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-02801-JMS-MJD **Opposition to Defendants' Motion to Dismiss**

Plaintiffs, Tyler Cameron Gutterman, Dale Nelson, Hunter Johnson, and Brian Hiltunen, submit their opposition to Defendant's Motion to Dismiss (Dkt. 19). Plaintiffs are students at Indiana University, Bloomington (the "University" or "IU"), who were subject to unlawful surveillance of their movements via IU's tracking of their student ID cards. They allege that this tracking violated both their Fourth Amendment rights and the contract established between them and the University. Defendants filed a Motion to Dismiss arguing that 1) they are entitled to sovereign immunity, 2) the tracking of the ID cards was not a Fourth Amendment violation, and 3) there was no breach of contract. For the reasons stated *infra*, this court should deny the Motion.

FACTUAL BACKGROUND

Plaintiffs are undergraduate students at Indiana University, Bloomington. Complaint, Dkt. 1 at ¶ 11. As a condition of their attendance at the University, Plaintiffs are required to carry an official, University-mandated Student ID Card, known as a "CrimsonCard," which facilitates their access to university services. *Id.* at ¶ 15-16. These ID cards track every time the student "swipes" the card at any of the many points where Plaintiffs are required to use it. 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. *Id.* at ¶ 23. This swipe data even tracks students off campus, including purchases at local restaurants and businesses that allow purchases using a student account. *Id.* at 24. The university maintains records of this swipe data, which it uses as part of official investigations. *Id.* at ¶¶ 16, 18. The University allows access to this data to "all eligible employees and designated appointees of the university for all legitimate university purposes." *Id.* at ¶ 25 (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.") Comp. at ¶¶ 12-13. During this Fall 2018 semester, the University investigated the fraternity regarding an alleged hazing incident. *Id.* at 18. 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. *Id.* at ¶¶ 18-19. In particular, the swipe data was used to track Plaintiffs' movements into and out of their dorms. *Id.* at ¶ 1. There was never any allegation the Plaintiffs sponsored or organized the alleged hazing; indeed, they were pledges to the fraternity at the time.

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." *Id.* at ¶ 32. Nothing in the CrimsonCard Terms and Conditions or the University's Policy Manual permits using the data to track students. *Id* at ¶ 34; *see also* Defendant's Exhibit A (CrimsonCard Terms and Conditions) (Dkt. 20-1), Exhibit B (ID Card Policy) (Dkt. 20-2), and Exhibit C (Data Policy) (Dkt. 20-3).

Plaintiffs therefore brought this case remedy the violations of their rights. Counts I and II of the Complaint allege violations of Plaintiffs' Fourth Amendment Rights. *Id.* at ¶¶ 40-55. 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. *Id.* at ¶¶ 56-62. The Defendants filed a Motion to Dismiss, along with an attached Memorandum. *See* Dkt. 20 ("Memo").

LEGAL STANDARD

To survive this Motion to Dismiss, Plaintiffs need only state in their Complaint "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 *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). They should prevail provided their Complaint demonstrates something "more than a sheer possibility that a defendant has acted unlawfully." *Iqbal*, 556 U.S. at 678.

ARGUMENT

I. Indiana University employees are subject to Section 1983 suits for violations of constitutional rights.

Defendants first argue that they enjoy state sovereign immunity, and therefore cannot be subjected to suit. But as the Seventh Circuit found, in a case upon which Defendants otherwise rely, "Indiana University is a public university, owned by the State of Indiana, and the student inspectors and university police are university employees and therefore state actors . . . [a]nd so they can be sued under section 1983 for violating the Fourth Amendment." *Medlock v. Trs. of Ind. Univ.*, 738 F.3d 867, 871 (7th Cir. 2013).

Even Defendants admit that claims for prospective relief—the majority of requested relief in the Complaint—are not subject to the protection of sovereign immunity, therefore there is no basis to dismiss Plaintiffs' claims on sovereign immunity grounds. *Kashani v. Purdue Univ.*, 813 F.2d 843, 848 (7th Cir. 1987) . President McRobbie is sued in his official capacity as president of the University. As such, under *Ex Parte Young,* 209 U.S. 123 (1908), he can be subject to the prospective relief Plaintiffs request. *See Colburn v. Trs. of Ind. Univ.*, 739 F. Supp. 1268, 1281 (S.D. Ind. 1990); *Shannon v. Bepko*, 684 F. Supp. 1465, 1475 (S.D. Ind. 1988). Plaintiffs' Complaint asks for declaratory and injunctive relief for the violation. There is no basis to dismiss these claims on sovereign immunity grounds, as Defendants concede. Memo at 7 (sovereign immunity "only prohibits 'action[s] for damages against [President McRobbie] in [his] official capacity.'" (quoting *Parsons v. Bourff*, 739 F. Supp. 1266 (S.D. Ind. 1989)).

Nor does sovereign immunity prevent this court from redressing Plaintiffs' breach-of-contract claim. As with the Fourth Amendment claims, *Ex Parte Young* allows for prospective relief on a breach of contract against university officials in their official capacity. *See Lassiter v. Ala. A & M Univ.*, 3 F.3d 1482, 1485 (11th Cir. 1993) ("the district court properly granted judgment for the defendants on Lassiter's breach of contract claim, with the exception of any claim Lassiter may have for prospective relief against Covington in his official capacity"). Even in one of the cases upon which Defendants otherwise rely, this Court went on to address the state-law breach-of-contract claim after resolving other claims on immunity grounds. *See Bissessur v.*

Ind. Univ. Bd. of Trs., No. 1:07-cv-1290-SEB-WTL, 2008 U.S. Dist. LEXIS 69299, at *28 (S.D. Ind. Sep. 10, 2008); *see also Turner v. Vincennes Univ.*, No. 3:17-cv-00044-RLY-MPB, 2019 U.S. Dist. LEXIS 229395 (S.D. Ind. Mar. 29, 2019); *Tyler v. Trs. of Purdue Univ.*, 834 F. Supp. 2d 830, 846 (N.D. Ind. 2011). Therefore, this court should reject Defendants' sovereign immunity argument and rule on the merits of Plaintiffs' breach-of-contract claim.

II. Plaintiffs have stated a viable claim 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)).

It is precisely the special protection for the home that this case implicates. Plaintiffs' 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 Plaintiffs' conduct (to see if it could convict them of the administrative equivalent of perjury), in violation of the Fourth Amendment.

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

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*, 217 Pa. Super. 432, 435, 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.

It is true, as Defendants suggest, Memo. at 18, that courts have sometimes viewed routine inspections by Resident Assistants for cleanliness and safety either as administrative searchers 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.

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, not RA's.

Defendants' argument treats the investigation in this case as equivalent to this sort of standard room inspection by an RA. For this, they cite to a decision of this court, *Medlock v. Trs. of Ind. Univ.*, No. 1:11-cv-00977-TWP-DKL, 2011 U.S. Dist.

LEXIS 103793, at *15 (S.D. Ind. Sep. 13, 2011), ultimately upheld by the Court of Appeals. *Medlock v. Trs. of Ind. Univ.*, 738 F.3d 867 (7th Cir. 2013). In that case, the Seventh Circuit rejected the premise that an RA inspection doesn't involve state action. *Medlock,* 738 F.3d at 871; *See also Morale v. Grigel*, 422 F. Supp. 988, 996 (D.N.H. 1976) (RA's are state actors). However, because it was a routine room inspection, the Court of Appeals found that it didn't violate the Fourth Amendment. *Medlock,* 738 F.3d at 872. This case is not comparable to *Medlock* because this was not a routine health-and-safety inspection, for at least three reasons:

1) The search of Plaintiffs here 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 Plaintiffs' 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 Plaintiffs were found innocent of any wrongdoing, sanctions were handed out to Beta—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) (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.*

[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

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 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

[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)."

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 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 Plaintiffs' 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.

Defendants also attempt to argue that Plaintiffs, by virtue of living in university housing, consented to this sort of tracking. 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*, 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).

Moreover, 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). Defendants argue that *Patel* doesn't apply because the search was of the hotel operator's records, rather than of the hotel guests themselves. But that is simply because the hotel operators in *Patel* were the subjects of the search, rather than third-

party guests. Here, Plaintiffs were the subject of the search, and as subjects of the search they were entitled to review.

B. Tracking Plaintiffs' movements 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 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.

Defendants attempt to analogize the intrusion here to older cases involving tracking of someone's movements in public. *See United States v. Knotts*, 460 U.S. 276 (1983). This analogy fails for two reasons. First, the information searched here reveals facts about the interior of the home, 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.

Defendants argue that this court should apply the "third party" doctrine of *Smith v. Maryland*, 442 U.S. 735, 737 (1979), where the government obtained pen register information in order to track down a stalker making threatening phone calls to his victim. Memo at 15. The pen register recorded incoming and outgoing phone numbers, and therefore allowed the state to identify particular pay phones from which the calls were made, apprehending the defendant. The court reasoned that since the defendant had provided the phone number in question to the phone company, he willing revealed all the relevant information to a third party and could no longer claim a reasonable expectation of privacy. *Id.* at 742.

This Court should join the Supreme Court in *Carpenter* in declining to apply the "third party" doctrine to modern technologies. The doctrine—developed in analog era for limited sorts of information such as phone numbers is a poor fit for the digital age. *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring). Even before *Carpenter,* the Supreme Court had previously recognized that the traditionally broad 'search incident to arrest' exemption should not be extended to the search of an arrestee's cell

phone, because just as GPS tracking could provide more information than an old-fashioned tail, a person's cell phone now contains far more personal information than the purses and wallets of prior Fourth Amendment cases. *Riley v. California*, 134 S. Ct. 2473, 2489 (2014). *Carpenter* declined to overrule *Smith*, but also declined to extend it to modern technology. 138 S. Ct. at 2219.

Defendants argue that the swipe data is unlike *Carpenter,* since it simply provides a "single data point for each 'swipe' or access to a student's residence hall or dorm room." Memo at 15. But by that reasoning the cell phone in *Carpenter* likewise only provided a set of single datapoints: each cell tower Mr. Carpenter's phone connected to. The swipe data tracks Plaintiffs 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 received 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 or even years 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.

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 diseases; 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 Court should therefore find that this sort of tracking violates Plaintiffs' 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.

III. The University has breached its contract with the Plaintiffs.

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 also Medlock,* 738 F.3d at 872–73 (considering policies in "The *A to Z Guide*—the university's student-housing handbook" as part of a § 1983 suit). 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).

Defendants respond to Plaintiffs' breach-of-contract claims with a series of arguments that will be taken in turn: first standing, and then several more focused on the merits.

A. The Plaintiffs have standing to assert the breach of the contract.

First, Defendants argue that, since they were not suspended or expelled (rather, they were vindicated) as a result of the investigation, the breach resulted in no cognizable injury, and therefore they lack standing. Memo at 21. But there were several different ways this breach injured Plaintiffs.

First, privacy violations are an inherent injury—if one learned that a secret camera had been placed in one's home, it wouldn't be a great comfort to learn that camera happened not to photograph anything criminal. *In re Facebook, Inc.*, 402 F. Supp. 3d 767, 777 (N.D. Cal. 2019) ("the law has long recognized that a privacy invasion is itself the kind of injury that can be redressed in federal court, even if the invasion does not lead to some secondary economic injury like identity theft."); *id.* at 802 (under California law, nominal damages are available for breach of contract when the breach is an invasion of privacy). Second, the continued retention of swipe data without appropriate safeguards represents an *ongoing injury* which is both cognizable and capable of this Court's redress. Third, Plaintiffs were injured by being subjected to an illegal process, part of an official investigation which is represented

in their academic records. Plaintiffs plead redress of this injury in their Complaint. *See* Comp. Prayer for Relief ¶ e ("Enjoin the University to expunge the investigation for which the University used swipe data of Plaintiffs from their permanent records"). Fourth, the breach injured Plaintiffs by violating their Fourth Amendment rights, for the reasons discussed *supra.* Fifth and finally, while Plaintiffs were not personally expelled or suspended, the fraternity, which they are still members of, *was* subject to sanction. Memo at 4. Those sanctions represent an injury to Plaintiffs, who otherwise would have enjoyed benefits of membership unencumbered by University sanction.

B. Plaintiffs' breach of contract claim should succeed on the merits.

On the merits, Defendants do not dispute the existence of a contractual relationship with Plaintiffs. Memo at 24. Instead, they make three arguments: that there was no breach, that there were no damages, and that the decision in *Amaya v. Brater,* 981 N.E.2d 125 (Ind. Ct. App. 2013) is not relevant.

1. IU breached its contract with Plaintiffs.

Defendants argue that "IU owns all CrimsonCards, and as such, owns the data they generate." Memo at 25. However, the fact that a contracting party has title to something covered by a contract simply means that they take ownership of the property *subject to the terms of the contract*—the formal "ownership" arrangement simply brings the analysis back around to the contract's terms.

Defendants' make much of the portion of the data policy that allows access "for all legitimate university purposes." *Id.* But this open-ended grant is not the only term of the agreement—rather, the agreement specifically outlines what "legitimate

university purposes" the cards are to be used for. Indiana University policy UA-13 states that the ID Card exists "to verify their [students, employees, 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."

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. Verification, validation, and authentication are all contemporaneous needs to permit access to a building—to "swipe in" in modern parlance. There is, of course, no question that Plaintiffs are and were who they say they are, and that Plaintiffs accessed University buildings they were entitled to enter using their ID Card. The use of this information to investigate Plaintiffs was therefore a breach of the contractual rights established by IU's own policies.

Nor does the use here of swipe data fit within the policy's "safety and security exception." That exception is strictly limited to "[i]dentification information collected for production" of the card; it says nothing about ongoing access to students'

individual, personal movements on campus. If anything, the fact that the contract includes a "safety and security exception" specific to a different circumstance shows that the contract does not cover this circumstance.

Defendants' final argument is that they have no duty to actually protect Plaintiffs' data—essentially, that the contract makes no promise of privacy. But this is not the law: "[a] contract between a private institution and a student confers duties upon both parties which cannot be arbitrarily disregarded and may be judicially enforced." *Ross,* 957 F.2d at 416 (quoting *DeMarco v. University of Health Sciences*, 40 Ill. App. 3d 474, 352 N.E.2d 361-62 (Ill. App. Ct. 1976)). In any case, the university's policy *does* lay out explicit things that "[u]sers of institional data" "must" and "must not" do—they "must" "respect the confidentiality and privacy of individuals," "must" "observe any ethical restrictions that apply to the data," and "must" "abide by applicable laws, regulations, standards, and policies," Defendants' Exhibit 3, Dkt. 20-3 at 4, and the policy specifically contemplates sanctions for misuses, *id.* at 6. The premise that there is no duty to follow their own rules is inconsistent with the rules as written.

2. IU's breach damaged Plaintiffs.

Defendants next argue that damages are an element of breach of contract, and Plaintiffs can show no damages. This is essentially the standing argument addressed above in a different form, and as explained above there are many ways in which the breach in this case damaged plaintiffs, including violating their constitutional rights, infringing their privacy, sanctioning an organization of which they were members,

and the ongoing injury as the University still retains their data. Plaintiffs concede that these sorts of injuries lead to damages that are difficult to calculate in the abstract, which is why they plead relief of nominal damages in their Complaint. *See* Comp. ¶ f. Nominal damages are the appropriate remedy where there is a breach of rights that is provable, but assigning an exact value to them is difficult or impossible. *See, e.g. Memphis Community Sch. Dist. v. Stachura*, 477 U.S. 299, 308 n.11 (1986). And Plaintiffs have also plead prospective relief, which is likewise an appropriate remedy for the breach of a contract.

3. Amaya establishes that there is a contractual relationship, but is otherwise distinguishable.

Finally, Defendants argue that the Indiana decision *Amaya v. Brater*, 981 N.E.2d 1235 (Ind. Ct. App. 2013), is distinguishable. Memo at 28. Plaintiffs agree.

Plaintiffs cited *Amaya* in their Complaint because it is the leading Indiana case for the proposition that University polices establish a contract between the institution and students. Comp. ¶¶ 38, 57, 61. Plaintiffs also plead that the University officials conduct was sufficient to meet *Amaya* standard of acting "illegally, arbitrarily, capriciously, and in bad faith." *Id.* at ¶ 39 (citing *Amaya*, 981 N.E.2d at 1240). However, Plaintiffs do not believe this standard is the most appropriate for this case because, as Defendants argue, this is a different circumstance.

Amaya involved a dismissal for academic misconduct (cheating on an exam). The Plaintiff challenged her expulsion, and the Court found that, yes, a contract existed between the student and the university, but in the context of *academic decisions* universities were entitled to deference as to their *academic judgment*: "The

university requires that the student's academic performance be satisfactory to the university in its honest judgment. Absent a showing of bad faith on the part of the university or a professor, the court will not interfere." *Amaya*, 981 N.E.2d at 1240 (quoting *Neel v. Indiana University Board of Trustees*, 435 N.E.2d 607, 610 (Ind. Ct. App. 1982)). In *Ross*, the Seventh Circuit likewise quotes the Indiana Court of Appeals in *DeMarco* for this proposition: "a decision of the school authorities relating to the academic qualification of the students will not be reviewed. Courts are not qualified to pass an opinion as to the attainments of a student and courts will not review a decision of the school authorities relating to academic qualifications of the students." 957 F.2d at 416 (Cleaned Up).

Therefore, the deference some student-university breach-of-contract cases provide universities is premised upon the special expertise universities have as to the setting of academic standards—courts will generally not second-guess whether a standard is an appropriate requirement for someone to get a degree in engineering, or become a medical doctor. That deference is inappropriate where, as here, the contractual relation, and the challenged conduct, implicates no special expertise the university has over the courts. Rather, this context—investigations into potentially criminal off-campus conduct—is, if anything, an area in which court have *more* expertise than universities. Requiring the sort of bad faith *Amaya* contemplates would therefore be inappropriate when ruling on Plaintiffs' breach-of-contract claim.

CONCLUSION

For the reasons stated above, the Motion to Dismiss should be denied.

Dated: March 9, 2021

Respectfully Submitted,

By: /s/ Reilly Stephens

Reilly Stephens*
Jeffrey M. Schwab*
Daniel R. Suhr*
Liberty Justice Center
208 South LaSalle Street, Suite 1690
Chicago, Illinois 60604
Telephone 312-637-2280
Facsimile (312) 263-7702
rstephens@libertyjusticecenter.org

*pro hac vice