2026 SA 07

People of the State of San Andreas, Plaintiff-Appellant,

v.

Marcus J. Cunningham, Defendant-Appellee.

No. 25CA3451.

Supreme Court of San Andreas.

February 27, 2026.

Interlocutory Appeal from the District Court Alameda County District Court Case No. 23CR1282 Honorable Silvia Lopez, Judge.

Attorneys for Plaintiff-Appellant: Rebecca C. Navarro, Attorney General, State of San Andreas. Elizabeth E. Morse, District Attorney Castro Valley, San Andreas.

Attorneys for Defendant-Appellee: Tracy C. McIntosh, Raquel R. Rivera, McIntosh Law Union City, San Andreas.

En Banc.

JUSTICE CORTEZ delivered the Opinion of the Court, in which CHIEF JUSTICE MORGAN, JUSTICE MIDDLETON, JUSTICE HALL, JUSTICE MCDOWELL, and JUSTICE SPRINGER joined. JUSTICE BENNETT delivered the Concurring Opinion.

OPINION OF THE COURT

CORTEZ, Justice.

¶1 This case presents a question that sits at the center of modern constitutional law: whether law enforcement officers may obtain extensive digital location information from a private technology company without first securing judicial authorization. As investigative practices increasingly rely upon data collected by private platforms, courts must determine whether constitutional protections developed for physical searches extend with equal force into the digital environment. The defendant contends that acquisition of his rideshare location history without a warrant violated the privacy guarantees of the San Andreas Constitution. We agree.

¶2 The Constitution of San Andreas provides unusually explicit protection for personal privacy. Article II, Section 11 declares that the right of the people to be secure against

governmental and corporate intrusion into their private affairs is inviolable and expressly forbids disclosure of personal information absent explicit consent or a warrant issued upon probable cause. Unlike constitutional provisions framed solely in general language, Section 11 directly addresses the modern reality that private corporations routinely collect and maintain vast repositories of personal data capable of revealing intimate details of daily life.

¶3 Article II, Section 6 reinforces this command by guaranteeing security against unreasonable searches and seizures and by expressly extending constitutional protection to communications, data, and electronic records. The inclusion of electronic information within the constitutional text reflects a deliberate recognition that privacy interests do not diminish merely because personal information exists in digital rather than physical form. Together, Sections 6 and 11 establish a comprehensive constitutional framework governing governmental access to personal data.

¶4 The facts underlying this case are largely undisputed. Investigators obtained approximately three weeks of historical rideshare records associated with Cunningham's account through a prosecutorial request directed to the rideshare company. The request sought detailed information including pickup and drop-off locations, timestamps, and GPS routing data sufficient to reconstruct Cunningham's movements over an extended period. No judicial warrant was sought prior to acquisition of the records.

¶5 The disclosed data allowed investigators to place Cunningham in geographic proximity to multiple alleged crime scenes and became a central component of the prosecution's evidentiary theory. Cunningham moved to suppress the information, arguing that compelled disclosure of detailed location history constituted a search requiring prior judicial authorization under the state constitution.

¶6 The district court denied suppression, concluding that the information constituted ordinary business records maintained by a private company and therefore fell outside constitutional protection. The Court of Appeals affirmed, relying upon traditional federal precedent suggesting that information voluntarily conveyed to third parties carries diminished privacy expectations. We granted review because those conclusions raise substantial questions concerning the independent meaning of Article II, Sections 6 and 11.

¶7 The State urges this Court to apply the traditional third-party doctrine developed under federal Fourth Amendment jurisprudence. Under that doctrine, information disclosed to a business entity may be obtained by law enforcement without a warrant because the individual assumes the risk of further disclosure. That reasoning emerged in an era when business records consisted largely of limited transactional information rather than comprehensive digital surveillance.

¶8 The constitutional text before us, however, rejects the assumption that corporate possession extinguishes personal privacy. Section 11 expressly regulates both governmental and corporate intrusion into private affairs and prohibits disclosure of

personal information absent consent or judicial authorization. The provision reflects a constitutional judgment that privacy rights follow the individual, not the physical location of stored information.

¶9 Participation in modern society frequently requires individuals to share information with service providers in order to obtain transportation, communication, employment, or financial services. The practical necessity of using digital platforms undermines the notion that disclosure to corporations represents meaningful voluntary relinquishment of privacy rights. Constitutional protections cannot depend upon abstention from ordinary technological life.

¶10 The records obtained in this case were not limited transactional receipts reflecting isolated commercial activity. Rather, they constituted an aggregated record of Cunningham's movements across time and space, permitting investigators to reconstruct patterns of travel, associations, habits, and routines extending far beyond the scope of any single rideshare trip.

¶11 Location information of this nature possesses an inherently revealing character. Repeated travel data may disclose visits to medical providers, participation in religious services, attendance at political gatherings, personal relationships, and other activities traditionally regarded as among the most private aspects of individual life. Access to such data enables retrospective surveillance of a breadth previously achievable only through sustained physical tracking.

¶12 The constitutional danger arises not merely from individual data points but from aggregation. When combined over weeks or months, digital location records create an intimate portrait of personal existence. The ability of the State to obtain such information without judicial oversight would fundamentally alter the balance between citizen privacy and governmental power.

¶13 Article II, Section 11 directly addresses this concern by prohibiting disclosure of personal information unless explicit consent has been granted or a valid warrant has issued upon probable cause. The constitutional language leaves no room for implied exceptions based solely upon corporate custody of the data.

¶14 The State argues that Cunningham consented to disclosure by using the rideshare platform. That argument misunderstands the constitutional requirement of explicit consent. Agreement to receive transportation services does not constitute authorization for governmental access to historical movement records for criminal investigation purposes.

¶15 Consent sufficient to waive constitutional protection must be knowing, voluntary, and directed toward the governmental intrusion at issue. Nothing in this record suggests Cunningham expressly authorized disclosure of his location history to law enforcement authorities.

¶16 Nor may the State evade constitutional scrutiny by directing requests to corporations rather than individuals themselves. Constitutional safeguards would become illusory if governmental actors could obtain protected information indirectly from private intermediaries without judicial approval.

¶17 Section 6 independently compels recognition that digital data constitutes a protected object of search. The explicit extension of constitutional protection to electronic records demonstrates that the framers intended warrant requirements to apply fully within technological environments.

¶18 Acquisition of Cunningham's location history therefore constituted a search within the meaning of the San Andreas Constitution because it invaded a protected sphere of personal privacy through compelled disclosure of electronic records.

¶19 Searches conducted without a warrant are presumptively unreasonable unless justified by recognized exceptions grounded in necessity or exigency. The State identifies no emergency circumstances, consent, or other exception capable of overcoming that presumption.

¶20 Administrative efficiency or investigative convenience cannot substitute for constitutional compliance. The warrant requirement exists precisely to ensure that decisions authorizing intrusive surveillance are made by neutral judicial officers rather than investigators engaged in the competitive enterprise of law enforcement.

¶21 Requiring a warrant does not impede legitimate criminal investigation. Courts routinely provide expedited warrant procedures, including electronic submissions and after-hours judicial review, ensuring that probable cause determinations may be obtained without undue delay.

¶22 What the Constitution demands is accountability prior to intrusion. Judicial authorization ensures that surveillance occurs only where sufficient factual justification exists rather than through exploratory data collection.

¶23 Permitting warrantless acquisition of corporate location databases would effectively grant law enforcement the ability to reconstruct the historical movements of any citizen whose activities generated digital records. Such authority would approach generalized surveillance inconsistent with constitutional liberty.

¶24 The framers of Article II recognized that technological change expands governmental capability and therefore embedded privacy protections capable of adapting to evolving investigative tools. Sections 6 and 11 function together to prevent erosion of personal autonomy through technological intermediaries.

¶25 The State's proposed rule would render those protections dependent upon corporate data practices rather than constitutional command. Privacy rights would fluctuate according to business models rather than enduring principles of liberty.

¶26 Our duty is not to preserve investigative convenience but to enforce constitutional guarantees as written. Where the Constitution requires a warrant, courts are not free to substitute lesser protections.

¶27 We therefore conclude that individuals retain a constitutionally protected privacy interest in historical rideshare location data notwithstanding corporate storage of that information.

¶28 Government acquisition of such data without prior judicial authorization constitutes an unreasonable search under Article II, Sections 6 and 11.

¶29 Because investigators failed to obtain a warrant supported by probable cause before compelling disclosure, the search conducted in this case violated the San Andreas Constitution.

¶30 The improperly obtained evidence formed a substantial portion of the prosecution's case linking Cunningham to the charged offenses and cannot be regarded as harmless.

¶31 Suppression of the evidence is therefore required to preserve the integrity of constitutional protections and to deter future warrantless acquisition of protected digital information.

¶32 Today's decision does not prohibit law enforcement from accessing digital records. It requires only that investigators comply with the constitutional process long required for entry into homes, seizure of papers, and interception of communications.

¶33 The Constitution guarantees that advancing technology will not diminish fundamental privacy rights simply because personal information is stored electronically rather than physically possessed.

¶34 Judicial oversight remains the mechanism through which liberty and investigation coexist within constitutional order.

¶35 Because the State obtained Cunningham's digital location history without a warrant, the acquisition constituted an unlawful search.

¶36 The judgment of the Court of Appeals is reversed, Cunningham's conviction is vacated, and the matter is remanded for proceedings consistent with this opinion.

I. Facts and Procedural History

¶37 The charges in this case arose from an investigation conducted by law enforcement officers in Alameda County concerning a series of late-night commercial burglaries occurring over a period of several weeks. Investigators identified similarities among the incidents, including timing, method of entry, and geographic proximity, leading officers to believe that the offenses were committed by the same individual or coordinated group operating within a defined area of the county.

¶38 During the course of the investigation, officers developed Marcus Cunningham as a potential suspect based upon witness descriptions and circumstantial evidence placing an individual matching Cunningham's appearance near one of the affected businesses shortly before a reported break-in. Investigators subsequently sought to determine Cunningham's movements during the relevant time period in order to assess whether his travel patterns corresponded with the locations and timing of the burglaries.

¶39 Rather than seeking judicial authorization, investigators directed a formal records request to a rideshare company known to have been used by Cunningham. The request sought historical account information associated with Cunningham's user profile, including trip histories, pickup and drop-off locations, timestamps, and GPS-generated route data covering approximately three weeks preceding the charged offenses.

¶40 The rideshare company complied with the request and produced the requested records without requiring presentation of a warrant or notifying Cunningham prior to disclosure. Law enforcement officers thereafter analyzed the data and constructed a timeline purporting to show Cunningham traveling to or near several commercial locations shortly before reported burglaries occurred.

¶41 Investigators relied heavily upon this reconstructed movement history to support probable cause determinations and to corroborate other investigative leads. The location data was later incorporated into investigative reports and presented to prosecutors as evidence linking Cunningham to the charged offenses.

¶42 Cunningham was subsequently charged in the District Court of Alameda County with multiple counts of burglary and conspiracy under state law. Prior to trial, defense counsel moved to suppress all evidence derived from the rideshare records, arguing that acquisition of detailed historical location data without a warrant constituted an unlawful search in violation of Article II, Sections 6 and 11 of the San Andreas Constitution.

¶43 The district court conducted an evidentiary hearing at which investigators testified regarding the manner in which the records were obtained. The State argued that the information constituted ordinary business records voluntarily conveyed to a private company and therefore fell outside constitutional warrant requirements. The defense contended that aggregated digital location data revealed intensely private information and remained constitutionally protected notwithstanding corporate storage.

¶44 The district court denied the motion to suppress, concluding that Cunningham lacked a protected privacy interest in records maintained by the rideshare company and that law enforcement's acquisition of those records did not constitute a search requiring judicial authorization. The court reasoned that existing precedent governing third-party business records permitted disclosure through prosecutorial request.

¶45 Following denial of the suppression motion, the rideshare location data was admitted at trial and presented by the prosecution as evidence establishing Cunningham's presence near several crime scenes. The jury returned verdicts of guilty on the charged offenses, and Cunningham was subsequently sentenced in accordance with statutory guidelines.

¶46 Cunningham appealed his conviction to the Court of Appeals, renewing his argument that warrantless acquisition of historical location data violated the privacy protections guaranteed by the San Andreas Constitution. The Court of Appeals affirmed the conviction, holding that the defendant possessed no reasonable expectation of privacy in information voluntarily transmitted to a commercial service provider and declining to recognize heightened constitutional protection for digitally stored location information absent legislative action.

¶47 Cunningham thereafter petitioned this Court for review, asserting that Article II, Sections 6 and 11 provide independent and broader privacy protections than federal doctrine and require a warrant before law enforcement may compel disclosure of detailed electronic location records.

¶48 We granted review to resolve whether acquisition of historical rideshare location data without a warrant constitutes an unlawful search under the Constitution of San Andreas and to clarify the scope of constitutional privacy protections applicable to digitally stored personal information.

II. The Pesky Constitutional Hurdles

¶49 The State's argument encounters an obstacle neither subtle nor newly discovered. It is found not in obscure precedent nor unsettled doctrine, but in the text of the Constitution itself. Article II, Section 6 provides that the people shall be secure against unreasonable searches and seizures and further declares—without qualification—that this protection extends to any communication, data, or electronic record. That language is neither aspirational nor symbolic. It is binding law. Yet the State's position proceeds as though this provision were optional guidance rather than constitutional command.

¶50 Section 6 resolves much of this case before interpretive analysis even begins. The provision expressly extends warrant protection beyond physical spaces to digital information. The framers—and more importantly, the people who ratified this Constitution—anticipated precisely the circumstance now before us: governmental acquisition of electronically stored personal data without judicial authorization. Where the

Constitution explicitly names electronic records as protected objects of search, courts are not free to pretend uncertainty exists.

¶51 There is, quite simply, a pesky and unavoidable requirement embedded in Section 6: searches require warrants. That requirement does not evaporate because information happens to reside on a server rather than in a filing cabinet, nor does it disappear because law enforcement finds it more convenient to request records from a corporation rather than present probable cause to a magistrate. Constitutional protections do not yield to administrative preference.

¶52 The State nevertheless urges this Court to treat compelled disclosure of detailed digital records as something other than a search. That argument cannot survive even casual comparison with the constitutional text. When the government demands access to an individual's electronic data for investigative purposes, it conducts precisely the type of intrusion Section 6 was written to regulate. Calling the request a "records inquiry" does not alter its constitutional character.

¶53 Even if Section 6 alone did not dispose of the matter—and it nearly does—the State confronts an additional and equally decisive provision. Article II, Section 11, ratified by the voters of San Andreas in 2020, declares that the right of the people to be secure against governmental and corporate intrusion into their private affairs is inviolable and prohibits disclosure of personal information absent explicit consent or a warrant issued upon probable cause.

¶54 Section 11 did not arise accidentally. It was adopted in direct response to growing public concern regarding the accumulation and exchange of personal data by both government and private corporations. The voters of this State chose to constitutionalize digital privacy protections in unmistakable terms. Courts are not empowered to dilute that democratic judgment through creative reinterpretation.

¶55 The State's theory would require us to conclude that although the Constitution forbids disclosure of personal information without a warrant, law enforcement may nevertheless obtain precisely that information so long as it is first stored by a corporation. Such reasoning transforms a constitutional safeguard into a procedural suggestion. The people did not ratify Section 11 to create a loophole large enough to swallow the rule.

¶56 Section 11 expressly regulates both governmental and corporate conduct because modern surveillance frequently occurs through compelled cooperation between the two. The Constitution therefore closes the very avenue the State now attempts to exploit: acquisition of private data indirectly from corporate custodians rather than directly from the individual.

¶57 To accept the State's position would require this Court to ignore not one but two constitutional provisions speaking directly to electronic data and personal information. Courts do not possess authority to suspend constitutional text when technological change

renders compliance inconvenient. The warrant requirement remains the mechanism through which liberty is preserved against expanding investigative capability.

¶58 The combined force of Sections 6 and 11 leaves no ambiguity. Electronic data is protected. Personal information may not be disclosed without consent or judicial authorization. Governmental access requires a warrant supported by probable cause. These commands are written plainly enough that their meaning does not depend upon judicial invention.

¶59 Constitutional adjudication sometimes demands careful balancing of competing interests. This is not such a case. The Constitution already performed that balancing when it extended search-and-seizure protections to electronic records and when the voters reaffirmed privacy as inviolable in 2020. Our responsibility is therefore straightforward: to enforce the Constitution as written, not to revise it in light of investigative convenience.

¶60 The State asks this Court to permit warrantless access to deeply revealing digital information despite explicit constitutional prohibition. We decline that invitation. Where the Constitution speaks clearly, judicial duty requires obedience rather than accommodation.

¶61 Sec. 6 Searches and Seizures – The right of the people to be secure in their persons, houses, papers, and possessions against unreasonable searches and seizures shall not be violated. A warrant may not be issued except upon probable cause, supported by a sworn statement, and specifically describing the place to be searched and the persons or items to be seized. This protection shall extend to any communication, data, or electronic record.

¶62 Sec. 11 Privacy – The right of the people to be secure against governmental and corporate intrusion into their private affairs is inviolable. No entity, public or private, shall collect, sell, or disclose the personal information of any individual without their explicit consent, unless a valid warrant has been issued upon probable cause in a manner prescribed by law. All healthcare and educational documents are considered confidential and shall not be released by any government or corporate entity without the explicit consent of the individual to whom they belong. This provision does not apply to disclosures required by a lawful warrant issued upon probable cause.

III. Conclusion

¶63 The question presented in this case reflects a broader constitutional challenge confronting courts in an era defined by rapid technological transformation. As methods of communication, transportation, and commerce migrate into digital platforms, vast quantities of personal information are routinely generated, stored, and maintained outside the physical possession of the individual. The Constitution of San Andreas anticipates this reality and provides clear instruction: the protections securing the people in their private affairs do not

diminish merely because personal information is held by a corporate intermediary rather than within the walls of the home.

¶64 Article II, Sections 6 and 11 together establish that digital data stands on equal constitutional footing with traditional papers and effects. Location records capable of revealing an individual's movements over extended periods implicate profound privacy interests because they allow the State to reconstruct the rhythms of daily life with precision unimaginable at the time of earlier search doctrines. Access to such information without judicial oversight would permit forms of retrospective surveillance fundamentally inconsistent with the constitutional guarantee that governmental intrusion occur only upon probable cause.

¶65 The warrant requirement serves as the constitutional boundary separating legitimate investigation from unchecked intrusion. It does not prevent law enforcement from obtaining relevant evidence, nor does it insulate criminal conduct from investigation. Rather, it ensures that the decision to invade private affairs is subjected to neutral judicial review before the intrusion occurs. That safeguard remains essential where modern technology enables the government to access deeply revealing information through a single request directed to a corporate database.

¶66 The State's argument that disclosure to a private company extinguishes constitutional protection cannot be reconciled with the express language of Article II, Section 11, which regulates both governmental and corporate handling of personal information. The Constitution does not permit privacy rights to fluctuate according to business practices or technological convenience. Personal data remains protected because it belongs to the individual whose life it reflects.

¶67 By requiring a warrant before law enforcement may compel disclosure of historical rideshare location data, today's decision preserves the balance carefully struck by the Constitution between public safety and personal liberty. The people of San Andreas remain secure not only in their homes and possessions, but also in the digital records that increasingly define modern existence. Constitutional protections endure precisely so that advances in investigative capability do not outpace the safeguards designed to restrain governmental power.

¶68 Because investigators obtained Cunningham's location history without a warrant supported by probable cause, the acquisition constituted an unlawful search under Article II, Sections 6 and 11 of the San Andreas Constitution. The evidence derived from that search must therefore be suppressed.

¶69 The judgment of the Court of Appeals is reversed, Cunningham's conviction is vacated, and this matter is remanded to the District Court for further proceedings consistent with this opinion.

CONCURRING OPINION

BENNETT, Justice.

¶70 I join the Court's opinion in full and agree that law enforcement officers must obtain a warrant supported by probable cause before compelling disclosure of an individual's historical rideshare location data. I write separately to emphasize that today's decision does not represent an expansion of constitutional privacy protections, but rather a faithful application of protections already embedded within the text and structure of the San Andreas Constitution.

¶71 Article II, Section 11 is remarkable not for its ambiguity but for its precision. Unlike many constitutional privacy provisions that require courts to infer protections through evolving interpretation, Section 11 expressly addresses governmental and corporate intrusion into private affairs and conditions disclosure of personal information upon either explicit consent or judicial authorization. The constitutional command is direct. Where personal information is disclosed to the State without consent and without a warrant, a violation occurs.

¶72 The present case illustrates why such clarity matters in the digital era. Modern life increasingly requires individuals to entrust private companies with vast quantities of personal information simply to participate in ordinary social and economic activity. Transportation services, communication platforms, financial institutions, and digital applications collectively maintain records capable of revealing far more about an individual than traditional physical searches ever could.

¶73 The State's position would effectively condition constitutional privacy upon technological abstinence. Under that view, citizens retain privacy only so long as they refrain from using modern services indispensable to daily life. The Constitution does not impose such a choice. Rights guaranteed to the people cannot depend upon withdrawal from contemporary society.

¶74 I write separately as well to underscore that the danger presented by digital location data lies not merely in isolated disclosure but in cumulative surveillance capacity. A single trip record may appear innocuous. Weeks of location history, however, allow the State to reconstruct patterns of association, belief, and behavior with extraordinary precision. Such aggregation transforms commercial data into a powerful instrument of governmental observation.

¶75 Article II, Section 6 anticipates this concern by extending search-and-seizure protections expressly to electronic records and data. That provision reflects an understanding that constitutional liberty must evolve alongside investigative capability. The Constitution protects substance rather than form; surveillance conducted through servers rather than physical tails remains surveillance nonetheless.

¶76 The State warns that requiring warrants may burden criminal investigations or delay access to useful evidence. Similar arguments have accompanied nearly every development in search-and-seizure jurisprudence. Yet constitutional structure deliberately interposes judicial oversight between suspicion and intrusion. The warrant requirement does not obstruct investigation; it legitimizes it.

¶77 Neutral judicial review serves an essential democratic function. It ensures that decisions authorizing access to deeply revealing personal information are made according to law rather than investigative expediency. Particularly where technology permits retrospective monitoring of large portions of a person's life, independent review becomes not merely advisable but indispensable.

¶78 I also emphasize that today's holding does not prohibit cooperation between private companies and law enforcement in circumstances involving true exigency. Emergencies presenting imminent threats to life or safety remain governed by well-established exceptions to the warrant requirement. Nothing in this decision prevents prompt governmental action where necessity demands it.

¶79 What the Constitution forbids is routine acquisition of comprehensive personal data through administrative request alone. Allowing such practices would gradually normalize suspicionless access to corporate databases containing intimate records of daily life, effectively transferring to the executive branch surveillance authority the Constitution reserves for judicial supervision.

¶80 The framers of Article II recognized that privacy is not limited to the home or to tangible papers but extends to the broader sphere of personal autonomy. In the twenty-first century, that sphere increasingly exists within digital systems maintained by private entities. Constitutional guarantees lose practical meaning if they fail to reach those environments.

¶81 The Court today correctly affirms that constitutional rights do not evaporate when personal information is stored electronically or entrusted to third-party service providers. The people remain secure in their private affairs unless a neutral magistrate determines that probable cause justifies intrusion.

¶82 Because the warrantless acquisition of Cunningham's location history violated the plain commands of Article II, Sections 6 and 11, suppression of the evidence is required. I therefore concur fully in the Court's judgment and reasoning.

¶83 For these reasons, I respectfully concur.