No. 2024AP469-CR

STATE OF WISCONSIN
SUPREME COURT OF WISCONSIN

STATE OF WISCONSIN,
Plaintiff-Respondent,

vs.

ANDREAS W. RAUCH SHARAK,
Defendant-Appellant.

On Certification
Appeal from the Circuit Court for Jefferson County
The Honorable Judge William F. Hue Presiding
Case No. 2022CF495

REPLY BRIEF OF DEFENDANT-APPELLANT

BRADLEY W. NOVRESKE
State Bar No. 1106967

Attorney for Defendant-Appellant

NOVRESKE LAW OFFICE, LLC
13422 W. Prospect Pl.
New Berlin, WI 53151
(414) 502-7558
brad@novreskelaw.com

ARGUMENT

A. Even if Mr. Rauch Sharak's use of Google's services created a bailment of his electronic data and communications (though it doesn't), this would not negate his Fourth Amendment rights grounded in *Katz*.

The State argues that an individual's use of an ESP's services to upload, store, or transmit electronic data and communications creates a bailment of that electronic data and communications between the user and the ESP such that the terms of service become the "private contract" that delimits Fourth Amendment expectations of privacy for those electronic data and communications. No court has analyzed an individual's expectations of privacy in electronic data and communications as a bailment. The only authority supporting this approach is a suggestion in the dissent of Justice Gorsuch in *Carpenter v. United States*, 585 U.S. 296, 400 (2018). This suggestion is squarely at odds with the holding of *Carpenter* itself and would require this Court to ignore the United States Supreme Court's holding in *Katz v. United States*, 389 U.S. 347 (1967) and its progeny (including *Carpenter*).

As recognized in *Carpenter*, the scope of an individual's Fourth Amendment rights are delineated by two lines of cases, *Katz* and *United States v. Jones*, 565 U.S. 400 (2012). Under *Jones*, Fourth Amendment search doctrine focuses on whether the government "obtains information by physically intruding on a constitutionally protected area," and follows the common-law focus on property law and trespass. *Jones*, 565 U.S. at 405. However, the United States Supreme Court has recognized that "property rights are not the sole measure of Fourth Amendment violations." *Soldal v. Cook County*, 506 U.S. 56, 64 (1992). *Katz* held that the Fourth Amendment also protects certain expectations of privacy – when an individual "seeks to preserve something as private," and where his expectation of privacy is "one that society is prepared to recognize as reasonable." *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

In *Carpenter*, the Supreme Court reiterated this dual approach to determining the scope of the Fourth Amendment: "Although no single rubric

definitively resolves which expectations of privacy are entitled to protection, the analysis is informed by historical understandings of what was deemed an unreasonable search and seizure when the Fourth Amendment was adopted." *Carpenter*, 585 U.S. at 304-05 (cleaned up). These cases recognized that the Fourth Amendment "seeks to secure the privacies of life against arbitrary power," *Boyd v. United States*, 116 U.S. 616, 630 (1886), and that a central aim of the Framers was "to place obstacles in the way of a too permeating police surveillance." *United States v. Di Re*, 332 U.S. 581, 595 (1948). Critically, in *Carpenter*, the U.S. Supreme Court reiterated that the Court's approach to Fourth Amendment jurisprudence when addressing advancements in technology that create significant new privacy concerns is to "assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.* at 305 (citation omitted).

Carpenter is important in rebutting the State's assertion that a theory of bailment defeats Mr. Rauch Sharak's claim to the protections of the Fourth Amendment for his electronic data and communications over Google's platform. *Carpenter* itself rejected Justice Gorsuch's position – which elevated rigid concepts of property law above all else and rejected *Katz* and its progeny as a separate source of Fourth Amendment protections – and went so far as to carve out a new rule extending protections to an area that was not adequately protected by existing rules. Whether Mr. Rauch Sharak has a property interest in his electronic data and communications on Google's platform and whether that privacy interest can best be described as a bailment does not impact the analysis of whether he has a subjective expectation of privacy in them and that this expectation is one that society is prepared to recognize as reasonable. In this case, Mr. Rauch Sharak has such an interest. It is an interest shared by the vast majority of society. That is no less the case simply because the issue does not fit neatly within existing 4th Amendment doctrine, much of which developed prior to the invention of the internet and smart devices.

B. The United States Supreme Court emphasized that Fourth Amendment jurisprudence must evolve with significant advances in technology and repeatedly created new rules where existing precedent was inadequate. This Court should take the lead.

In *Carpenter*, the U.S. Supreme Court recognized that Fourth Amendment principles must be re-evaluated as technological advances present surveillance scenarios that would have been unfathomable to the Framers so as to not leave the public "at the mercy of advancing technology." *Carpenter*, 585 U.S. at 305 (quoting *Kyllo v. United States*, 533 U.S. 27, 35 (2001). New rules "must take account of more sophisticated systems that are already in use or in development." *Kyllo*, 533 U.S. at 36. The pace of technological advancement, especially in the realm of data collection and telemetry from smart devices, has only accelerated in the 11 years since *Riley* and 7 years since *Carpenter* were decided. The State's advocated position leaves the public at the mercy of advancing technology to a greater extent than was the case in *Riley* and *Carpenter*.

In *Carpenter*, as in *Riley v. California*, 573 U.S. 373 (2014), the U.S. Supreme Court acknowledged that the then-existing Fourth Amendment precedent was insufficient to handle the unprecedented privacy concerns presented by smartphones and crafted new rules instead of clinging to the old. In *Riley*, the U.S. Supreme Court held that police must obtain a warrant before searching the contents of a cell phone given the "immense storage capacity" of modern cell phones and the increasingly ubiquitous nature of smartphones which the Court referred to as a "feature of human anatomy." *Id*. at 385. And in *Carpenter*, the U.S. Supreme Court rejected the application of the third-party doctrine of *Smith v. Maryland*, 442 U.S. 735 (1979) and *United States v. Miller*, 425 U.S. 435 (1976) and held that a warrant was required for the government to obtain cell-site location information (CSLI) from a suspect's cellular service provider. The *Carpenter* court explicitly recognized that CSLI was technically "business records" created and maintained by wireless carriers

but that the records contained such an "exhaustive chronicle of [the user's] location information" that it is categorically different than what would traditionally be thought of as business records.

Perhaps the biggest advancement since the *Riley* was decided is the shift away from local file storage on smartphones, laptops, and PCs to a hybrid model whereby the overwhelming majority of the user's data is uploaded and stored on the Cloud in addition to the user's hard drive by default. Cloud storage refers to warehousing digital files on servers managed by a third party over the internet. In a purely Cloud-based system, a user's files are saved only to the Cloud, accessed from the Cloud through the user's own device, files are downloaded into temporary local storage on the device as they are needed from the Cloud, and changes are then uploaded back to the Cloud. The user's device never contains the complete contents of their data stored on the Cloud.

In the more typical hybrid situation, specific directories on a user's device are backed up to the Cloud so that any changes made to a file on the Cloud are also made to the local copy of the file on the user's device, and changes made to the copy of the user's device are also changed on the version stored in the Cloud. The hybrid Cloud scenario is the most prevalent on modern devices. It is often a prerequisite to using these devices or the default setting.

For example, installations of Windows now use a Microsoft OneDrive account as the default location to save the user's files, housing the Documents, Photos, Videos, and default auto-save folder for Microsoft Office and other applications. Apple devices sync to Apple's iCloud Drive and iCloud Photos. Google and Android-based devices sync to Google Drive and Google Photos. Other common hybrid programs include Dropbox, Jottacloud, Box, and Proton Drive. The *Riley* court extended protections not afforded by existing precedent to cover the search of cell phones because those cell phones contained a hoard of private personal information detailing the day-to-day existence of the owner which made them categorically different than searching a physical "container." Now, the entire contents of one's smartphone are typically backed up to the

Cloud and stored on servers maintained by an ESP, no longer limited to the physical storage on the phone.

Given that we know that the vast majority of ESPs rely on automated hashing and scanning of every file uploaded or transmitted by users, the shift towards hybrid Cloud storage means that ESPs are able to search every file of every user, functionally searching the entirety of the contents of that user's device. If, as the State argues, the private search doctrine applies, police would be permitted to likewise scan and hash every file of every user of the ESP's service to the extent that the ESP has already done so because the reasonable expectation of privacy in those files would have been extinguished by the ESP's search (as long as law enforcement doesn't broaden the scope of that search).

In *Gasper*, the defendant argued that his expectation of privacy was derived from his use of a cell phone to access Snapchat and that the special protections afforded cell phones should extend to the internet-based actions of that user using a cell phone. The focus should not be on the particular device used to access the service but rather that the rationale used to extend protections to the contents of a user's cell phone are indistinguishable from the rationale that Rauch Sharak advocates for the expansion of *Riley* and *Carpenter* to cover data and communications (not otherwise posted publicly) that are uploaded to, transmitted through, or synced to the ESP's platform or Cloud service. The amount of data that would lose the protections of the Fourth Amendment is far greater than the data at issue in both *Riley* and *Carpenter*, and in both cases the U.S. Supreme Court recognized that existing Fourth Amendment precedent could not provide adequate protections. So too in this case, and to the extent existing precedent cannot adequately protect user data this Court should follow the U.S. Supreme Court's directive to craft a new rule that can.

C. The distinction between government and private actors is increasingly illusory in the realm of surveillance through data aggregation and telemetry highlighting the extreme risk to the public of unchecked ubiquitous government surveillance impossible to imagine by the Framers.

It is impossible to overstate the importance of the issues in this case and the extent to which the government has shifted towards outsourcing surveillance to private entities. This is particularly true with the landscape-changing integration of AI into nearly every facet of digital life, nearly all of which occurred in the years following *Carpenter*. This topic alone is worthy of independent briefing, as it sets the stage for the privacy battles to come in the next few years.

The distinction between private technology companies and government is rapidly fading. For example, this month executives from Meta (Facebook), OpenAI (ChatGPT) and Palantir were inducted into the Army Reserve and given the rank of lieutenant colonel to serve in a new "Executive Innovation Corps" called Detachment 201.[1] And it was recently announced that United States Immigration and Customs Enforcement is paying Palantir $30 million to build a tool that allows "near real-time visibility into instances of self-deportation."[2] Most recently, on June 24, 2025, U.S. Health Secretary Robert F. Kennedy Jr. revealed that DHHS plans to push for every American to adopt wearable devices that track health telemetry.[3] These efforts are in addition to the extensive use by local and federal law enforcement of commercially available intelligence. The breadth of data collected by ESPs through smart devices includes conversations and correspondence, second-by-second biometric data, location data, menstrual cycle tracking, proximity to other smart devices that can then be cross-referenced and de-anonymized to establish who the user is physically near at any given date and time, sleep data, deviations from daily rituals based on pattern recognition of long-term

[1] U.S. Army Public Affairs, accessed 6/25/2025, available at https://www.army.mil/article/286317/army_launches_detachment_201_executive_innovation_corps_to_drive_tech_transformation

[2] Department of Homeland Security Contract Justification ICM_70CTD022FR0000170-P00006, available at https://sam.gov/opp/f71acee6010c423db4902446a59a690c/view

[3] "US Health Secretary Kennedy says HHS to launch campaign to encourage wearable devices." Reuters. Accessed 6/25/2025, available at https://www.reuters.com/business/healthcare-pharmaceuticals/us-health-secretary-kennedy-says-hhs-launch-campaign-encourage-wearable-devices-2025-06-24/

data trends, and virtually every detail of the user's day to day existence over the course of years or even decades (the first iPhone was released in 2007).

All of this data is collected, aggregated cross-platform, and held by ESPs, almost always consistent with their Terms (which are adhesion contracts by definition) that users must agree to in order to utilize the ESP's platform. According to the State, all of this data is subject to search by the ESP and disclosure at the ESP's whim to the government without a warrant and without recourse for the individual user. Such a result was unacceptable to the United States Supreme Court in *Riley* and *Carpenter* and new rules were crafted to ensure that the Fourth Amendment's protections remained robust in the face of ever-increasing government surveillance capabilities. This case demands the same.

D. The trial court's finding of facts as related to the history, motivation behind, and impact on ESP behaviors of the several identified statutes was not an act of statutory interpretation and is reviewed only for clear error.

The State argues that the trial court's findings as related to the Protect Our Children Act, Section 230, FOSTA, and amendments to the TVPA should be reviewed de novo as statutory interpretation. The trial court's conclusions were findings of adjudicative fact. Mr. Rauch Sharak raised factual assertions about the history and motivation of the legislature in passing or amending the various statutes, the impact of the interaction between these sometimes overlapping statutes on ESPs regardless of the legislative intent or actual meaning of the statutes, and the ways in which the cumulative impact of these statutes compelled ESPs to engage in the type of active affirmative moderation that they were unwilling to do prior. Nothing about the historical factual inquiry into the creation and amendment of the federal statutes at issue required or relied upon statutory interpretation. And it relied on the type of real-world, factual analysis that this Court has treated as an exercise of judicial factfinding in other contexts that inherently involve the application of law to facts.

The best examples come from the *Franks/Mann* context in which a trial court's determination as to whether omitted facts are "material" to the finding of probable cause is treated by appellate courts as a question of fact despite being an application of law to facts which would traditionally be subject to de novo review. *Franks v. Delaware*, 438 U.S. 154 (1978); *State v. Mann*, 123 Wis. 2d 375, 367 N.W.2d 209 (1985). Another example is a trial court's determination as to whether a prospective juror is or is not objectively biased despite it being a mixed question of law and fact. *State v. Faucher*, 227 Wis.2d 700, 596 N.W.2d 770 (1999).

In each of these contexts, what appears to be a legal conclusion is treated as a factual finding for purposes of the standard of appellate review because the determination is so closely intertwined with factual findings that the trial court is deemed to be in a better position than the Court of Appeals to make the determination. The same is true in this case as it relates to the factual findings regarding historical facts surrounding the passage and amendment of the federal statutes. As such, these factual findings are reviewed only for clear error.

CONCLUSION

For the reasons stated, Mr. Rauch Sharak requests that this Court reverse the trial court and order the suppression of the contents of his Google account and any evidence derived therefrom.

Dated at New Berlin, Wisconsin this 26th day of June, 2025.

NOVRESKE LAW OFFICE, LLC

Electronically signed by
BRADLEY W. NOVRESKE
State Bar No. 1106967

13422 W. Prospect Pl.
New Berlin, WI 53151
(414) 502-7558
brad@novreskelaw.com

CERTIFICATE OF COMPLIANCE

I hereby certify that this reply brief conforms to the rules contained in Wis. Stat. § 809.19(8)(b), (bm) and (c) for a reply brief. The length of this brief is 2680 words as calculated by Microsoft Word's word count feature.

Dated at New Berlin, Wisconsin this 26th day of June, 2025.

Electronically signed by
BRADLEY W. NOVRESKE
State Bar No. 1106967