

Police surveillance of cell phone location data: Supreme Court versus public opinion

Emma W. Marshall¹ | Jennifer L. Groscup² | Eve M. Brank¹ |
Analay Perez¹ | Lori A. Hoetger³

¹University of Nebraska, Lincoln, NE, USA

²Scripps College, Claremont, CA, USA

³Douglas County Public Defender, Omaha, NE, USA

Correspondence

Emma W. Marshall, Department of Psychology,
University of Nebraska-Lincoln, P.O. Box
880308, Lincoln, NE 68588-0308, USA
Email: emma.marshall@huskers.unl.edu

The Fourth Amendment to the US Constitution protects individuals from unreasonable searches and seizures. As technology evolves, courts must examine Fourth Amendment concerns implicated by the introduction of new and enhanced police surveillance techniques. Recent Supreme Court cases have demonstrated a trend towards reconsidering the mechanical application of traditional Fourth Amendment doctrine to define the scope of constitutional protections for modern technological devices and personal data. The current research examined whether public opinion regarding privacy rights in electronic communications is in accordance with these Supreme Court rulings. Results suggest that cell phone location data is perceived as more private and deserving of protections than other types of location data, but the privacy of other types of information recorded on cell phones is valued even more than location data. These results have implications for the police and courts considering how the Fourth Amendment will apply to smart phone technologies.

1 | INTRODUCTION

Almost all Americans (96%) have a cell phone, and most have smart phones (86%; Pew Research Center, 2019). Referring to these devices simply as “phones” is an obvious misnomer because they are frequently used to record pictures and videos; save files to Cloud storage; wirelessly sync with computers; make payments; and provide hours of entertainment through social media, books, movies, and games (Riley v. California, 2014). For a growing number of Americans (approximately 20%), the smart phone is the only way they access the internet at home (Pew Research Center, 2019). With the modern luxury of smart phones comes potential for extensive and easy police surveillance. It takes minimal effort and little time to aggregate small slivers of information from phones and other sources to

develop a vivid picture of a person's day-to-day life (Kerr, 2012), collapsing all aspects of a person's life into one aggregation (DeZwart, Humphreys, & Van Dissel, 2014). How do we balance our civil liberties with national security when the police are collecting this information? The current research provides information that may be helpful in answering this question by comparing how individuals respond to searches of electronic devices and remote searches of data stored with third-parties. In addition, we examine recent US Supreme Court assumptions that individuals view searches of cell phone location data as uniquely intrusive.

1.1 | The Fourth Amendment, searches, and privacy

The Fourth Amendment of the United States Constitution protects US citizens from *unreasonable* searches and seizures by government actors. According to the US Supreme Court, the Fourth Amendment's "overriding function" is to "protect personal privacy and dignity against *unwarranted intrusion* by the State" (*Schmerber v. California*, 1966, p. 384, emphasis added). Thus, not all government intrusions are sufficiently "arbitrary" or "invasive" to trigger Fourth Amendment protections (*Skinner v. Ry. Labor Execs. 'Ass'n*, 1989, pp. 613–614). The scope of constitutional protection is limited to circumstances in which there has been a seizure or a search. A search occurs when the government infringes upon "an expectation of privacy that society is prepared to consider reasonable" (*United States v. Jacobsen*, 1984, p. 113). Yet, defining this phrase takes us on a winding jurisprudential trail through objective and subjective determinations that are difficult to pin down.

When the Constitution was originally drafted, the country was largely an agrarian society concerned with the threat of soldiers trespassing onto private property, and communication generally required face-to-face interaction. Accordingly, early understandings of the Fourth Amendment did not focus on the privacy of communications or information. Although the origins of the US Postal Service date back to pre-colonial times, it was not until the late 19th century that the Supreme Court expanded its definition of a search to require a warrant for the government to search the contents of a sealed letter sent through the mail (see *Ex Parte Jackson*, 1877). As time went on, technological progress continually complicated what it means to be secure in our *persons, houses, papers, and effects*. As a result, the focus of Fourth Amendment analysis shifted from colonists' fears of British intrusions on their lands and into their homes to less physical intrusions (Taslitz, 2006).

The tangible picture of bayonet-carrying police searching through homes began fading in earnest in the early part of the twentieth century, when the US Supreme Court considered the nebulous concept of electronic surveillance of the telephone. In *Olmstead v. United States* (1928), the defendant was suspected of bootlegging during the Prohibition era; in an attempt to confirm their suspicions, the police wiretapped his phone without a warrant. Olmstead argued, unsuccessfully, that the incriminating evidence should have been excluded at his trial because the police violated his Fourth (and Fifth) Amendment rights. Although the five-justice majority denying Olmstead's appeal relied on the fact that the wiretap did not physically intrude on Olmstead's property, the now famous dissent by Justice Brandeis in that case laid the foundation for a more expansive, and often abstruse, definition of privacy under the Fourth Amendment. In a technologically equalizing move, Brandeis argued that there should be no legal difference between reading of a sealed letter and listening to a phone conversation. He contended the Fourth Amendment requires that Americans have the "right to be let alone" and that "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment" (p. 478).

For the next 40 years, the Court remained generally hostile to this suggestion that Fourth Amendment protections might be unrelated to the physical properties of the area searched. Eventually however, the Supreme Court rejected the pure physical trespass requirement of the *Olmstead* majority decision and adopted a privacy-centric interpretation of Fourth Amendment protections in *Katz v. United States* (1967). The *Katz* ruling extended Fourth Amendment protections beyond a limited property-rights approach to also include any place where a person has a "reasonable expectation of privacy" (p. 360). Justice Harlan's concurring opinion provided the two-prong test the

Court adopted for determining when privacy expectations are reasonable. The first consideration is whether the individual claiming an expectation of privacy had an actual, subjective expectation that the searched area or item was private. The second consideration is whether that subjective expectation is one that society is willing to recognize as reasonable (*Smith v. Maryland*, 1979, p. 740). The second, objective “reasonableness” portion of this test requires the courts to engage in a complicated process involving integrating existing legal doctrine and contemporary social norms in a manner that can be consistently applied across various areas and technologies.

One problem with the reasonable expectation of privacy test is that, in determining what society is willing to recognize as reasonable, judges often have to rely on their own assumptions about people's expectations. The subjective component of the test has been referred to as a “phantom doctrine,” because the Supreme Court rarely even mentions it, must less bases decisions on it (Kerr, 2015, p. 114). Accordingly, Supreme Court jurisprudence has focused on the normative question—whether expectations of privacy are objectively reasonable—and not *actual* expectations of privacy in determining when Fourth Amendment protections apply (see, e.g., *Illinois v. Caballes*, 2005; *United States v. Jacobsen*, 1984).

Based on judges' general assumptions of privacy, modern jurisprudence defining when a Fourth Amendment “search” has occurred often relies on the distinction between searches that occur outside as opposed to inside spaces (e.g., out in the open versus the inside suspect's home) (see *California v. Ciraolo*, 1986; Kerr, 2010, 2012; *United States v. Knotts*, 1983). Defining boundaries related to access are relatively easy to understand, for our homes and other items in the physical world. However, the inside versus outside distinction is increasingly blurry as searched items become more technological and virtual. For instance, is a laptop sitting open at a coffee shop searchable because it is in “plain view”? What if its desktop image is an incriminating picture (Bector, 2009)? Do people have a reasonable expectation of privacy in that picture in the same way they might in a picture inside their home? Do the laptop's privacy settings matter? At least one court held that a suspect did not have a reasonable expectation of privacy when police officers were able to view passwords on a computer screen over the suspect's shoulder (*United States v. David*, 1991); indeed, password protection on a device is not dispositive, but only one factor considered in determining reasonable expectations of privacy (*United States v. Barrows*, 2007). Clearly, the inside versus outside distinction provides very little guidance with most technological devices.

Additionally, the Supreme Court's “third-party doctrine” complicates matters when the police investigate technological devices. The third-party doctrine is essentially the idea that a person should not have an expectation of privacy in something they have voluntarily turned over to a third party. First described in *United States v. Miller* (1976), the court there held that individuals should not have an expectation of privacy in bank records consisting of information surrendered to the bank because they are part of the bank's business operations and owned by the bank. A few years later, the Supreme Court similarly addressed a pen register that recorded the phone numbers dialed by the defendant (*Smith v. Maryland*, 1979). Once again relying on the third-party doctrine and the defendant's voluntary disclosure of the numbers to the telephone company, the court held that the pen register was not a search for the purposes of the Fourth Amendment. Even prior to the explosion of social media use, Slobogin (2008) raised concerns about the third-party doctrine related to technology in the context of government and private companies data mining and collecting extensive amounts of personal information.

More recent decisions by the Supreme Court suggest a rethinking of both the outside–inside distinction and the third-party doctrine. In *United States v. Jones* (2012) the government attached a Global Positioning System (GPS) tracker on Antoine Jones's wife's vehicle and tracked the vehicle for 28 days. Based on the tracking, the government indicted Jones and others on drug trafficking conspiracy charges. The lower court suppressed the data from the tracker while the vehicle was parked at Jones's residence, but held he had no reasonable expectation of privacy while the vehicle was on the public streets. However, the Supreme Court held that the attachment and tracking constituted a search under the Fourth Amendment. Although the majority opinion focused on traditional issues of trespass in the placing of the tracker device, Justice Sotomayor's concurrence in *Jones* (2012) noted that physical trespass is unnecessary for most modern surveillance techniques (including GPS tracking on the phone), yet they can cheaply provide a unique set of private information (e.g., “trips to the psychiatrist, the plastic surgeon” p. 415). Justice

Sotomayor asked 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” (p. 416). Additionally, she questioned the use of the third-party doctrine in the “digital age” (p. 417).

Consistent with Justice Sotomayor's concerns about the amount of information shared through technology, two years after *Jones* the court unanimously held that police cannot search arrestees' cell phones without a warrant (*Riley v. California*, 2014). Although a warrantless search incident to arrest is permitted in most circumstances, the court reasoned that neither the fear of evidence destruction nor police protection was an appropriate justification for searching an arrestee's cell phone. Recognizing the vast amount of information stored on cell phones, the court noted that they contain a “digital record of nearly every aspect of [the suspects'] lives—from the mundane to the intimate” (p. 19). The court distinguished cell phones as different in “both a quantitative and qualitative sense” than other items found on arrestees, because cell phones are effectively minicomputers that can also make phone calls (p. 17). The unanimous court clearly viewed cell phones as a new category of item that could not be equated to physical papers or other items that had been addressed in previous cases.

The infrastructure that supports the way that modern, internet connected technology functions further frustrates attempts to translate these traditional principles into workable Fourth Amendment doctrine. Whenever we use the internet to send an email or post online, we communicate with and through that remote computer to contact other computers (Kerr, 2004). Our private information ends up being sent to third parties and held far away on remote network servers (Kerr, 2004). In 1986, recognizing that judicial interpretations of existing law and legal constructs such as the third-party doctrine left individuals' privacy at risk in light of new and emerging electronic surveillance technologies, Congress enacted the Stored Communications Act (SCA) of 1986 as an update to the Federal Wiretap Act of 1968. This statute sought to create Fourth Amendment-like protection for email and other digital communications stored on the Internet by, among other things, establishing a structure and criteria for voluntary and involuntary disclosure of information maintained by internet service providers (ISPs) about their customers. It clarified the need for, and process for obtaining, a court order to compel ISPs to disclose certain information to law enforcement and made disclosure of information to the FBI mandatory only upon required certification and for the purpose of counter-intelligence investigations.

However, the Supreme Court's decision in *Carpenter v. United States* (2018) demonstrates how the SCA's approach to protecting individuals' privacy in information compiled incident to use of modern communications technologies has been undermined by enormous advances in, and expanded popular use of, technologies after the Act's passage. In *Carpenter*, police conducting a criminal investigation into a multi-state robbery acquired Carpenter's cell-site location information (CSLI) records pursuant to a court order issued under §2703(d) of the SCA 18 U.S.C. §§2701–2712. CSLI is the data cell phones send several times per minute to nearby cell towers. Such data from multiple cell towers can help triangulate a cell phone's location with great accuracy, especially in urban areas where there is a high concentration of cell towers. Wireless carriers collect and store the CSLI for their business purposes and without specific notice to the user. Under §2703(d) of the SCA, the government was only required to show “reasonable grounds to believe that records sought are relevant and material to an ongoing criminal investigation” (p. 2230). Such a showing is less stringent than the normal probable cause required to obtain a warrant. In investigating Carpenter, the government obtained such a court order to compel his wireless service carrier to turn over CSLI data that contained his public and private movements, as tracked by his cell phone pings, over a four-month period. These records included 12,898 individual cell-site location points, including data points that placed Carpenter's phone near four robbery locations at the time of the robberies. Using these location points as evidence, Carpenter was charged with multiple counts of robbery and carrying a firearm. Carpenter's legal team moved to suppress the CSLI on the ground that the government had not obtained a warrant. In response, the government countered that the records were properly obtained under a §2703(d) order because they were not protected by the Fourth Amendment under the third-party doctrine.

The Supreme Court ultimately agreed with *Carpenter*, holding that accessing the record of the defendant's movements in the form of his historical cell-site records was a search, and that therefore the police were required to obtain a search warrant before doing so. Although CSLI data would seem similar to traditional third-party data, the Court declined to extend *Miller* and *Smith*, noting that the CSLI data allowed the police to have a "detailed, encyclopedic, and effortlessly compiled" record (p. 2216). "There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.... [...] this is not a straightforward application of the third-party doctrine," but instead a significant extension of it to a "distinct category of information" (p. 2219).

The court concluded that the government should have obtained a warrant rather than relying on the §2703(d) order, because the Fourth Amendment is meant to protect the "privacies of life" and "to place obstacles in the way of a too permeating police surveillance" (p. 2214). Applying the third-party doctrine would "fail[] to contend with the seismic shifts in digital technology that made possible the tracking of not only *Carpenter's* location but also everyone else's, not for a short period but for years and years" (p. 2219). The court further observed that "[i]n fact, historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*. Unlike the bugged container in *Knotts* or the car in *Jones*, a cell phone – almost a feature of human anatomy—tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time" (p. 2218). The "[r]etrospective quality of the data here gives police access to a category of information otherwise unknowable" (p. 2218).

Since *Carpenter*, scholars have suggested principles to guide lower courts in applying the reasoning and decision to new situations and technologies. According to Kerr (in press), "*Carpenter* signals a major break from the traditional understanding" of focusing on the act that constitutes the search, and rather requires courts to examine the type of information that is revealed from such actions (p. 5). Kerr outlined three principles for a collection of information to receive Fourth Amendment protection under *Carpenter*: (i) law enforcement collects information using digital technology; (ii) the records are necessarily created when a person uses a core technology and not as a result of a meaningful, voluntary choice of the user; and (iii) the records reveal personal information, such as associations, religious beliefs, sexual preferences, and political views, that are beyond legitimate interests of a criminal investigation (p. 3). Thus, according to Kerr, pre-digital searches, such as security cameras, that existed before the digital age are not subject to the new analysis, and traditional third-party cases such as *Smith* (telephone numbers dialed) and *Miller* (bank records) still stand. Second, to receive Fourth Amendment protections under *Carpenter*, the user must not create the record through a meaningful voluntary choice. However, when technology automatically creates records as a condition of using a device, as occurred in *Carpenter*, Fourth Amendment protections fully apply. Finally, to qualify under *Carpenter*, the records must "reveal an intimate portrait of a person's life typically beyond legitimate state interest" (p. 22). These personal truths, such as sexual preferences, medical history, and religious affiliation, do not tend to reveal evidence of a crime but are merely representative of the sort of informational privacy concerns the Fourth Amendment ought to protect.

Rozenshtein (2019) takes a different view of *Carpenter*. He completely rejects the third-party doctrine and assumes that the Fourth Amendment applies to any (or most) government investigations. Then, the level of suspicion that is required for a particular search (probable cause or something less) is tailored to various factors, including the invasiveness of the government actions, the public-safety interests, and the costs and benefits of the different levels of authorization. Rozenshtein views *Carpenter* as less a discussion of when the Fourth Amendment comes into play, and more a beginning of an examination into what level of suspicion and pre-authorization are reasonable for digital searches. Other scholars (e.g., Slobogin, 2007) have previously suggested and addressed in more detail a similar graduated level of suspicion.

The more recent decisions from the Supreme Court and the scholarly views of how they should be interpreted make re-analysis of the expectations of privacy test imperative. One possibly helpful source of this re-analysis is lay views about privacy. As noted by Kugler and Strahilevitz (2016), "[w]hen there is a sharp divide between what the courts describe as the Fourth Amendment's scope and what the people actually expect the Fourth Amendment's

scope to be, various problems arise" (p. 227). Therefore, it is useful to consider what laypeople believe about the Fourth Amendment and what they hold as private against police and government intrusion.

We turn now to empirical research that has examined laypeople's interpretations of privacy and government intrusion.

1.2 | Previous empirical research on privacy

Generally, courts rely on their intuitive notions of privacy and what seems an appropriate expectation of such privacy. However, empirical social science research can aid in court determinations concerning what society is willing to recognize as reasonable (the objective prong of the two-prong test) by providing systematic information from society (Chanenson, 2004). Despite this seemingly clear need, the Fourth Amendment has not been a key law-psychology area of research (Wylie, Hazen, Hoetger, Haby, & Brank, 2018). What research has been done demonstrates that people's privacy expectations differ across situations and search targets and that these expectations also differ from the expectations that courts assume people have in varying situations (Blumenthal, Adya, & Mogle, 2009; Slobogin, 2002, 2008; Slobogin & Schumacher, 1993). For example, Slobogin and Schumacher (1993) compared lay individuals' evaluations of search scenarios with the Supreme Court's evaluations of cases addressing the same situations. For many of the 50 search scenarios presented, the participants' ratings of intrusiveness matched the Fourth Amendment protections the court provided (Slobogin & Schumacher, 1993). However, there were some key differences between Supreme Court rulings and participants' ratings of intrusiveness. For instance, participants viewed use of undercover agents and a dog sniff of a vehicle as fairly intrusive, while the Supreme Court has held that these searches do not violate reasonable expectations of privacy.

Slobogin extended this research and the methods used to examine laypersons' perceptions of the use of data mining (Slobogin, 2008) and surveillance cameras (Slobogin, 2002), compared with perceptions of more traditional police searches. Similar to the results of Slobogin and Schumacher, he found in that laypersons judged search intrusiveness in ways that were sometimes inconsistent with court rulings. Related to the Court's recent rulings touching on privacy expectations for cell phones, laypersons thought an isolated search of a single phone call was less intrusive than an aggregate composite of all phone records (Slobogin, 2008). Contrary to the assumptions of the third-party doctrine, intrusiveness was not systematically reduced for information that was shared with others in some way. Instead, intrusiveness was more related to the type of information searched (Slobogin, 2008).

Consistent with the findings by Slobogin and Schumacher (1993), Blumenthal et al. (2009) found additional evidence that contextual factors that tend to be undervalued in existing Fourth Amendment caselaw impact perceptions of search intrusiveness. Fradella et al. (2011) also expanded the work of Slobogin and Schumacher by providing participants with more contextual information, examining the extent to which their participants agreed with Fourth Amendment precedent, and exploring demographic and attitudinal influences on participants' expectations of privacy. Specifically, Fradella and colleagues were interested in bodily, territorial, informational, and communications privacy. Although there were some demographic differences, in general their sample had a greater expectation of privacy than the court has endorsed.

Of particular importance for the current study, participants in Fradella et al. (2011) had strong beliefs about communication and information privacy and significantly disagreed with court holdings that limited or infringed on that privacy. For example, 85% of respondents disagreed with the Court's analysis in *Miller* that no reasonable expectation of privacy exists for financial information shared with a third party. Additionally, almost 60% of the respondents disagreed with the legality of a warrantless search that revealed "sexted" images from a teen male to a teen (under-age) female. Conversely, nearly 55% of those same respondents agreed with the court that the act of placing trash on the curb for garbage collectors relinquished any reasonable expectation of privacy one might have to its contents, because anyone could easily go through the trash bags on the curb (*California v. Greenwood*, 1988). Taken together, these divergent expectations suggest that traditional principles identifying when a person relinquishes an

expectation of privacy in physical spaces are often perceived by laypeople as inapplicable to understanding the privacy interests implicated by a government search of electronic information or records.

In 2015, Scott-Hayward, Fradella, and Fischer conducted another survey of American adults' normative beliefs regarding the burden of proof that law enforcement should be required to have before conducting searches of electronic information: no proof, gut instinct, reasonable suspicion, probable cause, or never. The majority of participants reported they thought probable cause should be required for law enforcement to access location tracking data, social media profiles, cell phones, and email accounts. Older adults reported greater expectations of privacy in social media posts shared with friends, online purchase history, and online television shows watched than did younger adults, while younger adults reported greater privacy expectations in GPS location data than did older adults. Smith, Madden, and Barton (2016) extended this research and found, consistent with Fradella and colleagues, that participants overwhelmingly disapproved of technologically aided governmental intrusions into physical spaces without a warrant, even ones the Supreme Court has explicitly endorse as outside the scope of Fourth Amendment protections, such as aerial surveillance. Consistent with court holdings in *United States v. Jones* and *Riley v. California*, participants disapproved of police tracking suspects with a GPS tracking device or searching a cell phone. Moreover, relevant to the decision in *Carpenter*, participants were also disapproving of law enforcement tracking suspects via information shared between devices and local cell phone towers (i.e., CSLI data).

Kugler and Strahilevitz (2016) have used public opinion surveys to examine whether certain law enforcement activities would "violate people's reasonable expectations of privacy" (p. 246). Law enforcement activities included using a car's GPS system to locate it on public streets without the owner's permission. Participants were asked to make multiple evaluations of this type of governmental intrusion based on whether the GPS was used to track a person's movements for one day versus one week versus one month. For the most part, participants saw these activities as violating a reasonable expectation of privacy regardless of how long the information was collected. Kugler and Strahilevitz (2017) further examined their data to determine how much impact the Supreme Court opinion in *Riley* had on public opinion about privacy rights. In general, there was only a slight impact on public attitudes immediately after the decision for those respondents who were familiar with the case, but the impact was gone one year later. Kugler and Strahilevitz (2017) interpreted these findings as evidence that normative public opinions about privacy and search intrusiveness are not entirely responsive to actions taken by the Supreme Court, as had been previously proposed by others.

Related to the issues raised in *Carpenter*, Tokson (2016) surveyed 810 community members on MTurk about their knowledge concerning the privacy of their cell phone data. The results indicated that the majority of cell phone users are not aware that their cell phone provider collects their location data. In fact, about 15% of respondents believed that their data was not collected at all. Finally, only three percent of respondents were aware that cell phone location data can be used by the government in surveillance for court cases. Overall, this research indicated that the public's actual beliefs about how their cell phone information is used is contrary to courts' conclusions about the public's collective knowledge of cell phone data.

Most recently, Chao et al. (2018) conducted an online survey asking participants to evaluate 18 different investigative activities on how intrusive the described activities were and whether there was a violation of reasonable expectations of privacy. Additionally, the scenarios were described both from the first- and third-person perspective and the search outcome was manipulated as either evidence of criminal activity found, or no evidence found. Perspective and outcome both significantly impacted participants' responses concerning the reasonableness of the search. Replicating findings by Slobogin and Schumacher (1993), they found that when participants took the first-person perspective and when no evidence was found the search was seen as less reasonable than when the third-person perspective was taken and evidence was found. Similar to previous research, the participants of Chao et al. (2018) agreed with some of the Supreme Court determinations, but not others. For example, although the court has restricted police use of suspicionless roadblocks (*City of Indianapolis v. Edmond*, 2000), the participants in this study saw this technique as much less intrusive and only 27% thought it was a violation of a reasonable expectation of privacy. Chao et al. (2018) also focused on situations the court has not yet examined, such as police

obtaining information from Cloud storage and other technology searches. Participants were especially sensitive to many of these technology searches, seeing them as highly intrusive.

1.3 | The current research

Overall, previous research on perceptions of searches of technology indicates that people have high privacy expectations for information contained on their devices. While recent survey research (i.e., Chao et al., 2018; Kugler & Strahilevitz, 2016, 2017) is important in providing information about the beliefs of the typical innocent person, the questions were limited to plumbing reasonable expectations of privacy (Chao et al., 2018; Kugler & Strahilevitz, 2016, 2017) and intrusiveness (Chao et al., 2018), and did not include other measures of government intrusion that might provide insight into people's reactions to technology searches, such as knowledge that the government is searching or likelihood of consenting to a search. Additionally, previous research has tended to present laypersons with scenarios that provided some combination of information about the nature of the information searched, the investigatory techniques used to access it, and context-specific details related to the quantitative or qualitative characteristics of the item targeted by the search. Although all these factors have been identified as vital to the court's reasonableness analysis, previous research tended not to investigate whether the nature of the item itself impacts privacy expectations and perceptions of intrusiveness and how privacy, consent, and notice interact.

The purpose of the current research was to extend this research to compare privacy expectations and perceptions of searches for multiple types of technology. Specifically, this research investigated privacy expectations for cell phone contents, email, Cloud storage use, GPS tracking, and location tracking on cell phones. In addition to examining privacy expectations for these technologies, we also examined how laypersons perceive searches of these technologies in terms of how invasive they are, how likely it is that they could be conducted without the owner's knowledge, how likely it is that they could be conducted without a warrant, and how likely the owner would be to consent to a search of these items.

2 | METHOD

2.1 | Participants

Participants were 260 community members recruited on Mechanical Turk, an online work distribution website (Paolacci & Chandler, 2014). Although some researchers question the validity of samples derived from MTurk in the Fourth Amendment context (Kugler & Strahilevitz, 2016, 2017), research indicates that participants recruited on MTurk do not differ significantly in their responses to surveys from other community samples in other contexts (Kees, Berry, Burton, & Sheehan, 2017; Sheehan, 2018; Walter, Siebert, Goering, & O'Boyle, 2019). Data was collected in December 2017, six months prior to the Supreme Court handing down a decision in the *Carpenter* case in June 2018. Workers were limited to US residents. In the sample, 49.6% ($n = 129$) identified as female and 47.3% ($n = 123$) were male, 68.8% ($n = 179$) of the participants identified as White, 15.8% ($n = 41$) as Black, 5.4% ($n = 14$) as Latino/a, 5% ($n = 13$) as Asian, and 3.1% ($n = 8$) as other. Ages ranged from 18 to 71, with a mean age of 35.72 ($SD = 11.40$). All participants were treated according to the American Psychological Association Ethical Principles of Psychologists and the Office of Human Research Protection guidelines.

2.2 | Materials and procedures

Participants were directed to an online survey conducted using SurveyMonkey. Informed consent was obtained on the first page of the survey. The following pages asked five overarching questions about their opinions regarding

privacy and police searches of electronic devices or remote searches of personal data that might be stored by third-party electronic service providers.

2.2.1 | Devices and personal information included

As a part of a larger survey, participants rated their expectations of privacy and perceptions of police intrusions on a variety of personal devices, electronic services, and data commonly stored on those devices or by electronic service providers. Electronic devices and services of interest included a personal cell phone, a GPS or navigation system in a car, public traffic-surveillance cameras, personal email accounts, and Cloud data storage. Sub-categories of data associated with the use of email and cell phones also were included. For a personal cell phone, we asked about data that might implicate various information and communication privacy concerns: location-tracking data (i.e., CSLI), photos or videos (locally stored on device), notes or memos (locally stored on device), text messages, call-log history, information from calendars, health and activity tracking, and information about financial transactions (i.e., digital wallet activity). For email, we asked about email messages recently stored and older emails.

2.2.2 | Expectations of privacy

Participants first rated how much privacy they would generally expect for each item listed. Items were rated on Likert-type scales of 1–7, with 7 indicating higher levels of privacy expectation.

2.2.3 | Perceptions of police searches

Participants were then asked to consider each item and evaluate the intrusiveness of a hypothetical police search of that item. First, participants rated how much they would feel that their privacy would be violated if the item were searched by the police (privacy violation) to assess the relative intrusiveness of searches of those items by the government. Second, participants rated how likely they would be to consent to or to allow the police to search the item (consent), partly to assess perceptions of how likely they would be to voluntarily relinquish that information under the sharing principle of the third-party doctrine and partly as an indirect measure of how strongly they felt about the privacy of that information. Third, participants rated how likely it is that the police could conduct a search of the item without their knowledge (knowledge) to assess perceptions of government authority to search and expectations regarding government notice to a searchee. Finally, participants rated how likely it is that the police could conduct a search of the item without a search warrant (warrant) to assess perceptions of constitutional protections provided for each item. Participants responded to all of these questions on Likert-type scales of 1–7, with 7 indicating higher levels of privacy violation and likelihood (e.g., likelihood that the police would search without their knowledge).

2.2.4 | Technology usage, general privacy attitudes, and demographics

Following the questions about police searches for the various items, participants were asked to answer questions about their behaviors and attitudes related to technological privacy more generally. Participants were asked to self-report how frequently they used common devices or services such as cell phones, email accounts, and Cloud storage on eight-point Likert-type scales, with 0 being “Do not use,” 1 being “not very often,” and 7 being “very often.” Participants also self-reported their willingness to share private information on internet

connected devices and electronic services on a 1–7 Likert-type scale, with 7 indicating higher levels of private sharing.

Additionally, participants also completed a modified scale from Malhotra, Kim, and Agarwal (2004) to measure attitudes towards privacy on the internet more generally. Examples of scale items included “When websites I visit ask me for personal information, I sometimes think twice before providing it,” “I’m concerned that online companies are collecting too much personal information about me,” and “To me, it is important to keep my privacy intact from online companies.” All items were measured on seven-point Likert-type scales, with higher scores indicating stronger attitudes towards protecting one’s privacy online. The items together were reliable (Cronbach’s $\alpha = 0.93$). The items were averaged together to form the combined measure of “general privacy attitudes” (GPA) used in the following analyses ($M = 5.56$, $SD = 1.30$). Finally, participants answered a series of demographic questions including their current status of employment, gender, age, and ethnicity. All participants were debriefed at the end of the survey and compensated for their participation.

3 | RESULTS

3.1 | Technology usage and participant characteristics

3.1.1 | Technology usage

We used one-sample *t*-tests to examine how frequently participants used technologies of interest in the survey (comparing responses with the scale midpoint of 4). As shown in Table 1, participants reported frequently using personal cell phone devices and email, and only reported moderate usage of Cloud storage accounts. For navigation assistance, they reported frequently using an application on their cell phone device, and infrequently using a GPS or navigational system built into their car. We did not have specific hypotheses about the relationship between participant demographics and device usage, but we found several correlations that should be noted and are shown in Table 2. Age was significantly positively related to reported personal cell phone and email usage but was not related to use of a Cloud storage account or a GPS in the car. Gender (dummy coded, with male used as the reference category) was also not related to Cloud storage. However, there was a relationship between gender and reported usage of personal cell phones, email, and car GPS, such that male participants reported being more likely to use a car GPS but less likely to use cell phones and email.

TABLE 1 One-sample *t*-tests and descriptive statistics for reported frequency of technology usage

	Descriptives					One-sample <i>t</i> -test (comparison value = 4)	
	<i>N</i>	Mean	<i>SD</i>	Median	% do not use	<i>t</i>	<i>df</i>
Personal cell phone	255	6.05	1.61	7.00	0.8% (<i>n</i> = 2)	20.39***	254
Personal email	254	6.07	1.54	7.00	1.5% (<i>n</i> = 4)	21.48***	253
Cloud storage account	252	3.78	2.43	4.00	13.8% (<i>n</i> = 36)	−0.145	251
GPS or navigation system							
via cell phone application	256	4.30	2.30	5.00	10.0% (<i>n</i> = 26)	2.09*	255
in car	254	1.85	2.52	0.00	55.0% (<i>n</i> = 143)	−13.57***	253

Note:

* $p < 0.05$, *** $p < 0.001$.; Responses were measured on eight-point Likert-type scales (0 being “Do not use,” 1 being “not very often,” and 7 being “very often”).

TABLE 2 Spearman's rank order correlations for demographics, privacy attitudes, and device usage variables

	1	2	3	4	5
1. Age	—				
2. Gender (dummy coded: male = 1; female = 0)	−0.199**	—			
3. Ethnicity (dummy coded: white = 1; non-white = 0)	−0.070	−0.024	—		
4. Willingness to share private information	−0.034	0.130*	0.044	—	
5. GPA score	0.266***	−0.215**	0.053	−0.225***	—
6. Cell use	0.143*	−0.190**	−0.044	0.094	0.294***
7. Email use	0.340***	−0.224***	−0.045	−0.023	0.340***
8. Cloud use	−0.0107	0.048	0.087	0.169**	0.039
9. GPS car use	−0.104	0.230***	−0.015	0.141*	−0.122

3.1.2 | Privacy attitudes

We also used one-sample *t*-tests to determine whether willingness to share private information on various technologies were significantly above or below the midpoint of the scale (scale of 1–7, midpoint = 4). As indicated in Table 3, participants reported little willingness to share private information when using technology that is connected to the internet, and they reported making their settings private for social media websites, email accounts, and cell phones. Spearman's rank order correlations (see Table 2) were used to examine privacy attitudes and demographic factors. Age was not related to willingness to share private information, but it was positively related to general privacy attitude (GPA) scores, such that older participants reported valuing their privacy more. Gender (dummy coded with male used as the reference category) was positively related to willingness to share private information but negatively related to GPA score, such that female participants reported being more willing to share private information on the internet and valued their privacy less than males in our sample. Conversely, ethnicity (recoded with “white” as the reference category compared to “non-white”) was not significantly related to any of the privacy attitude or device usage variables.

3.1.3 | Technology usage and privacy attitudes

We hypothesized that participants' willingness to share private information and GPA scores would be related to their reported usage of various electronic devices or services. Contrary to the hypothesis, Spearman's rank order correlations (see Table 2) indicated that participants' willingness to share private information was not significantly related to their reported use of a personal cell phone or email account. Consistent with the hypothesis, willingness to share private information was positively correlated with usage of a Cloud storage account and a GPS device or navigational system in their car, such that the more willing they were to share private information, the more likely they were to use Cloud storage and GPS in their car. Conversely, GPA scores were not related to Cloud storage, but they were negatively correlated with car GPS use, and positively correlated with usage of a cell phone and email usage, such that people who value privacy more were less likely to use a GPS but more likely to use cell phones and email. These results must be interpreted with caution, however, as only a minority of our participants actually used a car GPS system.

TABLE 2 Spearman's rank order correlations for demographics, privacy attitudes, and device usage variables

	6	7	8	9
1. Age				
2. Gender (dummy coded: male = 1; female = 0)				
3. Ethnicity (dummy coded: white = 1; non-white = 0)				
4. Willingness to share private information				
5. GPA score				
6. Cell use	—			
7. Email use	0.613***	—		
8. Cloud use	0.118	0.034	—	
9. GPS car use	−0.313**	−0.276***	−0.280***	—

Note:

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$; Correlations were calculated in SPSS, and therefore with pair-wise deletion of missing variables.

TABLE 3 One-sample *t*-tests and descriptive statistics for privacy attitudes

	Descriptives			One-sample <i>t</i> -test (comparison value = 4)	
	<i>N</i>	Mean	<i>SD</i>	<i>T</i>	<i>df</i>
Willingness to share private information	254	3.59	1.56	−4.22***	253
GPA score	254	5.11	1.61	−10.99***	252

Note:

*** $p < 0.001$; Responses were measured on Likert-type scales of 1–7 (higher numbers indicate more privacy).

3.2 | Expectations of privacy and search invasiveness¹

3.2.1 | Location information in third-party contexts

Planned comparisons using a series of Wilcoxon signed-rank tests with a Bonferroni correction were used to examine differences in perceptions of CSLI, GPS data from a car, and data recorded from public traffic surveillance cameras. Based on the court's analysis in *Carpenter*, we hypothesized that people would generally expect more privacy and report greater privacy violations for a police search of cell phone location-tracking data than for other information about their public movements, such as information collected by public traffic cameras or recorded by a GPS device in a car. Consistent with the hypothesis, people expected more privacy in their public movements when obtained through tracking their cell phone than when recorded by traffic cameras or recorded by a GPS device in a car (see Table 4).

Also consistent with the hypothesis, people reported feeling like their privacy would be more violated by a police search of location-tracking data from their personal cell phone than either traffic camera surveillance or a search of location-information recorded by a GPS device in a car (see Table 5). They also were less likely to consent to a police search of their CSLI data than places their car has been as recorded by traffic cameras (see Table 5). Similarly, as expected, they reported believing that it was more likely that location information recorded by traffic cameras could be searched by the police without their knowledge or without a warrant (see Table 6), suggesting that people expect

¹Significant skew was observed for all measures of privacy expectations and perceptions of police searches. To correct for significant skew, all dependent measures were transformed by taking the square root of their raw value. Transformations did not correct non-normality; therefore, the raw values were used in non-parametric tests rather than parametric tests when appropriate.

TABLE 4 Expectations of privacy (CSLI versus GPS or car location information)

	Descriptives				Wilcoxon signed rank test	
	N	Mean	SD	Median	Wilcoxon Z	Effect size <i>r</i>
Locations you have been, as tracked by your personal cell phone (CSLI)	260	4.81	1.98	5.00	—	—
Places you have been that were recorded on a GPS system in your car	257	4.23	2.17	4.00	−3.87	0.24***
Places your car has been as recorded by public traffic cameras	257	3.63	2.14	4.00	−7.23	0.45***

Note:

****p* < 0.001.; Responses were measured on Likert-type scales of 1–7 (higher numbers indicate more privacy expected).

TABLE 5 Violation of privacy and likelihood of consent for police search (CSLI versus other GPS or car location information)

	Descriptives				Wilcoxon signed rank test	
	N	Mean	SD	Median	Wilcoxon Z	Effect size <i>r</i>
<i>Violation of privacy</i>						
Locations you have been, as tracked by your personal cell phone (CSLI)	259	5.66	1.65	6.00	—	—
Places you have been that were recorded on a GPS system in your car	255	5.05	2.16	6.00	−4.55	0.28***
Places your car has been as recorded by public traffic cameras	256	4.34	2.25	4.00	−8.45	0.52***
<i>Likelihood of consent</i>						
Locations you have been, as tracked by your cell phone (CSLI)	260	3.40	2.28	3.00	—	—
Places you have been that were recorded on a GPS system in your car	254	3.62	2.38	4.00	−1.86	0.12
Places your car has been as recorded by public traffic cameras	256	3.88	2.34	4.00	−3.81	0.24***

Note:

****p* < 0.001.; Responses were measured on Likert-type scales of 1–7 (higher numbers indicate more privacy violation or likely to consent).

less privacy for their public movements as recorded by traffic cameras. There were no significant differences between CSLI data and recorded car GPS location data on likelihood of consent (see Table 5) or the belief that the search could occur without a warrant (see Table 6). However, people rated as significantly more likely that the police could search CSLI data than recorded car GPS location data without their knowledge (see Table 6). Given the pattern of relationships between personal cell phone and car GPS device usage, it is unlikely that demographic characteristics provide a systematic explanation for the differences observed between CSLI and GPS data.

TABLE 6 Ability for police to search without the searchee's knowledge or a warrant (CSLI versus GPS or car location information)

	Descriptives				Wilcoxon signed rank test	
	N	Mean	SD	Median	Wilcoxon Z	Effect size <i>r</i>
<i>Ability to search without knowledge</i>						
Locations you have been, as tracked by your cell phone (CSLI)	259	4.64	1.95	5.00	—	—
Places you have been that were recorded on a GPS system in your car	255	4.29	2.09	4.00	−2.09	0.29*
Places your car has been as recorded by public traffic cameras	256	5.15	2.05	6.00	−3.99	0.18***
<i>Ability to search without a warrant</i>						
Locations you have been, as tracked by your cell phone (CSLI)	259	3.62	2.22	4.00	—	—
Places you have been that were recorded on a GPS system in your car	256	3.54	2.17	3.00	−0.18	0.01
Places your car has been as recorded by public traffic cameras	255	4.70	2.25	5.00	−6.17	0.39***

Note:

* $p < 0.05$.; *** $p < 0.001$.; Responses were measured on Likert-type scales of 1–7 (higher numbers indicate more likely to occur without knowledge or without a warrant).

3.2.2 | Cell phone activities in third-party contexts

We conducted the following analyses using Friedman's test to analyze differences in privacy expectations and perceptions of police searches across types of information recorded on a cell phone. A series of Wilcoxon signed-rank tests using a Bonferroni correction were used as follow-up tests to directly compare ratings of location-tracking data with the other categories of personal information associated with use of a cell phone device. Based on previous research on lay perceptions of government intrusions into cell phone devices and remote searches of electronic data, we predicted that privacy expectations and ratings of intrusiveness for different cell phone activities would be influenced by the nature of the particular data or information searched.

There was a significant difference among the distributions of privacy expectations for the seven categories of personal information from a personal cell phone ($\chi^2(7) = 169.732$, $p < 0.001$, Kendall's $W = 0.096$). People reported generally expecting less privacy for the records of locations indicating where they have been as tracked by their cell phone than for photos or videos, text messages, notes or memos, call history, calendar information, health or activity data, and information from a digital wallet (i.e., PayPal, Google Wallet, Visa Checkout) (see Table 7).

There were also significant differences in ratings of how much participants felt a police search would violate privacy across the categories of personal information from a personal cell phone ($\chi^2(7) = 135.782$, $p < 0.001$, Kendall's $W = 0.076$). People felt their privacy would be less violated by a police search of the records of locations tracked by their cell phone than for a search of photos or videos, text messages, notes or memos, calendar information, and information from a digital wallet. However, there was no significant difference between CSLI and call history or health and activity data (see Table 8).

Significant differences also emerged in ratings of likelihood of consenting to a police search across the categories of personal information from a personal cell phone ($\chi^2(7) = 72.76$, $p < 0.001$, Kendall's $W = 0.041$). People reported being more likely to consent to a police search of the records of locations tracked by their cell phone than a

TABLE 7 Expectations of privacy (CSLI versus other cell phone activities)

	Descriptives				Wilcoxon signed rank test	
	N	Mean	SD	Median	Wilcoxon Z	Effect size r
Locations you have been, as tracked by your personal cell phone (CSLI)	260	4.81	1.98	5.00	—	—
<i>Other cell phone items</i>						
Photos or videos (<i>locally stored on device</i>)	257	5.65	1.61	6.00	−7.54	0.47***
Text messages	259	5.48	1.65	6.00	−6.39	0.39***
Notes or memos (<i>locally stored on device</i>)	259	5.56	1.62	6.00	−6.82	0.42***
Call history (date, time, and duration of recent calls)	259	5.17	1.74	5.00	−3.97	0.25***
Information from calendars	258	5.24	1.72	6.00	−4.23	0.19***
Health and activity data	259	5.25	1.78	6.00	−4.74	0.29***
Information from a digital wallet (such as PayPal, Google Wallet, Visa Checkout, etc.)	260	5.88	1.53	7.00	−8.70	0.54***

Note:

*** $p < 0.001$.; Responses were measured on Likert-type scales of 1–7 (higher numbers indicate more privacy expected).

search of photos or videos, text messages, and information from a digital wallet. However, they reported being equally likely to consent to a search of notes or memos, call history, calendar information, and health or activity data (see Table 8). There was also a significant difference in perceptions of how likely it was that the police would be able to conduct a search across the categories of personal information from a personal cell phone without the searchee's knowledge ($\chi^2(7) = 316.86$, $p < 0.001$, Kendall's $W = 0.179$) and without a warrant ($\chi^2(7) = 82.734$, $p < 0.001$, Kendall's $W = 0.047$). Participants rated it more likely that the police could search the records of locations tracked by their cell phone than photos or videos, text messages, notes or memos, calendar information, health or activity data, and information from a digital wallet without their knowledge. However, we found no significant difference between CSLI and call history in perceptions that police could search without their knowledge (see Table 9).

Similar to police ability to search without the user's knowledge, participants rated it more likely that the police could search for the records of locations they have been as tracked by their cell phone than photos or videos, text messages, notes or memos, calendar information, health or activity data, and information from a digital wallet without a warrant. However, participants rated it equally likely that police would need to get a warrant for cell phone location data and call history (see Table 9). Taken together, these results indicate that people expect that many categories of data on their cell phone other than location data will remain private.

3.3 | Protections under the SCA

3.3.1 | Non-content versus content information in third-party contexts

Based on the Court's conclusion that the privacy interests associated with the CSLI records in *Carpenter* were sufficient to trigger full Fourth Amendment protections, we wanted to examine whether police searches for CSLI data are perceived as more intrusive than searches involving other types of information that remain accessible through a lesser process than a warrant. Currently, the SCA requires government officials to obtain a warrant to search the contents of emails stored by internet service providers for less than 180 days, but officials only need a subpoena to access emails stored for 180 days or longer. The Sixth Circuit has held that such subpoena-based searches do violate

TABLE 8 Violation of privacy and likelihood of consent for police search (CSLI versus other cell phone activities)

	Descriptives				Wilcoxon signed rank test	
	N	Mean	SD	Median	Wilcoxon Z	Effect size <i>r</i>
<i>Violation of privacy</i>						
Locations you have been, as tracked by your personal cell phone (CSLI)	259	5.66	1.65	6.00	—	—
<i>Other cell phone items</i>						
Photos or videos (<i>locally stored on device</i>)	260	5.94	1.49	7.00	−3.44	−21**
Text messages	258	6.03	1.52	7.00	−5.08	0.32***
Notes or memos (<i>locally stored on device</i>)	259	5.46	1.78	6.00	−2.54	0.16*
Call history (date, time, and duration of recent calls)	260	5.74	1.61	6.00	−1.08	0.07
Information from calendars	258	5.24	1.92	6.00	−4.05	0.25***
Health and activity data	260	5.57	1.80	6.00	−1.10	0.05
Information from a digital wallet (such as PayPal, Google Wallet, Visa Checkout, etc.)	260	6.09	1.46	7.00	−4.88	0.30***
<i>Likelihood of consent</i>						
Locations you have been, as tracked by your cell phone (CSLI)	260	3.40	2.28	3.00	—	—
<i>Other cell phone items</i>						
Photos or videos (<i>locally stored on device</i>)	259	3.40	2.28	3.00	−3.69	0.23***
Text messages	259	3.24	2.25	3.00	−2.46	0.15**
Notes or memos (<i>locally stored on device</i>)	260	3.32	2.27	6.00	−1.17	0.07
Call history (date, time, and duration of recent calls)	260	3.44	2.25	3.00	−.83	0.05
Information from calendars	256	3.43	2.28	3.00	−.55	0.03
Health and activity data	260	3.30	2.27	3.00	−.90	0.06
Information from a digital wallet (such as PayPal, Google Wallet, Visa Checkout, etc.)	260	2.78	2.16	1.00	−5.51	0.34***

Note:

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$; Responses were measured on Likert-type scales of 1–7 (higher numbers indicate more privacy violation or likely to consent).

the Fourth Amendment (*United States v. Warshak*, 2010), but the US Supreme Court has not directly addressed the issue, so the subpoena provision of the SCA still stands.

Specifically, we were interested in comparing evaluations of a police search of non-content information such as cell phone location-tracking data with searches of content information such as email messages stored on a personal email account. Moreover, we were interested in comparing expectations and ratings of intrusiveness across items that are afforded different statutory protections under the SCA. From this sample, 62.3% of participants rated using their personal email very often ($M = 6.07$, $SD = 1.59$). A series of Wilcoxon signed-rank tests were again used to determine if there were significant differences between cell-location data and email items on these variables. Consistent with hypothesis, participants reported generally expecting less privacy for the non-content records of cell location data than both the content records of recent email messages and older email messages (see Table 10).

Contrary to assumptions underlying the SCA, which permits access to records of CSLI and older email records under essentially the same (relatively easy-to-prove) circumstances, and contrary to *Carpenter* (which requires a

TABLE 9 Ability for police to search without the searchee's knowledge or a warrant (CSLI versus other cell phone activities)

	Descriptives				Wilcoxon signed rank test	
	N	Mean	SD	Median	Wilcoxon Z	Effect size <i>r</i>
<i>Ability to search without knowledge</i>						
Locations you have been, as tracked by your personal cell phone (CSLI)	259	4.64	1.95	5.00	—	—
<i>Other cell phone items</i>						
Photos or videos (<i>locally stored on device</i>)	258	3.64	2.10	4.00	−7.80	0.49***
Text messages	260	4.15	2.07	4.00	−4.83	0.30***
Notes or memos (<i>locally stored on device</i>)	259	3.53	2.08	3.00	−8.11	0.50***
Call history (date, time, and duration of recent calls)	259	4.64	1.97	5.00	−.248	0.02
Information from calendars	258	3.64	2.08	4.00	−7.69	0.48***
Health and activity data	260	3.66	2.13	4.00	−7.20	0.48***
Information from a digital wallet (such as PayPal, Google Wallet, Visa Checkout, etc.)	259	3.58	2.13	4.00	−7.40	0.46***
<i>Ability to search without a warrant</i>						
Locations you have been, as tracked by your cell phone (CSLI)	259	3.62	2.22	4.00	—	—
<i>Other cell phone items</i>						
Photos or videos (<i>locally stored on device</i>)	258	3.10	2.23	4.00	−4.49	0.28***
Text messages	259	3.27	2.27	3.00	−3.57	0.22***
Notes or memos (<i>locally stored on device</i>)	259	3.06	2.16	2.00	−5.11	0.32***
Call history (date, time, and duration of recent calls)	259	3.47	2.25	3.00	−1.61	0.10
Information from calendars	257	3.04	2.16	2.00	−5.22	0.33***
Health and activity data	260	3.08	2.20	2.00	−4.95	0.31***
Information from a digital wallet (such as PayPal, Google Wallet, Visa Checkout, etc.)	259	2.96	2.16	2.00	−5.75	0.36***

Note:

*** $p < 0.001$.; Responses were measured on Likert-type scales of 1–7 (higher numbers indicate more likely to occur without knowledge or without a warrant).

warrant for CSLI information), participants felt their privacy would be less violated by a police search of the records of cell-location data than for a search of their recent email messages and older email messages (see Table 11). There also was a significant difference between likelihood of consenting to a police search of the records of locations tracked by their cell phone and recent email messages, such that participants reported being less likely to consent to a search of their recent emails than to location tracking on their cell phones. However, there was no significant difference between likelihood of consenting to a police search of the records of locations tracked by their cell phone and older email messages (see Table 11). Additionally, participants rated more likely that the police could search the records of locations they have been as tracked by their cell phone than either the contents contained in their recent email messages, or older email messages, without their knowledge (see Table 12). The same pattern emerged for ratings of how likely the police could conduct a warrantless search of the records of locations they have been as tracked by their cell phone than of their recent email messages, or older email messages (see Table 12).

TABLE 10 Expectations of privacy (CSLI versus emails) non-content versus content information

	Descriptives				Wilcoxon signed rank test	
	N	Mean	SD	Median	Wilcoxon Z	Effect size <i>r</i>
Locations you have been, as tracked by your personal cell phone (CSLI)	260	4.81	1.98	5.00	—	—
Recent email messages (stored for less than 180 days)	260	5.58	1.66	6.00	−5.95	0.37***
Older email messages (stored for more than 180 days)	259	5.53	1.57	6.00	−5.45	0.34***

Note:

*** $p < 0.001$.; Responses were measured on Likert-type scales of 1–7 (higher numbers indicate more privacy, violation, or likely to consent, occur without knowledge, or occur without a warrant).

TABLE 11 Violation of privacy and likelihood of consent for police search (CSLI versus emails) non-content versus content information

	Descriptives				Wilcoxon signed rank test	
	N	Mean	SD	Median	Wilcoxon Z	Effect size <i>r</i>
<i>Violation of privacy</i>						
Locations you have been, as tracked by your personal cell phone (CSLI)	259	5.66	1.65	6.00	—	—
Recent email messages (stored for less than 180 days)	260	5.98	1.62	7.00	−3.65	0.23***
Older email messages (stored for more than 180 days)	260	5.91	1.66	7.00	−2.62	0.16**
<i>Likelihood of consent</i>						
Locations you have been, as tracked by your cell phone (CSLI)	260	3.40	2.28	3.00	—	—
Recent Email messages (stored for less than 180 days)	260	3.15	2.23	3.00	−2.21	0.14*
Older Email messages (stored for more than 180 days)	260	3.18	2.25	4.00	−1.86	0.11

Note:

* $p < 0.05$.; ** $p < 0.01$.; *** $p < 0.001$.; Responses were measured on Likert-type scales of 1–7 (higher numbers indicate more privacy violation or likely to consent).

3.4 | Privacy expectations and perceptions of searches for information stored on devices versus the Cloud

The Supreme Court in *Riley* highlighted that much of the extensive information accessible on a cell phone is also now uploaded to Cloud storage – another third-party context. Differences between the same types of information stored on a personal cell phone and on personal Cloud storage were examined with Wilcoxon signed-rank tests. Based on the opinion in *Riley*, it was hypothesized that participants would expect more privacy and find searches more intrusive when they were asked about information stored on their cell phone as opposed to their Cloud storage.

3.4.1 | Cell phone device versus backup in the Cloud

As hypothesized by the *Riley* Court, participants reported expecting more privacy for their physical cell phone device than for a back-up of all the information contained therein stored in the Cloud. Contrary to the hypothesis, however,

TABLE 12 Ability for police to search without the searchee's knowledge or a warrant (CSLI versus emails) non-content versus content information

	Descriptives				Wilcoxon signed rank test	
	N	Mean	SD	Median	Wilcoxon Z	Effect size <i>r</i>
<i>Ability to search without knowledge</i>						
Locations you have been, as tracked by your cell phone (CSLI)	259	4.64	1.95	5.00	—	—
Recent email messages (stored for less than 180 days)	258	3.74	2.11	4.00	−5.87	0.37***
Older email messages (stored for more than 180 days)	260	3.84	2.16	4.00	−5.20	0.32***
<i>Ability to search without a warrant</i>						
Locations you have been, as tracked by your cell phone (CSLI)	259	3.62	2.22	4.00	—	—
Recent Email messages (stored for less than 180 days)	260	3.12	2.10	3.00	−3.42	0.01**
Older Email messages (stored for more than 180 days)	259	3.16	2.10	5.00	−3.18	0.20**

Note:

** $p < 0.01$; *** $p < 0.001$; Responses were measured on Likert-type scales of 1–7 (higher numbers indicate more likely to occur without knowledge or require a warrant).

there was not a significant difference in how violated participants would feel if the police were to search their cell phone device or a backup stored in the Cloud. At the same time, they reported being more likely to consent to the search of the device than a backup of their device stored in the Cloud. They thought it was less likely that the police could search their physical cell phone device than back-ups of their cell phone data stored in the Cloud without their knowledge or without a warrant (see Table 13).

TABLE 13 Expectations of privacy and perceptions of police search (stored on device versus Cloud) device or backup of data

	Cell phone (<i>device</i>)				Device back-up (<i>stored in Cloud</i>)				Wilcoxon signed rank test	
	N	Mean	SD	Median	N	Mean	SD	Median	Wilcoxon Z	Effect size <i>r</i>
Expected privacy	259	5.50	1.53	6.00	258	4.78	2.15	5.00	−4.78	0.30***
Violation of privacy	260	5.82	1.52	6.00	257	5.74	1.73	7.00	−.048	0.003
Likelihood of consent	259	3.34	3.21	3.00	254	3.07	2.24	2.00	−2.41	0.15*
Ability to search without knowledge	260	3.64	2.023	4.00	258	4.20	2.08	2.00	−3.72	0.23***
Ability to search without a warrant	259	3.10	2.13	3.00	257	3.44	2.23	3.00	−2.59	0.16**

Note:

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$; Responses were measured on Likert-type scales of 1–7 (higher numbers indicate more privacy, violation, or likely to consent, occur without knowledge, or occur with a warrant).

3.4.2 | Photos or videos

Consistent with hypothesis and the *Riley* opinion, participants reported expecting more privacy and feeling that their privacy would be more violated by a police search of photos or videos stored on their cell phone than a search of that data stored in the Cloud. However, they were equally likely to consent to a search of photos or videos stored on their device and in the Cloud. They thought that it was less likely that the police could search a cell phone device for photos or videos without their knowledge or without a warrant (see Table 14).

3.4.3 | Electronic communications

Consistent with hypothesis and the *Riley* opinion, participants reported expecting more privacy and feeling their privacy would be more violated by a police search of text messages stored on their personal cell phone device than when those same communications were stored in the Cloud. However, people reported being equally unlikely to consent to a police search regardless of whether it would be conducted on their personal device or remotely in the Cloud. Similarly, whether the police search was on a device or in the Cloud did not impact perceptions that the police could search that information without their knowledge or without a warrant (see Table 15).

4 | DISCUSSION

Technology is advancing at an increasingly fast pace, and the increasing and almost ubiquitous use of smart phones is an example of how we rely on technology in our daily lives. As a reflection of the importance of cell phones in today's world, the Supreme Court has recently grappled with the privacy related to this technology in a series of cases. Prior research had already accumulated consistent evidence showing that lay expectations of privacy and reasonableness tend to differ from those of the courts in certain aspects for both physical and electronic places, papers, and effects. However, that previous research had not directly examined how privacy expectations and perceptions of searches are related to cell phones, cell phone location data, and other digital sources of information. The purpose

TABLE 14 Expectations of privacy and perceptions of police search (stored on device versus Cloud). Photos or videos

	Photos or videos (<i>locally stored on device</i>)				Photos or videos (<i>stored in Cloud</i>)				Wilcoxon signed rank test	
	N	Mean	SD	Median	N	Mean	SD	Median	Wilcoxon Z	Effect size <i>r</i>
Expected privacy	257	5.65	1.61	6.00	257	4.72	2.12	5.00	−6.59	0.41***
Violation of privacy	260	5.94	1.48	7.00	259	5.67	1.69	6.00	−2.41	0.15*
Likelihood of consent	260	3.13	2.17	3.00	258	3.15	2.20	2.50	−0.27	0.01
Ability to search without knowledge	258	3.64	2.10	4.00	257	4.36	2.01	5.00	−4.60	0.29***
Ability to search without a warrant	258	3.10	2.23	2.00	259	3.41	2.20	3.00	−2.78	0.17**

Note:

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$; Responses were measured on Likert-type scales of 1–7 (higher numbers indicate more privacy, violation, or likely to consent, occur without knowledge, or occur without a warrant).

TABLE 15 Expectations of privacy and perceptions of police search (stored on device versus Cloud). Text messages

	Text messages (locally stored on device)				Text messages (stored in Cloud)				Wilcoxon signed rank test	
	N	Mean	SD	Median	N	Mean	SD	Median	Wilcoxon Z	Effect size <i>r</i>
Expected privacy	259	5.48	1.64	6.00	258	4.68	2.09	5.00	-5.66	0.35***
Violation of privacy	258	6.03	1.52	7.00	259	5.73	1.65	7.00	-2.91	0.18**
Likelihood of consent	259	3.24	2.21	3.00	257	3.09	2.24	2.00	-1.57	0.10
Ability to search without knowledge	260	4.15	2.07	4.00	257	4.32	2.06	5.00	-1.42	0.09
Ability to search without a warrant	259	3.27	2.27	3.00	258	3.42	2.20	3.00	-1.49	0.09

Note:

** $p < 0.01$; *** $p < 0.001$; Responses were measured on Likert-type scales of 1–7 (higher numbers indicate more privacy, violation, or likely to consent, occur without knowledge, or occur with a warrant).

of this research was to examine whether laypersons' expectations of privacy and perceptions of searches for cell phone location-tracking data and other informational items stored on a cell phone were consistent with the Court's analysis in these cases.

As would be expected with an MTurk sample, our respondents were frequent users of technology devices and were therefore an informed group of whom to ask our questions. They also were generally protective of their privacy and not especially willing to share private information on their cell phone devices, which is consistent with the high level of privacy expectations found for cell phones by Fradella et al. (2011). The high expectations of privacy observed for information stored on a cell phone also is consistent with the Supreme Court's reasoning in *Riley* that smart phones contain a large amount of private information spanning many aspects of daily life.

In the *Carpenter* and *Riley* opinions, the Supreme Court reasoned that certain types of data generated by cell phones and the vast amount and type of information stored on cell phones raise issues of Fourth Amendment protection. One question raised by these decisions is whether the type of information or its likely location on the physical device is a more important factor predicting laypersons' privacy expectations that could be taken into account in court decision making. Our results provide some information about this type-versus-device question. Consistent with previous research (Kugler & Strahilevitz, 2016; Smith et al., 2016) demonstrating that people have high privacy expectations for location-tracking information in general, our participants also had high privacy expectations for location information in general. However, they expected more privacy, protection in the form of warrants, and notice of police search activity in the form of knowledge when that location information was derived from cell phone location data as opposed to a public traffic camera or GPS tracking. They also reported less likelihood of voluntarily providing CSLI information. Previous research (Slobogin & Schumacher, 1993; Blumenthal et al., 2009) stressed the importance of consent, implied or otherwise, in laypersons' evaluations of the intrusiveness of a search. Participants here reported being unlikely to provide consent to search CSLI, which indicates that laypersons place CSLI data in a more protected category than other forms of location tracking they are likely to experience in their daily lives. People's privacy expectations may be more dependent not so much on the type of information collected but rather on the source and location of that information; specifically, location information on the cell phone device may be considered more intimate and detailed than other types of location information. These perceptions are consistent with the reasoning in *Carpenter* that CSLI data, even though it is released to a third party, provides enough private information to trigger Fourth Amendment protections.

Even though our participants felt that CSLI data was more deserving of protection than other types of location data, in some respects they felt other content on their cell phones (i.e., pictures/videos, content of texts, call history information, calendar information, health/activity data, emails, and their digital wallet) should be entitled to even greater protection. A search of CSLI data was considered less of a privacy violation than a search of all of these items except call history or health/activity information, and was perceived as more likely to occur without a warrant than all of those types of cell phone information except call histories (which are incidentally also stored with phone companies in a similar manner to CSLI).

Similar patterns of difference between perceptions of CSLI data and other cell phone information occurred in connection with queries about consent and notice of searches. Laypersons may be less likely to voluntarily consent to a search for information likely to be stored locally on a cell phone including photos, texts, and wallets than to disclosure of CSLI information. They may be more likely to voluntarily provide information about call histories, calendars, health data, and notes. CSLI data is perceived as more likely to be searched without the target's knowledge than all other items except for call history, which was perceived as equally likely. These results also indicate that the *Riley* Court's reasoning that all cell phone content should enjoy Fourth Amendment protection in the context of a search incident to arrest is consistent with how people view their cell phones. These results also indicate that courts may consider expanding Fourth Amendment protections for all data collected on cell phones.

Another question raised by the *Carpenter* opinion and by the SCA is whether laypersons make distinctions among different types of information that are treated equally by the SCA and therefore potentially by the courts. Our results indicate that participants do distinguish between at least two similarly treated categories of information under the SCA: emails and CSLI. Our participants perceived CSLI as less private, less violating if searched, and more likely to be searched without notice or a warrant. However, people reported being equally unlikely to consent to a search of either CSLI or email information, indicating that they would be reluctant to voluntarily release either type of information to the police in a search. Overall, laypersons' perceptions that emails should be given Fourth Amendment protection in the form of a warrant to search is consistent with the previous research indicating that people believe the police would need probable cause to search their emails (Scott-Hayward et al., 2015). Based on this research, courts may want to consider revisiting SCA-permitted searches of other types of non-CSLI information.

If the courts are going to grapple more extensively with any differences in Fourth Amendment protections for cell phone information stored on the actual device versus cell phone information backed up to Cloud storage, our results comparing privacy expectations and perceptions of police searches of these items might help inform courts about the types of expectation laypersons have. Previous research by Chao et al. (2018) found that potential searches of Cloud storage were perceived as intrusive, and our results also demonstrate that participants have privacy expectations for Cloud storage. However, laypersons view Cloud storage differently and generally less likely to trigger Fourth Amendment protections than information stored locally on their cell phones. Although participants felt equally violated by a search of the entire contents of their phone and a complete backup of that phone on the Cloud, participants felt more violation of their privacy from a potential search of the photos/videos and texts on their actual device. These effects are consistent with the *Riley* Court's concern that identifying the privacy interests implicated by a device search is more challenging for an internet-connected device that utilizes Cloud-computing technology to remotely store some indeterminate amount of its users' data (p. 2491).

One possible explanation of why people make these distinctions is psychological distance. Previous research has established that physically touching an object increases feelings of ownership and positive valuation of the object (Peck & Shu, 2009; Ping, Dhillon, & Beilock, 2009) and that physical distance decreases psychological connectedness (Henderson, Wakslak, Fujita, & Rohrbach, 2011; Williams & Bargh, 2008). It is possible that information contained on the physical cell phone, carried around obsessively (as noted in *Riley*), is valued more because of its physical connection to the user. Seen from this viewpoint, the results distinguishing between privacy expectations for the Cloud are similar to the results for cell phone location data and cell phone call histories in that they all originate from the cell phone but are stored remotely. Other informational items such as photos, texts, emails, wallet contents, and health information may be viewed as more locally stored and therefore psychologically "closer," even when they are also

stored remotely. Future research should investigate whether psychological distance is a factor that contributes to laypersons' expectations about Fourth Amendment protections in a manner that should be considered by courts when reasoning about remote storage connected to physical devices in the future.

Although our research is limited by the non-representativeness of MTurk samples, the purpose of the current research was not to speak to general population beliefs, but rather to examine comparisons of beliefs about privacy, police surveillance, and technology. In other words, we are not claiming that the current research demonstrates public opinion on the topic, but it does shed light on how certain experiences with and beliefs about technology can influence behaviors with that technology and expectations of privacy for the technology. As Kugler and Strahilevitz (2016) note, MTurk samples are questionable for making claims about base rates but can be useful for examining the "relative intrusiveness of searches" (p. 22, fn. 29). Such interactions of beliefs are important to consider in developing more nuanced explanations and examining these issues with representative samples as researchers and the courts grapple with understanding lay conceptions of privacy. In addition, because MTurk samples are generally more technologically savvy than a representative sample (Kugler & Strahilevitz, 2016), our sample could also be thought of as providing a look into the future. As scholars (e.g., Tokson, 2016) have suggested, increased technological savviness could affect expectations of privacy.

In order to maintain participants' attention, we presented them with only short descriptions of the technology they were asked to rate. It would thus be desirable to replicate these findings with more detailed materials that would be more realistic to true search and privacy expectation experiences. Even better would be to examine these issues using an experimental design where the type of cell phone information searched was manipulated between subjects. Additionally, considering the importance placed on the size, or pervasiveness of the records in the *Carpenter* analysis and the length of time in *Jones*, it may be important to provide more information about the quantity of data or records implicated and the length of time involved in a search. Despite these limitations, the current research provides important insights into how laypersons view the privacy of the data they generate involuntarily and voluntarily when using the ubiquitous smart phone.

5 | CONCLUSION

Police today must adapt quickly to a world of vast and constant technological advancement. Unfortunately, the police are interacting with this technology as it emerges while the courts take months and even years to address each new piece of technology, and do so in ways that do not always seem consistent or in step with laypeople's expectations of privacy. This disconnect has resulted in uncertainty about the extent to which the Fourth Amendment should apply to information shared in various emerging technology contexts. Empirical research such as the current study could aid courts in determining broader factors to consider in their Fourth Amendment decision making, such as whether the information is stored locally or remotely, and whether laypersons' privacy expectations in specific types of emerging technologies should trigger their Fourth Amendment protection.

ACKNOWLEDGEMENTS

This research was funded in part by Mary W. Johnson Faculty Research Awards from Scripps College. Elements of this research have been presented at the annual meeting of the American Psychology-Law Society. The authors wish to thank Katherine Hazen and Kaitlyn Wilson for their help with this research.

REFERENCES

- Bector, S. (2009). Your laptop, please: The search and seizure of electronic devices at the United States border. *Berkeley Technology Law Journal*, 24(1), 695–718.
- Blumenthal, J. A., Adya, M., & Mogile, J. (2009). The multiple dimensions of privacy: Testing lay "expectations of privacy." *University of Pennsylvania Journal of Constitutional Law*, 11, 331–373.

- California v. Ciraolo, 476 U.S. 207 (1986).
- California v. Greenwood, 486 U.S. 35 (1988).
- Carpenter v. United States, 131 S.Ct. 2206 (2018).
- Chanenson, S. L. (2004). Get the facts, Jack! Empirical research and the changing constitutional landscape of consent searches. *Tennessee Law Review*, 71, 399–470.
- Chao, B., Durso, C., Farrell, I., & Robertson, C. (2018). Why courts fail to protect privacy: Race, age and bias, and technology. *California Law Review*, 106, 264–324.
- City of Indianapolis v. Edmond, 531 U.S. 32 (2000).
- DeZwart, M., Humphreys, S., & Van Dissel, B. (2014). Surveillance, big data and democracy: Lessons for Australia from the US and UK. *University of New South Wales Law Journal*, 37, 713–747.
- Ex parte Jackson, 96 U.S. 727 (1877).
- Fradella, H. F., Morrow, W. J., Fischer, R. G., & Ireland, C. (2011). Quantifying Katz: Empirically measuring "reasonable expectations of privacy" in the Fourth Amendment context. *American Journal of Criminal Law*, 38, 289–373.
- Henderson, M., Waksalak, C., Fujita, K., & Rohrbach, J. (2011). Construal level theory and spatial distance: Implications for mental representation, judgment, and behavior. *Social Psychology*, 42(3), 165–173. <http://doi.org/10.1027/1864-9335/a000060>
- Illinois v. Caballes, 543 U.S. 405 (2005).
- Katz v. United States, 389 U.S. 347 (1967).
- Kees, J., Berry, C., Burton, S., & Sheehan, K. (2017). An analysis of data quality: Professional panels, student subject pools, and Amazon's Mechanical Turk. *Journal of Advertising*, 46(1), 141–155. <http://doi.org/10.1080/00913367.2016.1269304>
- Kerr, O. S. (2004). A user's guide to the Stored Communications Act, and a legislator's guide to amending it. *George Washington Law Review*, 72(6), 1208–1243.
- Kerr, O. S. (2010). Applying the Fourth Amendment to the internet: A general approach. *Stanford Law Review*, 62(4), 1005–1038.
- Kerr, O. S. (2012). The mosaic theory of the Fourth Amendment. *Michigan Law Review*, 111, 311–354.
- Kerr, O. S. (2015). Katz has only one step: The irrelevance of subjective expectations. *University of Chicago Law Review*, 82(1), 113–134.
- Kerr, O. S. (in press). Implementing Carpenter. In *The digital fourth amendment*. Oxford University Press. USC Law Legal Studies Paper 18-29
- Kugler, M. B., & Strahilevitz, L. J. (2016). Actual expectations of privacy, Fourth Amendment doctrine, and the mosaic theory. *Supreme Court Review*, 2015(1), 205–263.
- Kugler, M. B., & Strahilevitz, L. J. (2017). The myth of Fourth Amendment circularity. *University of Chicago Law Review*, 84, 1747–1812.
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336–355. <https://doi.org/10.1287/isre.1040.0032>
- Olmstead v. United States, 277 U.S. 438 (1928).
- Paolacci, G., & Chandler, J. (2014). Inside the Turk: Understanding Mechanical Turk as a participant pool. *Current Directions in Psychological Science*, 23(3), 184–188. <https://doi.org/10.1177/0963721414531598>
- Peck, J., & Shu, S. B. (2009). The effect of mere touch on perceived ownership. *Journal of Consumer Research*, 36(3), 434–447.
- Pew Research Center. (2019). *Mobile fact sheet*. Washington, DC: Pew Research Center. Retrieved from <https://www.pewinternet.org/fact-sheet/mobile/>
- Ping, R. M., Dhillon, S., & Beilock, S. L. (2009). Reach for what you like: The body's role in shaping preferences. *Emotion Review*, 1(2), 140–150. <https://doi.org/10.1177/1754073908100439>
- Riley v. California, 134 S. Ct. 2473 (2014).
- Rozenshtein, A. Z. (2019). Fourth Amendment reasonableness after Carpenter. *Yale Law Journal Forum*, 128, 943–960.
- Schmerber v. California, 384 U.S. 757 (1966).
- Scott-Hayward, C. S., Fradella, H. F., & Fischer, R. G. (2015). Does privacy require secrecy: Societal expectations of privacy in the digital age. *American Journal of Criminal Law*, 43, 19–60.
- Sheehan, K. B. (2018). Crowdsourcing research: Data collection with Amazon's Mechanical Turk. *Communication Monographs*, 85, 140–156. <https://doi.org/10.1080/03637751.2017.1342043>
- Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602 (1989).
- Slobogin, C. (2002). Public privacy: Camera surveillance of public places and the right to anonymity. *Mississippi Law Journal*, 72, 213–315.
- Slobogin, C. (2007). *Privacy at risk: The new government surveillance and the Fourth Amendment*. Chicago, IL: University of Chicago Press.

- Slobogin, C. (2008). Government data mining and the Fourth Amendment. *University of Chicago Law Review*, 75, 317–341.
- Slobogin, C., & Schumacher, J. E. (1993). Reasonable expectations of privacy and autonomy in Fourth Amendment cases: An empirical look at "understanding recognized and permitted by society." *Duke Law Journal*, 42, 727–775. <https://doi.org/10.2307/1372714>
- Smith, A., Madden, S., & Barton, R. P. (2016). An empirical examination of societal expectations of privacy in the digital age of GPS, cell phone towers, & drones. *Albany Law Journal of Science and Technology*, 26, 111–142.
- Smith v. Maryland, 442 U.S. 735 (1979).
- Stored Communications Act, 18 U.S.C. §§2701–2712 (1986).
- Taslitz, A. E. (2006). *Reconstructing the Fourth Amendment: A history of search and seizure, 1789–1868*. New York: New York University Press.
- Tokson, M. (2016). Knowledge and Fourth Amendment privacy. *Northwestern University Law Review*, 111, 139–204.
- United States v. Barrows, 481 F.3d 1246 (2007).
- United States v. David, 756 F. Sup 1385 (1991).
- United States v. Jacobsen, 466 U.S. 109 (1984).
- United States v. Jones, 565 U.S. 400 (2012).
- United States v. Knotts, 460 U.S. 276 (1983).
- United States v. Miller, 425 U.S. 435 (1976).
- United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).
- Walter, S. L., Seibert, S. E., Goering, D., & O'Boyle, E. H. (2019). A tale of two sample sources: Do results from online panel data and conventional data converge? *Journal of Business and Psychology*, 34(4), 425–452. <http://doi.org/10.1007/s10869-018-9552-y>
- Williams, L., & Bargh, J. (2008). Keeping one's distance: The influence of spatial distance cues on affect and evaluation. *Psychological Science*, 19(3), 302–308. <https://doi.org/10.1111/j.1467-9280.2008.02084.x>
- Wylie, L. E., Hazen, K. P., Hoetger, L. A., Haby, J. A., & Brank, E. M. (2018). Four decades of the journal *Law and Human Behavior*: A content analysis. *Scientometrics*, 115(2), 655–693. <https://doi.org/10.1007/s11192-018-2685-y>

How to cite this article: Marshall EW, Groscup JL, Brank EM, Perez A, Hoetger LA. Police surveillance of cell phone location data: Supreme Court versus public opinion. *Behav Sci Law*. 2019;37:751–775. <https://doi.org/10.1002/bsl.2442>

Copyright of Behavioral Sciences & the Law is the property of John Wiley & Sons, Inc. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.