plaintiff can prove no set of facts that would entitle him to relief. *Marshall-Mosby v. Corp. Receivables, Inc.*, 205 F.3d 323, 326 (7th Cir. 2000).

ARGUMENT

I. Tracking Appellants' swipe data was an unreasonable search under the Fourth Amendment.

The Fourth Amendment protects persons from unreasonable searches of their homes and property. *See* U.S. Const. amend IV. A search occurs when the government intrudes on a reasonable expectation of privacy that society is prepared to recognize as legitimate. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Searches conducted without a warrant are "presumptively unreasonable." *Kentucky v. King*, 563 U.S. 452, 459 (2011) (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)). "At the Amendment's 'very core' stands 'the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" *Florida v.*

Jardines, 569 U.S. 1, 6 (2013) (quoting *Silverman v. United States*, 365 U.S. 505, 511 (1961)).

A. Students living in university housing enjoy the protection of the Fourth Amendment against unreasonable searches.

The Supreme Court has never directly addressed the Fourth Amendment in the context of a college dormitory. There are, however, many cases in the circuits, districts, and at the state level. These "courts have unanimously held that 'a student who occupies a college [or university] dormitory room enjoys the protection of the Fourth Amendment.'" Brian R. Lemons, *Public Education and Student Privacy: Application of the Fourth Amendment to Dormitories at Public Colleges and Universities*, 2012 BYU Educ. & L. J. 31, 38 (2012) (quoting *Piazzola v Watkins*, 442 F.2d. 284, 289 (5th Cir. 1971)). Generally, a "dormitory room is analogous to an apartment or a hotel room." *Piazzola*, 442 F.2d. at 288 (quoting *Commonwealth v. McCloskey*, 272 A.2d 271, 273 (1970)). And this protection is not necessarily limited to the four walls of the student's private living quarters. In *State v. Houvener*, 186 P.3d 370 (Wash. Ct. App. 2008), the court found that there could also be an expectation of privacy in common areas such as hallways, which the court analogized to the curtilage of a home. As *Houvener* recognized, in many dorms access to each floor is limited to the residents of that floor, who shared common areas—including communal bathrooms with "towel-clad residents navigating the hallways to and from shared shower facilities," which distinguish it from the public hallways of a typical apartment building that courts have not generally protected. *Id.* at 374.

The court below characterized the search at issue as simply to "ensure Plaintiffs' safety." S.A. 16. But this appeal to paternalism cannot justify such intrusion into constitutionally protected spaces. Appellants concede that courts have sometimes viewed *routine inspections* by Resident Assistants ("RA") for cleanliness and safety either as administrative searches or not searches at all. In *State v. Kappes*, 550 P.2d 121, 124 (Ariz. Ct. App. 1976), for instance, the RA conducted such a standard monthly room inspection after giving 24 hours' notice, and found marijuana sitting out in plain view, which was reported first to campus police and ultimately to the municipal police who charged the student with criminal possession. However, the court said that an intrusion by law enforcement into the dorm room, or by a school official at the instruction of law enforcement, *would* have violated the Fourth Amendment. *Id.* at 123. Since it was a part of the normal room inspection, not a search for evidence, the RA's entry did not meet the "government action" requirement of the Fourth Amendment.

In *Medlock v. Trs. of Ind. Univ.*, 738 F.3d 867, 871 (7th Cir. 2013), this Circuit rejected the premise that an RA inspection does not involve state action. *See also Morale v. Grigel*, 422 F. Supp. 988, 996 (D.N.H. 1976) (stating that RA's are state actors). However, because it was a routine room inspection, this Court found that it did not violate the Fourth Amendment. *Medlock,* 738 F.3d at 872. And unlike RAs, "[c]ourts have found campus police and other full-time employees of the university, such as head residents and directors of housing, to be state actors." Kristal O. Stanley, *The Fourth Amendment and Dormitory Searches: A New Truce*, 65 U. Chi. L. Rev.

1403, 1406 (1998). The people conducting the search in this case were University employees from the office of student life, who were pursuing an investigation. This case is therefore not comparable to *Medlock* because this was not a routine health-and-safety inspection, for at least three reasons:

1) The search of Appellants swipe data was not a routine room inspection for cleanliness, something one might also reasonably consent to as a tenant leasing an apartment. It was not scheduled on a monthly or quarterly basis; it was an event-driven search incident to an investigation. Indeed, this was not a room inspection at all: it was a search of electronic data to discern Appellants' whereabouts. Swipe data cannot show whether you are harming university property or creating a fire hazard by failing to keep your room clean. Swipe data cannot show whether you are respecting your roommate by maintaining a clean-living area.

2) Nor was the search here conducted by an RA, like the search in *Medlock*. An RA is typically another student, who gets a small stipend or free housing for helping the University look after a dorm, rather than a full-fledged employee, limited in their power to investigate or discipline students. This was an investigation by the University office tasked with investigating and punishing students, carried out by full-time University employees whose job it is to carry out such investigations and determine such punishments.

3) This was a formal investigation into conduct that allegedly occurred. Investigations of fraternity hazing are not equivalent to checking to make sure students pick up after themselves—they are not even limited to University discipline,

instead sometimes leading to criminal charges. *See, e.g.* Chris Woodyard, *DKE frat members arrested for hazing, urinating upon LSU pledges*, USA Today (Feb. 14, 2019);[1] Sara Ganim, *Recovered video leads to new charges in Penn State fraternity death*, CNN (Nov. 13, 2017).[2] And while Appellants were found innocent of any wrongdoing, sanctions were handed out to the fraternity—and under different facts could have been even more significant. As the Sixth Circuit recently explained, public university discipline proceedings must respect constitutional rights. *Doe v. Baum*, 903 F.3d 575, 581 (6th Cir. 2018) (holding universities must give students a right of cross examination during disciplinary proceedings as a matter of Due Process).

Public universities fulfill multiple roles with overlapping obligations—they are an educational institution that governs student conduct, a landlord administering housing, and also maintain the power of the state subject to constitutional limitations. Because of these multiple contexts, a review of the cases shows that "the courts that have examined the issue are split on whether the Fourth Amendment requires probable cause and a warrant in college searches." *Commonwealth v. Neilson*, 423 Mass. 75, 78 (1996). But this is because the rules for a landlord checking for fire hazards might be sensibly different than the rules for an institution that exists to investigate and punish. For instance, "when police are involved and the evidence obtained is to be used in a criminal proceeding, courts generally require probable

[1] https://www.usatoday.com/story/news/nation/2019/02/14/9-lsu-fraternity-members-arrested-hazing-charges/2872824002/.
[2] https://www.cnn.com/2017/11/13/us/penn-state-fraternity-hazing-death/index.html.

cause and a warrant, absent express consent or exigent circumstances." *Id.* (citing cases[3]).

Neilson well exemplifies what seems to be the basic line: there university employees entered for a routine inspection, and saw a lamp in a closet, which turned out to be a grow light for marijuana. They then alerted police, who searched the room and charged the student. The Court reasoned that "the initial search was reasonable because it was intended to enforce a legitimate health and safety rule that related to the college's function as an educational institution." *Id.* at 987. However, "[w]hile the college officials were legitimately present in the room to enforce a reasonable health and safety regulation, the sole purpose of the warrantless police entry into the dormitory room was to confiscate contraband for purposes of a criminal proceeding. An entry for such a purpose required a warrant where, as here, there was no showing of express consent or exigent circumstances." *Id.*

Disciplinarian investigations are far closer to a criminal matter than a routine health-and-safety inspection: the potential result is not simply a talking-to about the importance of dusting furniture or the dangers of leaving clothes on a radiator; such investigations can lead to suspension, expulsion, and depending on the findings even a criminal referral. This is fundamentally a prosecutorial function that implicates the

[3] *Compare Keene v. Rodgers*, 316 F. Supp. 217 (D. Me. 1970); *Moore v. Student Affairs Comm. of Troy State Univ.*, 284 F. Supp. 725 (M.D. Ala. 1968); *State v. Kappes*, 26 Ariz. App. 567, 550 P.2d 121 (1976); *People v. Kelly*, 195 Cal. App. 2d 669, 16 Cal. Rptr. 177 (1961); *State v. Hunter*, 831 P.2d 1033, 1037 (Utah Ct. App. 1992), with *Piazzola v. Watkins*, 442 F.2d 284, 289 (5th Cir. 1971); *Morale v. Grigel*, 422 F. Supp. 988, 997 (D.N.H. 1976); *Smyth v. Lubbers*, 398 F. Supp. 777, 785 (W.D. Mich. 1975); *People v. Cohen*, 57 Misc. 2d 366, 369, 292 N.Y.S.2d 706 (N.Y. Dist. Ct. 1968); *Commonwealth v. McCloskey*, 217 Pa. Super. 432, 435-436, 272 A.2d 271 (1970).

University's role as the government, rather than its role as landlord. This is especially true here, where the University was not investigating reports of misconduct or unsafe behavior within its residences. Rather, it was investigating alleged off-campus conduct and the search of Appellants' swipe data to determine their presence in the dorms was orthogonal to that investigation. Just as *Medlock* accepted that the University may enter rooms in its role as landlord, so this court should find that when its acting in a disciplinary role the University must respect constitutional norms and provide appropriate process.

The court below held that Appellants, by virtue of living in university housing—and using the ID Cards they were required to carry to access it—consented to this sort of tracking. S.A. 14. But waiving a constitutional right is not something one can do unwittingly or by implication. Supreme Court precedent provides that certain standards be met in order for a person to properly waive his or her constitutional rights. First, waiver of a constitutional right must be of a "known right or privilege." *Johnson v. Zerbst*, 304 U.S. 458, 464 (1938). Second, the waiver must be freely given; it must be voluntary, knowing, and intelligently made. *D. H. Overmyer Co. v. Frick Co.*, 405 U.S. 174, 185-86 (1972). Finally, the Court has long held that it will "not presume acquiescence in the loss of fundamental rights." *Ohio Bell Tel. Co. v. Public Utilities Comm'n*, 301 U.S. 292, 307 (1937).

Universities have often tried to claim express or implied consent to searches pursuant to a university agreement, and "the analysis by courts has not proceeded strictly on contract grounds, but rather on the doctrine of unconstitutional

conditions." Stanley, *A New Truce,* 65 U. Chi. L. Rev. at 1410. As a survey of the cases explains:

> Under the doctrine of unconstitutional conditions in the dormitory context, then, students can only be required to agree to a search that would not infringe upon their Fourth Amendment rights. While the courts agree that health and safety inspections by university officials without a warrant and probable cause do not violate a student's Fourth Amendment rights, they disagree about the constitutionality of drug or contraband searches without a warrant and probable cause.

Id.

This approach makes sense, as it treats the University much like a landlord, who may inspect for fire hazards and damage but cannot let the police in to search. "[C]ourts are understandably reluctant to put the student who has the college as a landlord in a significantly different position than a student who lives off campus in a boarding house." *People v. Superior Court (Walker)*, 143 Cal. App. 4th 1183, 1202, 49 Cal. Rptr. 3d 831, 845 (2006) (quoting 4 LaFave, Search and Seizure (4th ed. 2004) § 8.6(e), pp. 260–261). The district court's decision below creates exactly this discrimination between those students who live on versus off campus.

Despite the requests below by Appellees, the district court did not invoke the administrative search doctrine. But even if this were an administrative search, it would still be unconstitutional, since "in order for an administrative search to be constitutional, the subject of the search must be afforded an opportunity to obtain precompliance review before a neutral decisionmaker." *City of L.A. v. Patel*, 576 U.S. 409, 420 (2015). Appellants were the subject of the search, and as subjects of the search they were entitled to review. The University's policy provides for no such precompliance review—indeed there is no review at all: instead, this highly sensitive

information is available to "all eligible employees and designated appointees of the university for all legitimate university purposes." S.A. 6. There is no real question of the sufficiency of the University's policy and process, because there is no real process: any employee can request to access Appellants movements for anything they claim is a University purpose, with no review by ether the subject of the search, or a neutral decision maker, or even a more senior University official. As pled in Count II of the Complaint, S.A. 31, even under the administrative search doctrine the Fourth Amendment entitles Appellants to something more than no process at all.

B. Tracking Plaintiffs' movements was an unreasonable search that violated their Fourth Amendment right to be secure in their home.

Warrantless searches that intrude into the privacy of the home are "presumptively unreasonable absent exigent circumstances." *United States v. Karo*, 468 U.S. 705, 714–15 (1984). This protection extends not only to the physical space of the home, but also to information that emanates such that it is perceivable by the outside world. *Id* at 716; *see also Jardines*, 133 S. Ct. at 1415 (scents emanating from within a home); *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (heat emanating from within the home).

In *Karo*, officers placed a "beeper" inside a container of ether and proceeded to track its movements. *Karo,* 468 U.S. at 708. The Court found the monitoring of the beeper inside the defendants' residence "reveal[ed] a critical fact about the interior of the premises that the Government is extremely interested in knowing . . . [it] indicated that the beeper was inside the house, a fact that could not have been visually verified." *Id* at 715. The mere fact the beeper was inside the house was too

great an intrusion for the Fourth Amendment to tolerate. This is the same basic fact that Defendants tracked Plaintiffs' swipe data to learn: whether or not they were inside their home when they said they were.

In *Kyllo* the emanations from house were heat, rather than radio waves, but still the Court found that the intrusion into the home violated the Fourth Amendment. The Court rejected the government's contention that the lack of "intimate details" rendered the use of the thermal imaging permissible. 536 U.S. at 38. First,

> there is certainly no exception to the warrant requirement for the officer who barely cracks open the front door . . . In the home, our cases show, all details are intimate details, because the entire area is held safe from prying government eyes . . . [what was searched in *Karo*] were intimate details because they were details of the home, just as was the detail of how warm—or even how relatively warm—Kyllo was heating his residence.

Id. at 37–38. Second, there was no reason in principle the intrusion would remain so limited. While the device at issue may have only detected general heat levels, a more advanced version might well allow visitation directly into the most intimate areas of the home. *Id.*

It is therefore of little moment if the intrusion into the privacy of the home is minor. As *Kyllo* makes clear, in the context of the home there is no *de minimis* exception to the warrant requirement. The Court held that where "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." *Id.* at 40. More recently, the Supreme Court held that smells emanating from within a home are

protected from search, though the reasoning was limited to activities that violated the curtilage of the home. *Jardines,* 133 S. Ct. at 1415.

Karo and *Kyllo* are more analogous to the case at bar than *United States v. Knotts*, 460 U.S. 276 (1983), which approved the tracking of a suspects' movements in public, for at least two reasons. First, the information searched here revealed facts about the interior of the home, including access to interior hallways, elevators, and bedrooms, not simply public activity. Second, more recent cases have recognized that modern digital technology has greatly reduced the costs of pervasive round-the-clock surveillance. It was precisely the dangers of fast developing technology that the Supreme Court attempted to protect against in *Kyllo*. 536 U.S. at 36.

In *United States v. Jones*, 565 U.S. 400 (2012), the government attached a GPS tracking device under the bumper of a suspect's car, tracking his movements constantly for a month. The movements there were all public, the sort of thing that an old-fashioned tail could in theory have captured, but there was previously a resource constraint on the government's ability to tail someone so comprehensively. As Justice Alito explained:

> [I]n the pre-computer, pre-Internet age, much of the privacy . . . that people enjoyed was not the result of legal protections or constitutional protections; it was the result simply of the difficulty of traveling around and gathering up information. But with computers, it's now so simple to amass an enormous amount of information about people that consists of things that could have been observed on the streets, information that was made available to the public.

Transcript of Oral Argument at 10–11, *U.S. v. Jones*, 132 S. Ct. 945 (2012) (No. 10-1259).

While the majority opinion in *Jones* was content to resolve the case as an illegal trespass (the physical attachment of the tracker to the suspect's property), five justices expressed concern that "physical intrusion is now unnecessary to many forms of surveillance . . . the monitoring undertaken in this case [can be done] by enlisting factory—or owner—installed vehicle tracking devices or GPS-enabled smartphones." *Id.* at 415 (Sotomayor, J., concurring) (emphasis added); *see also id. at* 428 (Alito, J., concurring).

There was no majority as to how long such tracking had to last to violate the Fourth Amendment, but five justices agreed that "at the very least, longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id.* at 415 (Sotomayor, J., concurring) (internal quotation marks omitted). Justice Sotomayor went further, arguing that the court should consider

> whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques.

Id. In *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the Court partially answered the question that the majority in *Jones* had dodged, holding that warrantless tracking of cell phone locations violated the Fourth Amendment. The government in *Carpenter* had obtained records kept by the phone company of where the defendant's cell phone had been over the course of several months, and unfortunately for Mr. Carpenter the locations matched up with a string of robberies. The majority opinion held that even though the data in question was public movements, "[a] person does not surrender all

Fourth Amendment protection by venturing into the public sphere." *Carpenter,* 138 S. Ct. at 2217. It embraced the view taken by the concurrences in *Jones*:

> Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so for any extended period of time was difficult and costly and therefore rarely undertaken. For that reason, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.

Carpenter, 138 S. Ct. at 2217 (quoting *Jones,* 132 S. Ct. at 964 (Alito, J., concurring)) (internal quotation marks and citations omitted). The Court stressed that the backward-looking nature of the cell phone records was particularly troubling:

> Moreover, the retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers.

Carpenter, 138 S. Ct. at 2218.

The court below distinguished *Carpenter* on the theory that "the limited nature of Defendants' use of the SwipeData" did not rise to that level, since only a specific subset of the swipe records were reviewed. But by that reasoning the cell phone in *Carpenter* likewise only provided a limited set of data points: each cell tower Mr. Carpenter's phone connected to on the relevant days. The swipe data tracks Appellants all around campus: where and when they eat, sleep, do laundry, study, shop, and even go to the bathroom—single datapoints add up to a comprehensive portrait of their movements. In *Carpenter*, the government had months of location information, even though in the end at trial it only needed the four locations that

corresponded to the four robberies. In this case, the University retains months of historical swipe data—the fact that it only needed a few days' worth of swipes for this specific investigation doesn't lessen the pervasiveness of the surveillance.

The district court also reasoned that Appellants should expect this sort of surveillance, because they also carry cell phones that sometimes track their movements. S.A. 15. But the entire point of *Carpenter* is that citizens do not forfeit their expectation of privacy simply by living in the modern world. Even before *Carpenter*, the Supreme Court had rejected searching cell phones incident to arrest, since 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).

The district court relied on this Court's decision in *Naperville Smart Meter Awareness v. City of Naperville,* 900 F.3d 521, 528 (7th Cir. 2018), where a public utility collected data on resident's electricity use. But that case is distinguishable on the key point: "[c]ritically, Naperville conduct[ed] the search with no prosecutorial intent." That is not this case. This was a disciplinary investigation, which could well have resulted in suspension, expulsion, or referral to law enforcement. That context is fundamentally different than a utility keeping track of how much electricity its selling.

The district court closed its opinion with an extended passage from this Court's recent opinion in *United States v. Tuggle*, 4 F.4th 505, 509–10 (7th Cir. 2021). The quoted portions make out an argument that advancing technology can alter

expectations of privacy, including curtailing privacy that was once expected. *Id.* But *Tuggle* made these observations in a particular context: it held that "extensive pole camera surveillance in this case did not constitute a search . . . [because] the government's use of a technology in public use, while occupying a place it was lawfully entitled to be, to observe plainly visible happenings, did not run afoul of the Fourth Amendment." *Id.* at 511. The three cameras in *Tuggle* were recording *in public* at a *single location* (Tuggle's residence). *Id.* The cameras did not follow Tuggle around town, and they did not invade the interior of his home. There was therefore no search because there was no expectation of privacy in what was taking place in public at a single location. In Appellants' case, by contrast, the data tracking followed them all across (and even off) campus—and then into the interior of their home, where it tracked their movement among interior floors and hallways, as well as their access to their own bedrooms. Unlike *Tuggle*, therefore, the data accessed here "reveal[ed] a critical fact about the interior of the premises that the Government is extremely interested in knowing." *Karo,* 468 U.S. at 715. No such facts about the interior of *Tuggle's* home were similarly revealed.

This Court should recognize the ways in which pervasive tracking of this information could be misused. A hostile university administration could track which students attended meetings of the Federalist Society or Black Lives Matter; university employees would know who is going to the campus psychologist for counseling or to the campus clinic that tests for sexually transmitted infections; they may have records of each evening students spent with their significant other (or were

cheating on their significant other), including whether a closeted student is visiting a significant other of the same sex. And if the fact that the government is acting as landlord means they can use these records to investigate residents of a dorm, then the government as landlord can also use them in public housing projects to track poorer citizens going about their daily movements. Such a broad assertion of authority has already been rightly rejected. *Pratt v. Chicago Hous. Auth.,* 848 F. Supp. 792 (N.D. Ill. 1994).

This sort of tracking violates Appellants' Fourth Amendment rights: it invades students' privacy in the most intimate of spaces, their home, and uses modern technology that places this information in the context of all their activities across their days. This Court should reverse the dismissal of Appellants' Fourth Amendment claims, finding that the facts alleged are sufficient to demonstrate an unreasonable search under the Fourth Amendment.[4]

CONCLUSION

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

Dated: November 8, 2021

[4] Since the federal claims were dismissed, it was within the district court's discretion to decline to exercise jurisdiction over Appellants' state law claim. *See* 28 USCS § 1367(c)(3). Since the court did not issue a ruling on that issue, Appellants do not address the issue in this appeal. But because the federal claims (Counts I and II) should not have been dismissed for the reasons stated herein, Count III should therefore not have been dismissed for lack of jurisdiction, and Appellants will continue to seek redress for the breach of contract in district court should this court reverse.

/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

Attorney for Plaintiff-Appellant

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 5,877 words.

/s/ Jeffrey M. Schwab
Jeffrey M. Schwab

CERTIFICATE OF SERVICE

I hereby certify that on November 8, 2021, I electronically filed the foregoing Appellants' 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

REQUIRED SHORT APPENDIX

Contents

Certificate

Pursuant to Circuit Rule 30(d), I hereby certify that this short appendix includes all the materials required by Circuit Rules 30(a) and (b).

/s/ Jeffrey M. Schwab
Jeffrey M. Schwab

Counsel for Plaintiffs-Appellants

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

TYLER CAMERON GUTTERMAN, DALE NELSON, HUNTER JOHNSON, and BRIAN HILTUNEN,	)	
Plaintiffs,	)	No. 1:20-cv-02801-JMS-MJD
vs.	)	
INDIANA UNIVERSITY, BLOOMINGTON and PAMELA S. WHITTEN, *in her official capacity as President of Indiana University,*	)	
Defendants.	)	

ORDER

Plaintiffs Tyler Gutterman, Dale Nelson, Hunter Johnson, and Brian Hiltunen are all undergraduate students at Defendant Indiana University, Bloomington ("IU"). In 2018, Plaintiffs were pledges at Beta Theta Pi, a fraternity at IU. They allege that IU used data gathered from their Official University Identification Card ("CrimsonCard") to track their movements as part of an investigation into hazing at Beta Theta Pi, which violated their rights under the Fourth and Fourteenth Amendments to the United States Constitution, and constituted a breach of contract. IU and Defendant Pamela Whitten,[1] IU's President, have filed a Motion to Dismiss pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6), [Filing No. 19], which is now ripe for the Court's consideration.

[1] Plaintiffs originally sued Michael McRobbie, who was IU's President when this litigation was initiated. [*See* Filing No. 1.] Since then, Pamela Whitten became IU's President, IU moved to substitute her for former-President McRobbie as a Defendant, [Filing No. 46], and the Court granted the motion, [Filing No. 47]. The Court will consider all references that the parties make to former-President McRobbie in their filings to apply equally to President Whitten.

I.
STANDARD OF REVIEW

Rule 12(b)(1) "allows a party to move to dismiss a claim for lack of subject matter jurisdiction." *Hallinan v. Fraternal Order of Police of Chicago Lodge No. 7*, 570 F.3d 811, 820 (7th Cir. 2009). When deciding a motion to dismiss under Rule 12(b)(1), the Court accepts the allegations in the plaintiff's complaint as true and draws all reasonable inferences in the plaintiff's favor. *Long v. Shorebank Dev. Corp.*, 182 F.3d 548, 554 (7th Cir. 1999). The burden is on the plaintiff to prove, by a preponderance of the evidence, that subject matter jurisdiction exists for his or her claims. *See Lee v. City of Chicago*, 330 F.3d 456, 468 (7th Cir. 2003).

Under Rule 12(b)(6), a party may move to dismiss a claim that does not state a right to relief. The Federal Rules of Civil Procedure require that a complaint provide the defendant with "fair notice of what the…claim is and the grounds upon which it rests." *Erickson v. Pardus*, 551 U.S. 89, 93 (2007) (quotation and citation omitted). In reviewing the sufficiency of a complaint, the Court must accept all well-pled facts as true and draw all permissible inferences in favor of the plaintiff. *See Active Disposal Inc. v. City of Darien*, 635 F.3d 883, 886 (7th Cir. 2011). A Rule 12(b)(6) motion to dismiss asks whether the complaint "contain[s] sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 570). The Court will not accept legal conclusions or conclusory allegations as sufficient to state a claim for relief. *See McCauley v. City of Chicago*, 671 F.3d 611, 617 (7th Cir. 2011). Factual allegations must plausibly state an entitlement to relief "to a degree that rises above the speculative level." *Munson v. Gaetz*, 673 F.3d 630, 633 (7th Cir. 2012). This plausibility determination is "a context-specific task that requires the reviewing court to draw on its judicial experience and common sense." *Id.*

II.
BACKGROUND

The following factual allegations are taken from the Complaint, and are accepted as true solely for the purpose of this Order.

A. Plaintiffs' Membership in Beta Theta Pi

Plaintiffs are undergraduate students at IU and in the fall of 2018, they were all freshmen completing their first semester of study. [Filing No. 1 at 3.] As freshmen, Plaintiffs chose to take part in IU's campus traditions and activities, including IU's Greek life. [Filing No. 1 at 3.] Plaintiffs all chose to pledge the same fraternity, Beta Theta Pi. [Filing No. 1 at 3.]

B. CrimsonCards and Swipe Data

Plaintiffs were required to carry their CrimsonCard as a condition of their attendance at IU, and IU retains historical records of CrimsonCard usage. [Filing No. 1 at 4.] IU's records track every time a student "swipes" their CrimsonCard to gain access to a university building or to use a university facility ("Swipe Data"). [Filing No. 1 at 4.] IU's website explains: "CrimsonCard is much more than a photo ID. It's a print release card, keycard to authorized university buildings, library card, and if you're enrolled in a dining service plan, it's your meal ticket." [Filing No. 1 at 4.]

The back of the CrimsonCard provides:

> **INDIANA UNIVERSITY**
>
> If found, please contact: (317) 274-0400
>
> Manage your account online: crimsoncard.iu.edu
>
> Use of this card constitutes acceptance of the CrimsonCard terms and conditions. This card is the property of Indiana University and is intended for use only by Indiana University and its affiliates. Unauthorized use, lending, or tampering with the card warrants confiscation and/or disciplinary action.

[Filing No. 20 at 11.][2]

> The CrimsonCard Terms and Conditions provide as follows:
>
> The CrimsonCard…is issued by [IU] to its students and employees, and others associated with [IU], to verify their identity and manage access to [IU] services and facilities.
>
> The Card also functions as a stored value card, and is associated with an account, the "CrimsonAccount – CrimsonCash."
>
> * * *
>
> This Agreement is entered into between [IU] and each student….
>
> In exchange for being issued a Card, Cardholder agrees to abide by the *Official University Identification Card Policy* (available on the University Policies website at http://policies.iu.edu) (the "Policy") and to the following terms and conditions:
>
> * * *
>
> **Use and Ownership**
>
> Cardholder understands and agrees that the Card is the property of [IU].
>
> * * *
>
> **Damaged, Lost, Stolen, Misused or Expired Cards**
>
> Cardholder is responsible for care and protection of the Card. If the magnetic stripe, or any of the technology contained in or on the card, is damaged and becomes

[2] Defendants have included a photo of the back of the Crimson Card in their brief in support of their Motion to Dismiss, and have attached the CrimsonCard Terms and Conditions, IU's Official University Identification Card Policy (UA-13), and IU's Management of Institutional Data Policy (DM-01) to their brief. [Filing No. 20 at 11; Filing No. 20-1; Filing No. 20-2; Filing No. 20-3.] When reviewing a motion to dismiss, the Court considers only the factual allegations of the complaint and any reasonable inferences; however, the Court may also consider any documents to which the complaint refers and that are central to the plaintiff's claims. *Adams v. City of Indianapolis*, 742 F.3d 720, 729 (7th Cir. 2014). Here, Plaintiffs refer to the CrimsonCard and all of the documents that Defendants attach to their Motion to Dismiss, and the Court finds that the CrimsonCard and those documents are central to Plaintiffs' claims. Consequently, the Court may consider the CrimsonCard, the CrimsonCard Terms and Conditions, IU's Official University Identification Card Policy (UA-13), and IU's Management of Institutional Data Policy (DM-01) in connection with Defendants' Motion to Dismiss.

> unreadable by any Card reader or terminal, Cardholder is required to obtain a replacement of the Card at Cardholder's expense….

[Filing No. 20-1 at 2-3.]

> IU's Official University Identification Card Policy (UA-13) provides:
>
> **Policy Statement**
>
> [IU] issues Photo Identification Cards…to employees, students, and others associated with [IU] to verify their identity and manage their access to [IU] services and facilities.
>
> The ID card will be used to verify the identity of the bearer of the card in [IU] facilities when such identification is needed to be present at those facilities or on [IU] grounds.
>
> * * *
>
> **Intended Use of the Official University Identification Card**
>
> * * *
>
> 2. The Official University Identification Card is intended for use as an electronic identification, validation, and authentication credential for authorized access to services and facilities. The Official University Identification Card is the property of the University and will be deactivated and/or invalidated by the University upon expiration of its intended use.
>
> * * *
>
> 4. The Official University Identification Card may be used to verify the identity of the bearer of the card while on University grounds.

[Filing No. 20-2 at 4-6.]

> IU's Management of Institutional Data Policy (DM-01) states:
>
> **Scope**
>
> This policy applies to all users of [IU] information and information technology resources regardless of affiliation, and irrespective of whether these resources are accessed from on-campus or off-campus locations.

> This policy applies to all institutional data, and is to be followed by all those who capture data and manage administrative information systems using university assets.
>
> **Policy Statement**
>
> * * *
>
> The permission to access institutional data should be granted to all eligible employees and designated appointees of the university for all legitimate university purposes.

[Filing No. 20-3 at 4.]

The Swipe Data includes the whole range of students' movements and activities, including access to dorm buildings, individual dorm rooms, elevators, and dorm building common areas. [Filing No. 1 at 5.] The Swipe Data also reflects students' movements around campus, including checking out library books, accessing academic buildings, accessing parking garages, using parking meters, purchasing meals at university dining halls, purchasing sodas and snacks from campus vending machines, using laundry machines, printing materials they need for class on university printers, and other daily activities. [Filing No. 1 at 5.] The Swipe Data is not limited to campus facilities, as the CrimsonCard operates as a payment card at numerous businesses near campus, including restaurants, grocery stores, pharmacies, airport shuttles, tanning salons, and wellness centers. [Filing No. 1 at 6.] The subject of a search of Swipe Data is not given "the opportunity to obtain precompliance review before a neutral decisionmaker." [Filing No. 1 at 6.]

C. IU's Investigation Into Hazing at Beta Theta Pi

During the fall 2018 semester, Beta Theta Pi was being investigated by IU for a suspected hazing incident. [Filing No. 1 at 3.] As part of its investigation, IU officials accessed Plaintiffs' Swipe Data, which it retained for several months, to track Plaintiffs' movements. [Filing No. 1 at 3-4.] Specifically, IU compared the Swipe Data associated with Plaintiffs to their testimony

regarding their whereabouts at the time of the incident. [Filing No. 1 at 4.] Plaintiffs had testified that they were in their dorm rooms at the time of the suspected hazing incident. [Filing No. 1 at 4.] The investigation resulted in sanctions for Beta Theta Pi, but Plaintiffs were not found guilty of any wrongdoing. [Filing No. 1 at 4.]

D. The Lawsuit

Plaintiff initiated this litigation on October 29, 2020, and set forth claims for: (1) violation of the right to be free of unreasonable searches under the Fourth and Fourteenth Amendments to the United States Constitution; (2) violation of the Fourth and Fourteenth Amendments to the United States Constitution because IU's use of Swipe Data does not provide an opportunity for students being searched to obtain "precompliance review from a neutral third party"; and (3) breach of contract. [Filing No. 1 at 10-12.] Plaintiffs seek nominal damages, declaratory relief, and attorneys' fees and costs, and request that the Court enjoin IU from "further use of swipe data in investigations except where [IU] has obtained a warrant or can demonstrate exigent circumstances," and require IU to "expunge the investigation for which [IU] used swipe data of Plaintiffs from their permanent records, to the extent that Plaintiffs' records include information about such investigation." [Filing No. 1 at 13.] IU and President Whitten have filed a Motion to Dismiss all of Plaintiffs' claims. [Filing No. 19.]

III. DISCUSSION

A. Constitutional Claims

Defendants argue in their Motion to Dismiss that Plaintiffs' constitutional claims are barred by Eleventh Amendment immunity (with the exception of their claim for prospective injunctive relief against President Whitten), and that their constitutional claims do not state claims for which

relief can be granted because IU did not perform a search of their information, and because any search was reasonable in any event. The Court addresses each issue in turn.

1. Whether Defendants Are Immune From Liability Under the Eleventh Amendment

In support of their Motion to Dismiss, Defendants argue that IU is entitled to sovereign immunity under the Eleventh Amendment because it has not waived that immunity or consented to this lawsuit. [Filing No. 20 at 6.] Defendants also assert that President Whitten is entitled to Eleventh Amendment immunity for the constitutional claims against her in her official capacity that seek damages, but acknowledge that immunity does not shield her from Plaintiffs' constitutional claims for prospective injunctive relief. [Filing No. 20 at 7.]

In their response, Plaintiffs argue that IU employees are state actors and can be sued under 42 U.S.C. § 1983 for violating the Fourth Amendment. [Filing No. 28 at 4.] They then appear to concede that Eleventh Amendment immunity shields IU from their constitutional claims, and also shields President Whitten in her official capacity except in connection with their claims for prospective injunctive relief, but assert that to the extent they seek declaratory and injunctive relief, their constitutional claims are not barred by sovereign immunity. [Filing No. 28 at 4-5.]

In their reply, Defendants contend that § 1983's enactment did not abrogate the State's Eleventh Amendment immunity and reiterate the arguments set forth in their opening brief. [Filing No. 33 at 3-4.]

Eleventh Amendment immunity bars suits against states and their agencies regardless of whether the relief sought is monetary damages or injunctive relief. *Seminole Tribe of Florida v. Florida*, 517 U.S. 44, 58 (1996); *Pennhurst State School & Hosp. v. Halderman*, 465 U.S. 89, 101-02 (1984). The only exceptions to this rule are when a state has waived immunity by consenting to suit in federal court or Congress has abrogated the state's immunity "through a valid exercise of

its powers under recognized constitutional authority." *Ind. Prot. & Adv. Servs. v. Ind. Fam. & Soc. Servs. Admin.*, 603 F.3d 365, 371 (7th Cir. 2010).

IU is a state entity. *See* Ind. Code § 21-20-2-1 ("Indiana University is recognized as the university of the state"); *Haynes v. Ind. Univ.*, 902 F.3d 724, 731 (7th Cir. 2018) ("[IU] and its Board of Trustees are state agencies for sovereign-immunity purposes") (citing *Peirick v. Ind. Univ.-Purdue Univ. Indianapolis Athletics Dep't*, 510 F.3d 681, 695 (7th Cir. 2007)); *Woods v. Ind. Univ.-Purdue Univ. at Indianapolis*, 996 F.2d 880, 883 (7th Cir. 1993) ("Indiana University enjoys the same Eleventh Amendment immunity as the State of Indiana itself…."); *Feresu v. Ind. Univ. Bloomington*, 2015 WL 5177740, at *3 (S.D. Ind. 2015) ("IU is an 'instrumentality,' 'arm,' or 'alter ego' of the State of Indiana for purposes of the Eleventh Amendment"). Because IU is a state entity, and since it has not consented to being sued in federal court, Plaintiffs' constitutional claims against it for damages and injunctive relief are barred by Eleventh Amendment immunity. *McDonough Assoc., Inc. v. Grunloh*, 722 F.3d 1043, 1049 (7th Cir. 2013) ("[T]he general rule is that private individuals are unable to sue a state in federal court absent the state's consent").

As for Plaintiffs' constitutional claims against President Whitten, it is well-settled that claims against state officials in their official capacities for monetary relief are barred by the Eleventh Amendment. *Id.* (Eleventh Amendment bars claims seeking "awards of 'accrued monetary liability which must be met from the general revenues of a State'") (quoting *Edelman v. Jordan*, 415 U.S. 651, 664 (1974)). However, a state official is not entitled to Eleventh Amendment immunity where the relief sought is prospective injunctive relief to remedy an ongoing violation of federal law. *Ex parte Young*, 209 U.S. 123, 159-60 (1908). A plaintiff may file suit "against state officials seeking prospective equitable relief for ongoing violations of federal law." *Marie O. v. Edgar*, 131 F.3d 610, 615 (7th Cir. 1997); *see also Ind. Prot. & Adv. Servs.*, 603

F.3d at 371 (discussing exceptions to the Eleventh Amendment's bar to actions in federal court against state officials acting in their official capacities). Accordingly, Eleventh Amendment immunity shields President Whitten from Plaintiffs' constitutional claims to the extent they seek monetary or declaratory relief, but not to the extent that they seek prospective injunctive relief.

The Court **GRANTS** Defendants' Motion to Dismiss Plaintiffs' constitutional claims against IU and Plaintiffs' constitutional claims against President Whitten to the extent that those claims seek monetary or declaratory relief. The Court goes on to discuss the viability of Plaintiffs' constitutional claims against President Whitten to the extent that they seek prospective injunctive relief.

2. Whether Plaintiffs Have Stated A Claim For Constitutional Violations Against President Whitten

In support of their Motion to Dismiss, Defendants argue that Plaintiffs' constitutional claims are premised on IU conducting searches by tracking Plaintiffs' movements with their CrimsonCards, retaining the data, and continuing to access the data without giving the subject of the search an opportunity to obtain precompliance review before a neutral decisionmaker. [Filing No. 20 at 9.] Defendants argue that these allegations do not amount to a search under the Fourth Amendment because IU did not infringe upon Plaintiffs' privacy. [Filing No. 20 at 10-11.] Defendants assert that IU owns all CrimsonCards, and IU policy provides that "'permission to access institutional data should be granted to all eligible employees and designated appointees of the university for all legitimate university purposes.'" [Filing No. 20 at 10.] They assert that IU accessed the Swipe Data "to protect the safety and well-being of its students, which is a legitimate university purpose under [IU] policy." [Filing No. 20 at 10 (quoting Filing No. 20-3 at 4).] Defendants also point to the back of the CrimsonCard, which states that use of the card "constitutes acceptance of the CrimsonCard terms and conditions," and that the card "is the property of [IU]

and is intended for use only by [IU] and its affiliates." [Filing No. 20 at 11.] Defendants argue further that Plaintiffs did not have a reasonable expectation of privacy in their use of the CrimsonCard because they were "aware of the capabilities of the CrimsonCard, and its connection to both IU and University life, from the very beginning." [Filing No. 20 at 12.] Defendants note that the CrimsonCard Terms and Conditions state that the CrimsonCard is used "to verify [students' and employees'] identity and manage access to university services and facilities," and that users are required to obtain a replacement if the magnetic strip is damaged or becomes unreadable. [Filing No. 20 at 13.] Further, Defendants argue that Plaintiffs' movements were out in the open and "anyone could have visually observed [them]," so tracking their movements in not considered a search. [Filing No. 20 at 14.] Defendants distinguish the Swipe Data from data gathered from a GPS device installed on a car, and note that the Swipe Data "provides a single data point for each 'swipe' or access to a student's residence hall or dorm room," but does not show where Plaintiffs went when they were inside or what they did while inside. [Filing No. 20 at 15-16 (emphasis omitted).] Defendants assert that Plaintiffs accepted the CrimsonCard in exchange for the privilege of attending IU and for using the conveniences afforded by the CrimsonCard, and cannot now object to IU's use of the Swipe Data for the legitimate purpose of investigating an alleged hazing incident. [Filing No. 20 at 16.] They argue that the Swipe Data constitutes IU's business records, since the CrimsonCards are IU property. [Filing No. 20 at 17.] Finally, Defendants argue that even if gathering the Swipe Data is considered a search, any search was reasonable because the Swipe data was collected without physical entry into Plaintiffs' homes and it was not collected with prosecutorial intent – but rather to confirm that Plaintiffs were not the victims of hazing. [Filing No. 20 at 20.]

In response, Plaintiffs point to case law which they contend stands for the proposition that students enjoy the protection of the Fourth Amendment in their dormitory rooms. [Filing No. 28 at 7.] They distinguish cases allowing universities to routinely inspect dorm rooms, and contend that IU's use of Swipe Data "is fundamentally a prosecutorial function that implicates [IU's] role as the government, rather than its role as landlord." [Filing No. 28 at 12.] They note that IU "was investigating alleged off-campus conduct and the search of Plaintiffs' [Swipe Data] to determine their presence in the dorms was orthogonal to that investigation." [Filing No. 28 at 12.] Plaintiffs also argue that they did not consent to the gathering and use of Swipe Data because they could not waive their constitutional rights "unwittingly or by implication." [Filing No. 28 at 12.] They contend that even if using the Swipe Data was considered an administrative search, they would then be entitled to "precompliance review before a neutral decisionmaker." [Filing No. 28 at 13.] Finally, Plaintiffs argue that the Swipe Data "tracks [them] all around campus: where and when they eat, sleep, do laundry, study, shop, and even go to the bathroom – single datapoints add up to a comprehensive portrait of their movements." [Filing No. 28 at 19.]

In their reply, Defendants argue that Plaintiffs focus on the interior of their dorm rooms, but that "[t]here are simply no allegations that support any inference that [IU] searched or entered [their] dorm rooms" or otherwise invaded their privacy in their homes. [Filing No. 33 at 6.] They note that they only accessed limited Swipe Data for the time of the hazing incident and to determine whether members of Plaintiffs' pledge class were the victims of hazing. [Filing No. 33 at 6.] Defendants assert that Plaintiffs' argument regarding IU's use of Swipe Data – that it was used to track Plaintiffs "all around campus" – is "vastly different from the allegations in their Complaint that [IU] 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.'" [Filing No. 33 at 6-7.] Defendants point again

to IU's policies, which provide that CrimsonCards and the Swipe Data are IU's property, and note that the CrimsonCard generates data when it is voluntarily used to access a building or room and not continuously or involuntarily. [Filing No. 33 at 8-9.] Defendants reiterate their arguments that even if gathering and using the Swipe Data was a search, it was reasonable. [Filing No. 33 at 11-13.]

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. "The 'touchstone' of the Fourth Amendment analysis is whether a person has a 'constitutionally protected reasonable expectation of privacy.'" *Henry v. Hulett*, 969 F.3d 769, 776-77 (7th Cir. 2020) (quoting *Oliver v. United States*, 466 U.S. 170, 177 (1984)). To trigger protection, an individual must have "a subjective expectation of privacy and…society [must be] prepared to recognize [that expectation] as reasonable." *United States v. Hammond*, 996 F.3d 374, 383-84 (7th Cir. 2021) (quotations and citations omitted). "To determine whether someone has a legitimate expectation of privacy, courts must consider (1) whether that person, by his conduct, has exhibited an actual, subjective expectation of privacy and (2) whether his expectation of privacy is one that society is prepared to recognize as reasonable." *United States v. Sawyer*, 929 F.3d 497, 499 (7th Cir. 2019).

The Seventh Circuit has instructed that a search occurs "either when the government physically intrudes without consent upon 'a constitutionally protected area in order to obtain information,' or 'when an expectation of privacy that society is prepared to consider reasonable is infringed.'" *United States v. Thompson*, 811 F.3d 944, 948 (7th Cir. 2016) (quoting *United States v. Jones*, 565 U.S. 400, 407 (2012) and *United States v. Karo*, 468 U.S. 705, 712 (1984)). Only searches which are unreasonable violate the Fourth Amendment. *Florida v. Jimeno*, 500 U.S. 248,

250 (1991). When an alleged search is not performed as part of a criminal investigation, the Court may "turn immediately to an assessment of whether [the search is] reasonable." *Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 528 (7th Cir. 2018). The Court follows this principle, assumes without deciding that a search occurred, and turns directly to the question of whether the search was reasonable.

In order to determine whether a search was reasonable, the Seventh Circuit has instructed that the Court should "balance[e] [the search's] intrusion on the individual's Fourth Amendment interests against its promotion of legitimate government interests." *Hiibel v. Sixth Judicial Dist. Court*, 542 U.S. 177, 187-88 (2004); *see also United States v. White*, 781 F.3d 858, 862 (7th Cir. 2015). This requires considering "[t]he totality of the circumstances" by assessing "one's status and privacy expectations and the context in which the search occurs." *United States v. Wood*, 426 F.Supp.3d 560, 565-66 (N.D. Ind. 2019) (citing *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 654 (1995)).

The Court first considers Plaintiffs' status and privacy expectations. Plaintiffs allege that they were students at IU when their Swipe Data was accessed, and when they became IU students, they received their CrimonCards and had access to the CrimsonCard Terms and Conditions. The CrimsonCard itself states on the back that the user of the card accepts its terms and conditions, and that the card is the property of IU. [Filing No. 20 at 11.] The CrimsonCard Terms and Conditions state that the CrimsonCard is used "to verify [a student's] identity and manage access to [IU] services and facilities." [Filing No. 20-1 at 2.] Given that Plaintiffs were on notice that the CrimsonCard was used to access IU's services and facilities, and that IU owned the card, it is not reasonable to conclude that Plaintiffs expected their use of the CrimsonCard – which, in turn, reflected which IU facilities and services they accessed – to be private. The Court finds that this

is particularly true in today's day and age, when Plaintiffs were likely carrying cell phones which also could be used to track their locations to some extent, and where cameras on buildings, traffic lights, and businesses were likely to capture many of Plaintiffs' public movements. While the CrimsonCard does not explicitly state that Plaintiffs were agreeing to IU using the Swipe Data to verify their whereabout at a specific point in time, Plaintiffs were certainly on notice that the CrimsonCard would reflect their movements to some degree.

As for the context in which the search occurred, Plaintiffs allege that IU retains "historical records" of Swipe Data, and "retained the [Swipe Data] for several months and used it to check the alibis of several students – including Plaintiffs." [Filing No. 1 at 3-4.] But Plaintiffs only allege that Defendants accessed their personal Swipe Data for a limited time period, and for the purpose of checking Plaintiffs' whereabouts at the time of the hazing incident for which the Beta Theta Pi house was ultimately disciplined. *See Naperville Smart Meter Awareness*, 900 F.3d at 528 (finding that collection of energy use data was a reasonable search and noting "[c]ritically, Naperville conducts the search with no prosecutorial intent. Employees of the city's public utility – not law enforcement – collect and review the data"). Plaintiffs do not allege that IU used the Swipe Data to track their movements all around campus, or to track their locations for an extended period of time. The collection of Swipe Data is "far less invasive than the prototypical Fourth Amendment search of a home." *Id.* Moreover, the limited nature of Defendants' use of the Swipe Data, as alleged in the Complaint, indicates that the Swipe Data does not provide "an intimidate window into [a student's] life, revealing…his familial, political, professional, religious, and sexual associations" to the degree the United States Supreme Court has recognized as unreasonable. *Carpenter v. U.S.*, 138 S.Ct. 2206, 2217 (2018). Finally, according to Plaintiffs' own allegations, the Swipe Data was used to verify Plaintiffs' whereabouts at the time of the alleged hazing incident,

and "as freshmen pledges, [Plaintiffs] would have been far more likely to be the victims of any hazing activity, rather than the perpetrators." [Filing No. 1 at 4.] In other words, as Plaintiffs allege, the Swipe Data was used to ensure Plaintiffs' safety by confirming that Plaintiffs were not subjected to hazing – an interest the Court finds to be plainly legitimate.

In short, the Court finds that, assuming a search occurred in the first instance, such a search was reasonable based on Plaintiffs' status as IU students who agreed to the Terms and Conditions of the CrimsonCard, and based on IU's limited, non-prosecutorial use of the Swipe Data to confirm that Plaintiffs were not present during a hazing incident. The Court **GRANTS** Defendants' Motion to Dismiss Plaintiffs' constitutional claims against President Whitten to the extent that they seek prospective injunctive relief.

B. Breach of Contract Claim

In support of their Motion to Dismiss, Defendants argue that they are entitled to Eleventh Amendment immunity on Plaintiffs' breach of contract claim because the Court's supplemental jurisdiction does not extend to state-law claims against "non-consenting state defendants." [Filing No. 20 at 8 (quotation omitted).] Defendants also argue that Plaintiffs lack standing to assert a breach of contract claim because they do not allege any injury, and that IU did not breach a contract with Plaintiffs. [Filing No. 20 at 21-29.]

In response, Plaintiffs argue that privacy violations constitute an inherent injury, and that retaining the Swipe Data caused an ongoing injury. [Filing No. 28 at 21.] They contend that IU breached its own policies by using the Swipe Data "to check past entries to University buildings to check the alibis of students during an investigation," and that this "does not comport with the intended purpose of the [CrimsonCard]." [Filing No. 28 at 22-23.]

In their reply, Defendants reiterate many of their arguments. [Filing No. 33 at 13-20.]

Because the Court has dismissed all of Plaintiffs' federal claims, it must determine whether it will exercise jurisdiction over Plaintiffs' breach of contract claim. A district court ultimately has discretion whether to exercise supplemental jurisdiction over a plaintiff's state law claims. *Carlsbad Tech., Inc. v. HIF Bio, Inc.*, 556 U.S. 635, 639 (2009); 28 U.S.C. § 1367(c) ("The district courts may decline to exercise supplemental jurisdiction over a claim…if…the district court has dismissed all claims over which it has original jurisdiction…"). When deciding whether to exercise supplemental jurisdiction, "a federal court should consider and weigh in each case, and at every stage of the litigation, the values of judicial economy, convenience, fairness, and comity." *City of Chicago v. Int'l Coll. of Surgeons*, 522 U.S. 156, 173 (1997) (quotations and citations omitted).

The Court finds that the balance of factors weighs in favor of declining to exercise supplemental jurisdiction over the remaining state law claim. First, as to judicial economy, the parties have not yet engaged in discovery on the breach of contract claim. Second, as far as convenience, witnesses and evidence related to the breach of contract claim would likely be located in Bloomington, where a state court could decide the claim, and not in Indianapolis, where this Court is located. And third and fourth, whether IU breached the Terms and Conditions of the CrimsonCard or its own policies through activities which occurred at a university located in Bloomington is quintessentially a local issue which is best decided by a state court, making the interests of fairness and comity factors weigh in favor of this Court declining to exercise supplemental jurisdiction over the state law breach of contract claim.

The Court **DENIES** Defendants' Motion to Dismiss Plaintiffs' breach of contract claim, but declines to exercise supplemental jurisdiction over that claim and **DISMISSES** it **WITHOUT PREJUDICE** to re-file that claim in state court.

IV.
CONCLUSION

> One day, in a not-so-distant future, millions of Americans may well wake up in a smart-home-dotted nation. As they walk out their front doors, cameras installed on nearby doorbells, vehicles, and municipal traffic lights will sense and record their movements, documenting their departure times, catching glimpses of their phone screens, and taking note of the people that accompany them. These future Americans will traverse their communities under the perpetual gaze of cameras…. [A]s society's uptake of a new technology waxes – cars, GPS devices, cameras, and the Internet come to mind – expectations of privacy in those technologies wane. In today's interconnected, globalized, and increasingly digital world, for example, Americans largely accept that cell phones will track their locations, their Internet usage will leave digital footprints, and ever-watching fixed cameras will monitor their movements. These evolving expectations thus continually undermine themselves. As long as the government moves discreetly with the times, its use of advanced technologies will likely not breach society's reconstituted (non)expectations of privacy.

United States v. Tuggle, 4 F.4th 505, 509-10 (7th Cir. 2021). Given the very limited scope of Plaintiffs' reasonable privacy expectations as IU students required to use the CrimsonCard to access various facilities and use certain amenities, and the context in which Plaintiffs allege that IU used the Swipe Data, the Court finds that Plaintiffs have not plausibly alleged that IU's use of the Swipe Data, to the extent it constituted a search, was unreasonable. Accordingly, the Court:

- **GRANTS** Defendants' Motion to Dismiss to the extent that it **DISMISSES [19]** Plaintiffs' federal constitutional claims **WITH PREJUDICE**;[3] and

[3] The Court is dismissing Plaintiffs' constitutional claims with prejudice. Pursuant to Federal Rule of Civil Procedure 15(a)(1)(B), a plaintiff may amend his complaint once as a matter of course in response to a motion to dismiss. Fed. R. Civ. P. 15(a)(1)(B). The 2009 notes to that rule emphasize that this amendment "will force the pleader to consider carefully and promptly the wisdom of amending to meet the arguments in the motion. A responsive amendment may avoid the need to decide the motion or reduce the number of issues to be decided, and will expedite determination of issues that otherwise might be raised seriatim." Plaintiffs chose not to exercise their right to amend their Complaint pursuant to Rule 15(a)(1)(B) in response to Defendants' Motion to Dismiss but, instead, chose to brief the motion and have the Court adjudicate the issues. The Court is not required to give Plaintiffs another chance to plead their claims because they have already had an opportunity to cure deficiencies in their pleadings. *See Emery v. Am. Gen. Fin., Inc.*, 134 F.3d 1321, 1322-23 (7th Cir. 1998). Consequently, the Court, in its discretion, dismisses Plaintiffs' constitutional claims with prejudice.

- **DENIES** Defendants' Motion to Dismiss Plaintiffs' breach of contract claim, but declines to exercise supplemental jurisdiction over that claim and **DISMISSES** it **WITHOUT PREJUDICE [19]**.

Final judgment shall enter accordingly.

Date: 9/1/2021

Hon. Jane Magnus-Stinson, Judge
United States District Court
Southern District of Indiana

Distribution via ECF only to all counsel of record

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

TYLER CAMERON GUTTERMAN, DALE NELSON, HUNTER JOHNSON, and BRIAN HILTUNEN,	)	
Plaintiffs,	)	No. 1:20-cv-02801-JMS-MJD
vs.	)	
INDIANA UNIVERSITY, BLOOMINGTON and PAMELA S. WHITTEN, *in her official capacity as President of Indiana University,*	)	
Defendants.	)	

FINAL JUDGMENT PURSUANT TO FED. R. CIV. P. 58

For the reasons set forth in the Court's Order entered this day, the Court now enters **FINAL JUDGMENT** against Plaintiffs and in favor of Defendants. Plaintiffs' federal constitutional claims for damages and declaratory relief against Indiana University and President Whitten in her her official capacity are **DISMISSED FOR LACK OF JURISDICTION,** Plainitffs claims for injunctive relief against President Whitten in her official capacaity are **DISMISSED WITH PREJUDICE**, and their breach of contract claim is **DISMISSED WITHOUT PREJUDICE**.

Date: 9/1/2021

Hon. Jane Magnus-Stinson, Judge
United States District Court
Southern District of Indiana

Distribution via ECF only to all counsel of record

Roger A.G. Sharpe, Clerk

BY: _____
Deputy Clerk, U.S. District Court

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF INDIANA

Tyler Cameron Gutterman, Dale Nelson, Hunter Johnson, *and* Brian Hiltunen, Plaintiffs, v. Indiana University, Bloomington; *and* Michael McRobbie, *in his official capacity as President of Indiana University,* Defendants.	Case No. 1:20-CV-2801 **Complaint**

1. Plaintiffs, undergraduate students at Indiana University Bloomington, were subject to illegal surveillance by the University that violated the Fourth Amendment's prohibition on unreasonable searches and breached the University's contractual obligations to Plaintiffs. The University used Student ID Cards, which it required Plaintiffs to carry, as a tool to track Plaintiffs' movements into and out of their dorms as part of an official investigation into Plaintiffs' fraternity's conduct. The University continues to collect data on students' movements using Student ID Cards, and may access such data without providing the subject of the search an opportunity to challenge the use of such data before a neutral decisionmaker.

2. Plaintiffs therefore bring this action pursuant 42 U.S.C. § 1983 and 28 U.S.C. § 1367, seeking declaratory and injunctive relief for the violations of their constitutional and contractual rights, and nominal damages in the amount of $1.

PARTIES

3. Plaintiff Tyler Cameron Gutterman is an undergraduate student at Indiana University Bloomington, who began his studies in the fall of 2018. During the school year, he resides in Monroe County, Indiana.

4. Plaintiff Dale Nelson is an undergraduate student at Indiana University Bloomington, who began his studies in the fall of 2018. During the school year, he resides in Monroe County, Indiana.

5. Plaintiff Hunter Johnson is an undergraduate student at Indiana University Bloomington, who began his studies in the fall of 2018. During the school year, he resides in Monroe County, Indiana.

6. Plaintiff Brian Hiltunen is an undergraduate student at Indiana University Bloomington, who began his studies in the fall of 2018. During the school year, he resides in Monroe County, Indiana.

7. Defendant Indiana University Bloomington is a public research university in Bloomington, Monroe County, Indiana, and the flagship institution of the Indiana University system.

8. Defendant Michael McRobbie is the President of Indiana University, and is sued in his official capacity. His office address is Bryan Hall 200, 107 S. Indiana Ave. Bloomington, Indiana 47405.

JURISDICTION AND VENUE

9. This case raises claims under the Fourth Amendment of the United States Constitution and 42 U.S.C. § 1983. The Court has subject-matter jurisdiction under 28 U.S.C. § 1331 and 28 U.S.C. § 1343; The Court has pendant jurisdiction over Plaintiffs' breach of contract claim under 28 U.S.C. § 1367.

10. Venue is appropriate under 28 U.S.C. § 1391(b) because a substantial portion of the events giving rise to the claims occurred in the Southern District of Indiana.

FACTUAL ALLEGATIONS

11. Plaintiffs Gutterman, Nelson, Jackson, and Hiltunen are undergraduate students at Indiana University Bloomington ("IU").

12. In the fall of 2018, all four Plaintiffs were freshmen completing their first semester of study at IU.

13. As freshmen, Plaintiffs chose to take part in IU's campus traditions and activities, including its Greek life. All four plaintiffs chose to pledge for the same fraternity, Beta Theta Pi.

14. During the fall 2018 semester, Beta Theta Pi was subject to an investigation by IU officials into suspected or alleged hazing incidents.

15. As part of this disciplinary investigation, IU officials accessed the historical records of Plaintiffs' Official University Identification Card ("ID Cards," also referred to as a "CrimsonCard") to track Plaintiffs' movements.

16. Plaintiffs are required to carry an ID Card as a condition of their attendance at the University. Upon information and belief, IU retains historical records of ID Card usage.

17. These records track every time a student "swipes" his card to gain access to a university building or to use a university facility ("swipe data"). As the University website explains, "CrimsonCard is much more than a photo ID. It's a print release card, keycard to authorized university buildings, library card, and if you're enrolled in a dining services plan, it's your meal ticket." Indiana University, Using your Card.[1]

18. The University retained the swipe data for several months and used it to check the alibis of several students — including Plaintiffs — after an alleged off-campus hazing incident by comparing their "swipe" data to their testimony as to their whereabouts at the time of the incident. The Plaintiffs had testified they were in their dorm rooms at the time.

19. The investigation resulted in sanctions for Beta Theta Pi, but Plaintiffs were not found guilty of any wrongdoing. Indeed, as freshmen pledges, they would have been far more likely to be the victims of any hazing activity, rather than the perpetrators.

20. The Constitution protects persons from unreasonable searches of their homes and property. U.S. Const. amend IV. *See* Ind. Const. Art. I, Sec. 11. Warrantless searches that intrude into the privacy of the home are "presumptively

[1] https://crimsoncard.iu.edu/using/index.html

unreasonable absent exigent circumstances." *United States v. Karo*, 468 U.S. 705, 714–15 (1984).

21. A college or university dorm room enjoys the same constitutional status as a home, because for the student it is his or her primary/personal residence during the school year. *See Piazzola v Watkins*, 442 F.2d. 284, 289 (5th Cir. 1971).

22. The swipe data encompasses the whole range of students' movements and activities. It is used to access not only students' dorm buildings, but their individual bedrooms — as well as access elevators and dorm building common areas — all spaces in which dorm residents enjoy an expectation of privacy. *See Piazzola*, 442 F.2d. at 288 (quoting *Commonwealth v. McCloskey*, 217 Pa. Super. 432, 435, 272 A.2d 271, 273 (1970)) (a "dormitory room is analogous to an apartment or a hotel room."); *State v. Houvener*, 186 P.3d 370 (Wash. Ct. App. 2008) (recognizing an expectation of privacy in dorm building common areas).

23. The swipe data also records students' movement around campus: students use their ID Cards to check out library books, access academic buildings, parking garages, parking meters, to purchase meals at university dining halls, sodas and snacks from campus vending machines, laundry machines, print materials they need for class on university printers, and all manner of sundry other daily activities — whether eating, sleeping, or studying, the swipe data records and reveals it. *See* Indiana University, Who Accepts CrimsonCard.[2]

[2] https://crimsoncard.iu.edu/using/Who%20Accepts%20CrimsonCard.html

24. Moreover, the swipe data is not limited to campus facilities — it operates as a payment card at numerous businesses nearby, including restaurants, grocery stores, pharmacies, airport shuttles, tanning salons, and or wellness centers. *Id.* Though not involved in this incident, the assertion of authority in this case would equally permit evaluation of students' personal financial information, i.e., swipe data for monetary transactions to determine if a student's alibi that he was at an off-campus restaurant was truthful.

25. The University continues to maintain a database of student swipe data from student ID cards, giving permission to access institutional data to "all eligible employees and designated appointees of the university for all legitimate university purposes." Management of Institutional Data policy (DM–01). The University does not provide the subject of such a search of swipe data the opportunity to obtain precompliance review before a neutral decisionmaker.

26. 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.

27. "[I]n order for an administrative search to be constitutional, the subject of the search must be afforded an opportunity to obtain precompliance

review before a neutral decisionmaker." *City of L.A. v. Patel*, 576 U.S. 409, 420 (2015).

28. The case law supports the rights of students to an expectation of privacy, even when they live in University supplied housing, since "courts are understandably reluctant to put the student who has the college as a landlord in a significantly different position than a student who lives off campus in a boarding house." *People v. Superior Court (Walker),* 143 Cal. App. 4th 1183, 1202, 49 Cal. Rptr. 3d 831, 845 (2006) (*quoting* 4 LaFave, Search and Seizure (4th ed. 2004) § 8.6(e), pp. 260–261).

29. Such actions are subject to challenge under the federal civil rights laws, since "[c]ourts have found campus police and other full-time employees of the university, such as head residents and directors of housing, to be state actors." Kristal O. Stanley, *The Fourth Amendment and Dormitory Searches: A New Truce,* 65 U. Chi. L. Rev. 1403, 1046 (1998) (collecting cases cases); *see also Morale v. Grigel*, 422 F. Supp. 988, 996 (D.N.H. 1976) (Resident Assistants are state actors).

30. Tenants do not lose their Fourth Amendment rights simply because the government is serving as their landlord. To hold otherwise would endanger the reasonable expectations of millions of Americans — college students in this case, but also residents of public housing projects. *See Pratt v. Chicago Hous. Auth.,* 848 F. Supp. 792 (N.D. Ill. 1994) (enjoining Chicago's warrantless searches of public housing residents).

31. Moreover, IU's use of the swipe data to track students' movements constitutes a violation of its own policies.

32. Indiana University policy UA-13 states that the ID Card exists "to verify their [students, employees, others] 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." 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."

33. The policy does not entitle the University to access, use, or release this swipe data, and the 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.

34. 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 breach of the contractual rights established by IU's own policies.

35. The use here of swipe data does not fit within the policy's explicit "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.

36. The Seventh Circuit has expressly held that University policies are part of the contract between a student and the university. *Ross v. Creighton Univ.*, 957 F.2d 410, 416 (7th Cir. 1992). *See Medlock v. Trustees of Indiana Univ.,* 738 F.3d 867, 872–73 (7th Cir. 2013) (considering policies in "The *A to Z Guide*—the university's student-housing handbook" as part of a § 1983 suit).

37. The tracking of Plaintiffs' movements violated this contractual obligation the University owed to its ID Card holders.

38. Indiana courts have likewise found that in the university context "the relationship between a student and an educational institution is contractual in nature." *Amaya v. Brater*, 981 N.E.2d 1235, 1240 (Ind. Ct. App. 2013) (quoting *Neel v. Indiana University Board of Trustees*, 435 N.E.2d 607, 610 (Ind. Ct. App. 1982)). While "Indiana courts have taken a very flexible approach to the scope of contractual promises between students and universities," *Id.*, courts hold that "it is generally accepted that a university's catalogues, bulletins, circulars, and regulations that are made available to its students become of part of this contract." *Chang v. Purdue Univ.,* 985 N.E.2d 35, 46 (Ind. Ct. App. 2013).

39. In violating Plaintiffs' contractual rights and invading their privacy, IU officials acted illegally, arbitrarily, capriciously, and in bad faith. *Amaya*, 981 N.E.2d at 1240.

COUNT I

The tracking of Plaintiffs' movements constitutes a violation of their Fourth Amendment and Fourteenth Amendment rights against unreasonable searches.

40. The allegations in the preceding paragraphs are incorporated herein by reference.

41. The Fourth Amendment has been incorporated against the State of Indiana via the Fourteenth Amendment. *Mapp v. Ohio*, 367 U.S. 643 (1961).

42. Defendants deprived Plaintiffs of their Fourth Amendment right against unreasonable searches by tracking their movements into and out of their homes using swipe data.

43. In depriving Plaintiffs of their Fourth Amendment right, Defendants, and their agents, were acting under color of state law.

44. Plaintiffs have a reasonable expectation of privacy that society is prepared to recognize as legitimate in their swipe data. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J. concurring).

45. Plaintiffs have a reasonable expectation of privacy that society is prepared to recognize as legitimate in their movements into, out of, and within their homes. *United States v. Karo*, 468 U.S. 705, 714–15 (1984).

46. Defendants do not have any substantial or exigent government interest that would justify the search in this case.

47. The University's policies are not narrowly tailored to the means least restrictive of Plaintiffs' privacy.

48. Plaintiffs are therefore entitled to declaratory and injunctive relief and nominal damages under 42 U.S.C. § 1983.

COUNT II

Defendants' use of student ID card's swipe data constitutes a violation of their Fourth Amendment and Fourteenth Amendment rights because it does not provide an opportunity for the student being searched to obtain precompliance review from a neutral third party.

49. The allegations in the preceding paragraphs are incorporated herein by reference.

50. Defendants deprived Plaintiffs of their Fourth Amendment right against unreasonable searches by retaining student ID card swipe data and continuing to access it without providing the subject of the search an opportunity to obtain precompliance review before a neutral decisionmaker. *Patel*, 576 U.S. at 420.

51. In depriving Plaintiffs of their Fourth Amendment right, Defendants, and their agents, were acting under color of state law.

52. Plaintiffs have a reasonable expectation of privacy that society is prepared to recognize as legitimate in their swipe data. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J. concurring).

53. Defendants do not have any substantial or exigent government interest that would justify the search without precompliance review before a neutral decision maker.

54. The University's policies are not narrowly tailored to the means least restrictive of Plaintiffs' privacy.

55. Plaintiffs are therefore entitled to declaratory and injunctive relief and nominal damages under 24 U.S.C. § 1983.

COUNT III

Defendants' tracking of Plaintiffs' movements constitutes a breach of the contract between Plaintiffs and the University.

56. The allegations in all preceding paragraphs are incorporated herein by reference.

57. The University's polices constitute a contract between the University and Plaintiffs. *Amaya v. Brater*, 981 N.E.2d 1235, 1240 (Ind. Ct. App. 2013).

58. The University's policies do not permit access to swipe data for purposes other than Identification.

59. The University's policies do not permit officials to track students' movements using swipe data.

60. The use of swipe data violated the enforceable contractual promise made to Plaintiffs' by the University.

61. In violating Plaintiffs contractual rights and invading their privacy, IU officials acted illegally, arbitrarily, capriciously, and in bad faith. *Amaya*, 981 N.E.2d at 1240.

62. In the alternative, the University's polices constituted a representation by the University upon which Plaintiffs reasonably relied to their detriment, and therefore the University is collaterally estopped from using swipe data to track Plaintiffs' movements.

PRAYER FOR RELIEF

Plaintiffs respectfully request that this Court:

a. Declare that the use of swipe data to track Plaintiffs' movements violated their Fourth Amendment right against unreasonable searches.

b. Declare that the use of swipe data to track Plaintiffs' movements without providing them an opportunity to obtain review by a neutral decisionmaker violated their Fourth Amendment right against unreasonable searches.

c. Declare that the use of swipe data to track Plaintiffs' movements violated the University's contractual obligations to Plaintiffs.

d. Enjoin the University from further use of swipe data in investigations except where the University has obtained a warrant or can demonstrate exigent circumstances.

e. Enjoin the University to expunge the investigation for which the University used swipe data of Plaintiffs from their permanent records, to the extent that Plaintiffs' records include information about such investigation;

f. Award Plaintiffs nominal damages of $1;

g. Award Plaintiffs their costs and attorney's fees under 42 U.S.C. § 1988.

h. Award any further relief to which Plaintiffs may be entitled.

Dated: October 29, 2020

Respectfully Submitted,

By: /s/ Anita Y. Milanovich

Jeffrey M. Schwab*
Daniel R. Suhr*
Reilly Stephens*
Liberty Justice Center
190 South LaSalle Street, Suite 1500
Chicago, Illinois 60603
Telephone (312) 263-7668
Facsimile (312) 263-7702
jschwab@libertyjusticecenter.org

*pro hac vice motions to be filed

Anita Y. Milanovich
Milanovich Law, PLLC
100 E Broadway Street
The Berkeley Room
Butte, MT 59701
Telephone: 406-589-6856
aymilanovich@milanovichlaw.com

Attorneys for Plaintiffs