Journal of Technology Law & Policy

Volume 11 | Issue 1 Article 3

June 2006

GPS Technology in Cellular Telephones: Does Florida's Constitutional Privacy protect Against Electronic Locating Devices?

Peter Caldwell

GPS TECHNOLOGY IN CELLULAR TELEPHONES: DOES FLORIDA'S CONSTITUTIONAL PRIVACY PROTECT AGAINST ELECTRONIC LOCATING DEVICES?

Peter Caldwell[*]

I. INTRODUCTION 40

II. THE FLORIDA CONSTITUTION 41
A. *Article I, Section 12 of the Florida Constitution: Its Scope* 43
B. *Article I, Section 23 of the Florida Constitution: Its Scope* 44
C. *The Same "Expectation of Privacy" Under Both Sections 12 & 23?* 52

III. APPLICATION OF SECTIONS 12 & 23 OF THE FLORIDA CONSTITUTION 56
A. *Is There an Expectation of Privacy in Cellular Calls?* 56
B. *Technologies Which Extract Contentful Personal Information* 60
C. *Technologies Which Extract Contentless Electronic Information* 63
D. *Technologies Which Extract Contentless Electronic Information: Those Most Analogous to GPS* 66
E. *Technologies Which Extract Contentless Electronic Information: When GPS is Part of the Cellular Telephone* 71

IV. CLOSING CONSIDERATIONS 73
A. *What Is the Privacy Trend in the Florida Legislature?* 73
B. *Observations and Final Analysis* 74
1. Section 23 74
2. Section 12 75
C. *Conclusion* 75

---

* Peter Caldwell holds law degrees in both the United States and Canada. He has been a lawyer for the national law firm of Ford & Harrison, LLP, and has been published extensively in law journals and conference proceedings. Mr. Caldwell currently resides in Florida.

I. INTRODUCTION

GPS technology is not new, but in the recent past, it has become so widespread that it now affects most everyone's lives. The term "GPS" refers to a "global positioning system," by which a GPS tracking device communicates through satellites to reveal its precise location. Since GPS units are now mandatorily built into all cellular telephones, service providers can locate their users wherever they may be, if required to do so.[1]

Yet, because of the intimate, locational nature of GPS data, these technologies have engendered privacy questions which beg closer examination, particularly due to the potential law enforcement (or other government) exploitation of GPS locational information. The present commentary will address whether individuals have an expectation of privacy in the GPS information that their cellular telephones transmit. With this objective in view, this Article focuses particularly on the Florida Constitution's two privacy provisions, sections 12 and 23 of article I.

The first portion of this Article will therefore closely examine the rules, uses, and potential applications of sections 12 and 23 alone, without regard to GPS technology. This initial discussion will establish the framework for the subsequent hypothetical applications of sections 12 and 23 jurisprudence to cellular telephone communications, contentless locational technology, and finally, to GPS itself. By considering the application of sections 12 and 23 to this broad range of technology, this Article contextualizes the GPS privacy questions that the constitutional provisions potentially protect.

Since there is no Florida case law directly addressing the question of GPS-cellular devices under sections 12 or 23, the following analysis depends partially on legal predictions. The case law related to this subject matter, albeit peripherally, suggests the Florida courts' future position on GPS privacy and serves as a predictor of future legal reasoning.

In order to arrive at predictive analysis, this Article begins by elaborating the constitutional privacy framework for article I, sections 12 and 23 of the Florida Constitution.

---

1. All cellular telephones are now equipped with GPS locators. These devices regularly provide signals to satellites which, in turn, relay the user's location data to the cell phone provider. The cellular company may choose to ignore the data much of the time, but the location data is nonetheless being received by it at regular intervals as long as the handset is within the network's range and is turned on. Although rare, some sophisticated cellular telephones even transmit GPS location data when the handset is turned off. These satellite updates allow the cellular provider to pinpoint the user's position within a maximum distance of 300 feet.

II. THE FLORIDA CONSTITUTION

Much like the U.S. Constitution, the Florida Constitution protects the privacy of its people in several ways. In addition to the constitutional privacy which protects decisional autonomy,[2] both constitutions prohibit government intrusions into personal zones where an expectation of privacy exists.

Apart from the decisional type of privacy, the Florida Constitution protects Floridians against two other types of privacy invasions by the state. First, it explicitly protects against unreasonable searches, seizures, and private communication interceptions, most typically where such intrusions arise in the context of a police investigation for criminal evidence. This privacy right is embodied in article I, section 12 of the Florida Constitution, which states:

> The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, and against the unreasonable interception of private communications by any means, shall not be violated. No warrant shall be issued except upon probable cause . . . . This right shall be construed in conformity with the 4th Amendment to the United States Constitution, as interpreted by the United States Supreme Court . . . .[3]

As this phraseology indicates, section 12 does not offer any broader or narrower privacy right than that provided by the Fourth Amendment of the U.S. Constitution, and must be interpreted accordingly by the Florida courts. The Florida Constitution therefore differs in no way from the federal constitution regarding matters of search and seizure.

---

2. This references the decisional autonomy crafted by the U.S. Supreme Court in its landmark contraception rights decision, *Griswold v. Connecticut*, and was created as an implicit extension of constitutional substantive due process. Griswold v. Connecticut, 381 U.S. 479 (1965). It was also deemed to have been derived from several constitutional amendments, rather than from a single explicit constitutional provision. *Id.* at 484. This type of "privacy" protects one's personal choices from state intervention in the areas of child-rearing, contraception, and marriage. The same privacy right to decisional autonomy exists under article I, section 23 of the Florida Constitution, as evidenced by *In re T.W.*, in which the rights of a minor to terminate her pregnancy were analyzed by the Florida Supreme Court. *In re* T.W., 551 So. 2d 1186, 1191-92 (Fla. 1989). However, the decisional autonomy aspect of section 23 will not be dealt with in this Article; instead, it will consider whether cellular GPS technologies, when used by government entities, could amount to a privacy violation under article I, section 23.

3. FLA. CONST. art. I, § 12 (1982).

There is, however, a second type of privacy guaranteed by the Florida Constitution. This second constitutional privacy right is located in article I, section 23, and unlike its implied federal counterpart, it is articulated explicitly as follows:

> Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law.[4]

This provision offers a broad, general privacy right proscribing government invasions into private life. It not only affects the decisional areas of marriage, contraception, and related aspects of personal autonomy,[5] but also is invoked to prevent government disclosure of personal information[6] and the state's own acquisition of proprietary information[7] without the owner's consent.[8] It is the latter (non-decisional) coverage of section 23 that will be addressed in this Article, rather than the personal autonomy element of the provision.

Since GPS technologies may involve potential privacy invasions through warrantless government searches for criminal evidence, the possible application of article I, section 12 will be addressed in the analysis that follows. The application of section 23 privacy will also be explored here, because the GPS location of cellular telephones is not limited to criminal searches for evidence, and may additionally arise where

---

4. FLA. CONST. art. I, § 23 (1998).

5. *In re T.W.*, 551 So. 2d at 1191. This case involved the personal autonomy right of a woman and her fundamental right to make contraception choices.

6. *See* Rasmussen v. S. Fla. Blood Serv., Inc., 500 So. 2d 533 (Fla. 1987). In *Rasmussen*, the personal information and identities of confidential blood donors could not be disclosed by the government, despite the plaintiff's subpoena attempts to obtain this information. *Id.* at 536-37. The privacy interests of blood donors, under article I, section 23 of the Florida Constitution, outweighed the plaintiff's interest in receiving this information. *Id.*

7. Mozo v. State, 632 So. 2d 623 (Fla. 4th Dist. Ct. App. 1994). In *Mozo*, the government had illegally intercepted the appellant's telephone calls, which amounted to an invasion of both the appellant's section 12 privacy (unlawful interception) and section 23 privacy (invasion of the right to be left alone from government intrusion). *Id.* at 635. When appealed to the Florida Supreme Court, the same decision was reached. State v. Mozo, 655 So. 2d 1115, 1117 (Fla. 1995). Yet, since the decision could be reached more simply without discussion of sections 12 and 23, the Florida Supreme Court avoided addressing the constitutional issues. *Id.*

8. Since section 23 of the Florida Constitution is only two decades old, it will surely evolve to reveal additional applications in the future that are beyond the scope of those listed here.

a government entity attempts to obtain locational information for other purposes.

Within this framework, the Article will consider the extent to which either sections 12 or 23 are applicable to the warrantless government interception of GPS locator signals in cellular telephones. In order to do so, however, the legal parameters and applications of sections 12 and 23 must first be defined more acutely, beginning with section 12.

A. *Article I, Section 12 of the Florida Constitution: Its Scope*

The Florida courts have reiterated that, since the 1982 amendment of section 12, the legal analysis applied to section 12 should be the same as that used for the Fourth Amendment of the U.S. Constitution.[9] Therefore, the Florida courts must rely on the precedential case law from the U.S. Supreme Court itself and the developments which that Court permitted to evolve over time. For this reason, the Article will explain the appropriate analysis used for section 12 with the aid of leading U.S. Supreme Court cases.

As discussed below, to ascertain section 12 or Fourth Amendment privacy, three elements must be established: (1) whether the party claiming a privacy right indeed had a reasonable expectation of privacy, (2) whether the government conducted a "search," and (3) whether, if a search was conducted, it was nonetheless "reasonable" enough to avoid constitutional privacy scrutiny.[10] Ordinarily, a warrant authorizing a search or the consent of the searched individual will render the search "reasonable."

The Fourth Amendment and article I, section 12 of the Florida Constitution both require freedom from unreasonable government intrusion into the constitutionally protected areas of a citizen's life,[11] including one's private home, car, hotel room, phone booth, and locker. For this reason, a warrantless search of one's home or car is unconstitutional in Florida, absent the owner's consent.[12] However, in most cases, the government must make an actual intrusion into the protected private space in order for a "search" to have been committed in violation of section 12 or the Fourth Amendment.[13] Thus, mere visual

---

9. Madsen v. Florida, 502 So. 2d 948, 949 (Fla. 4th Dist. Ct. App. 1987).

10. Kyllo v. United States, 533 U.S. 27, 40 (2001).

11. Silverman v. United States, 365 U.S. 505, 511-12 (1961) (stating this requirement of the Fourth Amendment). Section 12 of the Florida Constitution similarly states this principle. FLA. CONST. art. I, § 12 (1982).

12. Illinois v. Rodriguez, 497 U.S. 177, 181 (1990); Tollett v. State, 272 So. 2d 490, 493 (Fla. 1973).

13. *See Silverman*, 365 U.S. at 510-12.

surveillance of the exterior of one's home or car does not constitute an intrusion or search and is therefore lawful.

On the other hand, there is some authority which modifies this general rule. For instance, when a government entity searches the portion of one's home or yard which is visible to the public eye, this may constitute a "search," yet may nonetheless be deemed "reasonable" enough not to violate either federal or Florida constitutional privacy.[14] Most authorities have held that any visual surveillance possible with the naked eye, even with the use of some visual enhancement technology, does not "search" a citizen's private places and is therefore constitutional.[15]

At the opposite end of the spectrum, there are also limits on technologically-aided searches and a point at which government technology can no longer escape constitutional scrutiny, both under the Florida and federal constitutions. As a general rule, if the government uses "sense-enhancing technology" to obtain information from one's private space without physical intrusion, this is a "search" if the technology used is not in "general public use."[16] This observation was made in *Kyllo v. United States,* in which thermal imaging technology had been used by the police outside a home to ascertain the home's contents.[17]

As *Kyllo* demonstrates, there is a limit to the permissible use of technology in obtaining private information from an individual's constitutionally protected areas. In short, the government may use commonplace technologies to ascertain a person's whereabouts (within constitutionally protected space) or to determine the contents of that private space, but only with technology which is in "general public use."[18] Seeing through walls is not permitted, unless a warrant authorizes the use of such technology.[19]

B. *Article I, Section 23 of the Florida Constitution: Its Scope*

While some authorities insist that section 23 cannot apply to the privacy zone already encompassed by section 12,[20] other authorities have

---

14. Minnesota v. Carter, 525 U.S. 83, 104 (1998) (Breyer, J., concurring).

15. In *Dow Chemical v. United States,* the U.S. Supreme Court ruled that the government had not illegally searched a manufacturer's private curtilage when using satellite aerial imaging. Dow Chem. v. United States, 476 U.S. 227, 235, 238-39 (1986). This type of surveillance did not constitute a search because human visualization of these protected areas was made possible with the naked eye, albeit a vastly enhanced naked eye. *Id.*

16. Kyllo v. United States, 533 U.S. 27, 34 (2001).

17. *Id.* at 30.

18. *Id.* at 34.

19. *Id.* at 40.

20. As Robert Whorf has noted:

ruled to the contrary.[21] Based on these authorities, however, it would appear that section 23 indeed can apply to section 12 search and seizure subject matter in the broader "right to be left alone" sense. Despite this, relatively few courts have proceeded to undertake a section 23 analysis where the more directly relevant section 12 analysis is already adequate to analyze a criminal search, seizure, or communication interception case.

Section 23 may occasionally prove necessary to secure privacy even in criminal matters, particularly where section 12 is not available to a defendant. Recall that section 12 can only be invoked where there is a reasonable expectation of privacy and the protected information is contained in a private home, car, hotel room, locker, or phone booth. Like section 12, section 23 also requires an expectation of privacy, but does not mandate that the protected information be located in a contained private space, such as one's home or car. Nor is section 23 privacy automatically defeated because the government has a warrant for the information sought,

---

> Florida courts have generally endeavored to minimize confusion created by the apparent overlap of sections 12 and 23. In that endeavor, they have sought to foreclose any tendency for interpretation under section 23 to override the effect of the conformity requirement of section 12 . . . . Therefore, article I, section 12 is likely to be applied in criminal contexts while article I, section 23 is more likely to be applied in non-criminal contexts . . . . The Florida Supreme Court has construed "criminal context" rather broadly to avoid application of article I, section 23 in favor of application of article I, section 12.

Robert H. Whorf, *The Privacy Interests of Floridians and the Effect of "Conformity" under Florida Constitution Article 1, Section 12*, 2 BARRY L. REV. 3, 7 (2001) (citing State v. Smith, 641 So. 2d 849, 851 (Fla. 1994)). Whorf further explains that "[t]he Florida Supreme Court has said that article I, section 23 'does not modify the applicability of article I, section 12.'" *Id.* (citing State v. Hume, 512 So. 2d 185, 188 (Fla. 1987)). The Florida Supreme Court's concern in *Hume* was that section 23 might expand the search, seizure, and interception protection afforded by section 12 beyond that of the Fourth Amendment. *Hume*, 512 So. 2d at 185. This is the underlying rationale for keeping sections 12 and 23 as separate as possible in scope.

21. For instance, in *Mozo v. State*, Justice Anstead of the Fourth District Court of Appeals reasoned that both sections 12 and 23 of the Florida Constitution, article I, should apply to cordless telephone conversations electronically intercepted by police, without a warrant, from outside a suspect's home. Mozo v. State, 632 So. 2d 623, 631-38 (Fla. 4th Dist. Ct. App. 1994). Although sections 12 and 23 each applied differently to these facts, the inclusion of section 12 in the analysis did not exclude the applicability of section 23. Nor did the fact that the matter was one of a criminal nature. *Id.* Additionally, in *Winfield v. Division of Pari-Mutuel Wagering*, the government had subpoenaed a citizen's banking records for a criminal investigation. Winfield v. Div. of Pari-Mutuel Wagering, 477 So. 2d 544, 546 (Fla. 1985). Section 23 of the Florida Constitution, article I, formed the basis of the Florida Supreme Court's privacy analysis in this decision, despite the fact that this was a criminal matter (ordinarily reserved for section 12 analysis). *Id.* at 546-48. The case law therefore suggests a zone of overlap that entails the privacy protections of both sections 12 and 23 of the Florida Constitution, article I.

unlike section 12 privacy. Part 2.C below explains how section 23 privacy therefore applies to a broader range of subject matter than the more limited section 12.

Yet, apart from this distinction between sections 12 and 23 privacy, there is indeed a zone of overlap where both sections 12 and 23 can protect a citizen's personal information under the Florida Constitution. While, as previously stated, section 23 cannot extend the scope of section 12, there is no reason why section 23 cannot apply independently to prevent the state from obtaining one's personal information without reference to section 12.[22]

Winfield v. Division of Pari-Mutuel Wagering, is the leading case in Florida establishing the legal parameters of article I, section 23.[23] In *Winfield,* Justice Adkins begins by acknowledging that privacy under section 23 is a "fundamental right,"[24] much like the privacy right recognized under the U.S. Constitution.[25] As such, it follows that the standard of review is one of strict scrutiny, and accordingly, the state must demonstrate a compelling interest before it can supersede one's fundamental right to privacy.[26]

The first step in article I, section 23 analysis is for a court to determine whether the individual actually has a "legitimate expectation of privacy."[27] In *Winfield,* the Florida Supreme Court recognized that the petitioners did have a valid expectation of privacy in their personal banking records and in the maintenance of their confidentiality.[28] If the individual relying on section 23 does not possess this reasonable expectation, a court will not pursue the analysis further, and the government may obtain access to the personal information it seeks.[29]

On the other hand, if the legitimate expectation of privacy exists, then the second step in the *Winfield* analysis is to determine whether the government has a compelling state interest in obtaining the individual's personal information.[30] This second step led Justice Overton, in his *Forsberg v. Housing Authority of the City of Miami Beach* concurrence, to call the section 23 test a "balancing test," whereby the "privacy interests

22. *Hume*, 512 So. 2d at 188.
23. *Winfield,* 477 So. 2d at 546-48.
24. *Id.* at 547.
25. Roe v. Wade, 410 U.S. 113, 152 (1973).
26. *Winfield*, 477 So. 2d at 547.
27. *Id.*
28. *Id.*
29. *Id.*
30. *Id.* at 548.

of the individual must be weighed against the public interest."[31] In *Winfield,* the government did have a compelling interest in investigating the pari-mutuel industry effectively, and this interest was held to outweigh the petitioner's own interest in bank record personal privacy.[32]

Finally, the third prong of the *Winfield* test requires the government to show that it obtained or attempted to obtain the private information through the least intrusive means.[33] If this prong is met, the government's compelling interest will successfully outweigh the section 23 privacy interest of the citizen in question.[34] This is precisely what transpired in *Winfield,* since the government demonstrated that it had used a subpoena to obtain the petitioner's bank records. Because a subpoena was less invasive than the other means available to seize bank information, the Supreme Court of Florida ruled that the government had met all three prongs of the section 23 balancing test.[35]

Although the foregoing three-part test has been set out clearly in *Winfield,* there remains much that we do not know about article I, section 23 of the Florida Constitution. For this Article, it is useful to understand how broadly section 23 can be applied to personal information, and to what type of information. Section 23's scope is particularly important since understanding it may assist in determining how, analogously, it might translate into potential GPS privacy protection.

The Florida case law says that section 23 can form a legitimate expectation of privacy in the following personal information: personal banking records;[36] personal autopsy records;[37] cordless telephone communications intercepted by the police;[38] private data emanating from a telephone pen register (i.e. intercepted "caller ID");[39] private identification information of blood donors, even in the face of a

---

31. Forsberg v. Hous. Auth. of Miami Beach, 455 So. 2d 373, 379 (Fla. 1984) (Overton, J., concurring).

32. *Winfield,* 477 So. 2d at 548.

33. *Id.* at 547.

34. *Id.*

35. *Id.* at 548.

36. *Id.*

37. Campus Commc'ns, Inc. v. Earnhardt, 821 So. 2d 388, 392-93 (Fla. 5th Dist. Ct. App. 2002).

38. Mozo v. State, 632 So. 2d 623, 634 (Fla. 4th Dist. Ct. App. 1994). On appeal, this case was decided by the Florida Supreme Court on a non-constitutional basis. State v. Mozo, 655 So. 2d 1115, 1117 (Fla. 1995). However, the fact that this matter was ruled on by the Florida Supreme Court on different grounds does not rule out the otherwise valid constitutional legal analysis made by Justice Anstead in his decision from the Fourth District Court of Appeals.

39. Shaktman v. State, 529 So. 2d 711, 715 (Fla. 3d Dist. Ct. App. 1988); Shaktman v. State, 553 So. 2d 148, 149 (Fla. 1989).

subpoena;[40] and medical and other personal information contained in the files of judicial proceedings, unless the information becomes an integral part of the judicial proceeding.[41]

On the other hand, section 23 does not create a legitimate expectation of privacy in the following areas: personal information, such as private e-mail found in a government computer;[42] records providing the personal information of tenants and all other persons who ever applied to live in public housing complexes;[43] the contentless private data emitted from a personal pocket pager or "beeper," when intercepted by the police;[44] privileged medical or psychiatric reports, when disclosed to the state bar for admission to practice;[45] and personal information regarding one's smoking habits.[46]

Thus, at the present time, the classes of personal information that can be protected by section 23 are not defined by any precise rule. To date, what constitutes a reasonable expectation of privacy under section 23 has been a matter of judicial discretion in Florida. Until many more cases are tried by the Florida courts, the defining threshold between unprotected privacy and protected subject matter shall remain a blurred line.

What is clear, however, is that article I, section 23 of the Florida Constitution affords a broader right of anti-disclosural and anti-invasive privacy than the Federal Constitution. Although the balancing test used by the Florida courts for section 23 was crafted on the federal model,[47] U.S.

---

40. Rasmussen v. S. Fla. Blood Serv., Inc., 500 So. 2d 533, 534 (Fla. 1987).

41. Barron v. Fla. Freedom Newspapers, Inc., 531 So. 2d 113, 119 (Fla. 1988); Cape Publ'ns, Inc., v. Hitchner, 549 So. 2d 1374, 1376 (Fla. 1989).

42. State v. City of Clearwater, 863 So. 2d 149, 150 (Fla. 2003).

43. Forsberg v. Hous. Auth. of Miami Beach, 455 So. 2d 373, 375 (Fla. 1984).

44. Dorsey v. State, 402 So. 2d 1178, 1180 (Fla. 1981).

45. Fla. Bd. of Bar Exam'rs Re: Applicant, 443 So. 2d 71, 74-76 (Fla. 1984).

46. City of N. Miami v. Kurtz, 653 So. 2d 1025, 1026 (Fla. 1995).

47. *Forsberg*, 455 So. 2d at 374-80 (Overton, J., concurring). *Forsberg* set the stage for *Winfield*, which immediately followed it and adhered largely to Overton's concurrence in *Forsberg*. *See* Winfield v. Div. of Pari-Mutuel Wagering, 477 So. 2d 544, 547-48 (Fla. 1985). However, in the majority *Winfield* opinion, Justice Adkins noted that the federal balancing test for privacy is distinguishable from the type of non-disclosural and non-invasive privacy right that section 23 guarantees. *Id.* at 546. He remarked that Supreme Court cases should be limited to privacy in connection with personal autonomy, stating:

> Other privacy interests enunciated by the Court in *Nixon v. Administrator of General Services*, 433 U.S. 425, 97 S.Ct. 277, 53 L.Ed.2d 867 (1977), and *Whalen v. Roe*, 429 U.S. 589, 97 S.Ct. 869, 51 L.Ed.2d 64 (1976), involve one's interest in avoiding the public disclosure of personal matters. However, *Nixon*, *Whalen*, and those cases involving the autonomy zone of privacy are not directly applicable to the case at bar.

constitutional cases show considerable reticence in recognizing the disclosural privacy right.

For instance, in *Whalen v. Roe,* the U.S. Supreme Court was reluctant to formally acknowledge a fundamental privacy right in non-disclosural subject matter.[48] In his majority opinion, Justice Stevens remarked that the government collection of personal data "require[s] the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed."[49] The Court did not reject constitutional non-disclosural privacy altogether, but fell short of making this right equal to personal autonomy privacy, a fundamental freedom.[50]

As Erwin Chemerinsky has observed, "[A]lthough there is a strong argument that the [U.S.] Constitution should be interpreted to protect a right to control information, there is thus far little support for such a right from the [U.S.] Supreme Court."[51]

Id. In *Winfield,* the disclosure issue was one of personal banking records and the government's compelling interest in having access to them. *Id.* at 548. The government's interest was based on its need to properly investigate the pari-mutuel industry. *Id.*

48. Whalen v. Roe, 429 U.S. 589, 605-06 (1977).

49. *Id.* at 605.

50. In *Whalen v. Roe,* the U.S. Supreme Court ruled on a New York law requiring doctors to report patient prescription drug information to the state government. *Id.* at 591. This regulation was intended to curtail drug abuse, and therefore provided a compelling state interest which outweighed any individual privacy right under the U.S. Constitution. *Id.* at 597-99. The U.S. Supreme Court used the balancing test which would later be adopted into Florida's section 23 privacy analysis, but was reluctant to formally assert a fundamental right to non-disclosural, non-invasive privacy under the U.S. Constitution. *See supra* text accompanying note 47; *Whalen,* 429 U.S. at 605. The "penumbra" of rights underlying U.S. constitutional privacy, as espoused in prior case law, did not clearly apply to the non-disclosural privacy context. *See* Griswold v. Connecticut, 381 U.S. 479 (1965); *Whalen,* 429 U.S. at 605. Similarly, in *California Bankers Ass'n v. Schultz,* the government's compelling need to curtail banking fraud outweighed the privacy rights of individuals who, absent the Bank Secrecy Act of 1970, would not have endured the disclosure of their bank transactions to the government. Cal. Bankers Ass'n v. Schultz, 416 U.S. 21 (1974).

51. ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 696 (1997). To a certain extent, this may be regarded as an anomaly in the law's evolution, since Florida's constitutional privacy has advanced and developed much more quickly than any non-disclosural privacy right under the U.S. Constitution. In the early twentieth century, the U.S. Supreme Court seemed prepared to recognize a non-disclosure, anti-intrusion right of constitutional privacy, back when this would have been inconceivable in Florida (prior to the addition of section 23 to the Florida Constitution). In his oft-quoted passage from *Olmstead v. United States,* the dissenting Justice Brandeis of the U.S. Supreme Court makes his interpretation of the U.S. Constitution clear: "The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness . . . . They conferred, as against the Government, the right to be let alone." Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). Thus, the concept of the "right to be let alone" originated in U.S. Supreme Court interpretations of the Federal Constitution, and

Furthermore, many Florida cases have explicitly asserted that the section 23 privacy right is greater than its (still underdeveloped) non-disclosural privacy counterpart in the U.S. Constitution.[52] This observation is normally made because section 23 is explicit, while the U.S. Constitution's general privacy notion is found in no one particular amendment and is largely an implied right. As noted by Justice Overton in his *Forsberg* concurrence, "Although the United States Supreme Court has recognized a fundamental constitutional right of privacy which applies in certain limited circumstances, that Court has refused to establish a general right of privacy under the federal constitution."[53]

Justice Overton took this observation further in his scholarly writings, where he and Katherine Giddings wrote:

> Article I, section 23 affords greater protection from government intrusion than the [F]ederal Constitution. The privacy right is explicit, it extends to all aspects of an individual's private life rather than simply extending to some elusive 'penumbra' of rights, and it ensures that the state cannot intrude into an individual's private life absent a compelling interest.[54]

In *Winfield,* though Justice Adkins does not state that section 23 affords an absolute privacy right, he emphasizes that this provision is phrased in very strong terms. In fact, as noted by Justice Adkins, section 23 was drafted to avoid creating a mere *reasonableness* or *unreasonableness* standard of privacy, instead favoring a much more firmly entrenched right. As Justice Adkins remarks:

> The citizens of Florida opted for more protection from government intrusion when they approved article I, section 23, of the Florida Constitution .... Article I, section 23, was intentionally phrased in strong terms. The drafters of the amendment rejected the use of the words "unreasonable" or "unwarranted" before the phrase "governmental intrusion" in order to make this privacy right as

---

was later imported into the Florida Constitution's consideration of section 23. *Winfield,* 277 So. 2d at 546. Paradoxically, it seems that the federal privacy right has lost some of its potency along the way. *See, e.g., Whalen,* 429 U.S. at 605-06; *Schultz,* 416 U.S. at 21.

52. *Winfield,* 477 So. 2d at 548; *Forsberg,* 455 So. 2d at 377.

53. *Forsberg,* 455 So. 2d at 377.

54. Ben F. Overton & Katherine E. Giddings, *The Right of Privacy in Florida in the Age of Technology and the Twenty-First Century: A Need for Protection from Private and Commercial Intrusion,* 25 FLA. ST. U. L. REV. 25, 40-41 (1997).

> strong as possible. Since the people of this state exercised their prerogative and enacted an amendment to the Florida Constitution which expressly and succinctly provides for a strong right of privacy not found in the United States Constitution, it can only be concluded that the right is much broader in scope than that of the Federal Constitution.[55]

The judicial commentary of Justices Adkins and Overton are instructive. They aid in determining that section 23 was intended to form a stronger right than federal constitutional privacy, and one which could be compromised only in special circumstances. Yet even when accompanied by the section 23 case law, these commentaries only reveal a portion of what the parameters of section 23 are now and will evolve to become in future years. Determining what could or could not be a section 23 zone of privacy is not yet identifiable by any bright line rule or formula. After two decades of case law, one can still only speculate as to where a legitimate expectation of privacy might be found by future courts.

---

55. *Winfield,* 477 So. 2d at 548. In contrast with the remarks that section 23 privacy is stronger than the Federal Constitution's protection, Timothy Lenz states:

> The Florida Supreme Court held in Shevin v. Byron, Harless, Schaffer, Reid & Associates that a person's right to disclosural privacy is no greater under the state constitution than it is under the federal constitution. The court ruled that there was no state constitutional right to privacy to prevent public disclosure of papers compiled by a consultant conducting a search for applicants to be managing director of a public utility. By refusing to construe a state constitutional right of disclosural privacy, the court, while acknowledging the existence of such a privacy interest under the federal constitution, held "the federal constitutional right of privacy [does not] preclude [] dissemination of private information by the government."

Timothy Lenz, *"Rights Talk" about Privacy in State Courts,* 60 ALB. L. REV. 1613, 1624-25 (1997) (referring to the Florida Supreme Court decision of *Shevin v. Byron, Harless, Schafer, Reid & Assocs.,* 379 So. 2d 633 (Fla. 1980)). However, what is not apparent from Lenz's observations is that *Shevin* is not used for section 23 disclosural privacy analysis, as it was rendered shortly before the adoption of article I, section 23 of the Florida Constitution. It therefore presents an outdated analysis of disclosural privacy under the Florida Constitution. Arguably, the current view of Florida's section 23 is that it presents a much more encompassing form of anti-disclosure, anti-invasiveness privacy than the highly undeveloped federal brand discussed earlier in the cases of *Whalen* and *Schultz. Whalen,* 429 U.S. at 589; *Schultz,* 416 U.S. at 21-22.

C. *The Same "Expectation of Privacy" Under Both Sections 12 & 23?*

As discussed in the preceding section, privacy under article I, section 12 of the Florida Constitution is limited to places where one enjoys a reasonable expectation of privacy,[56] such as inside persons' private homes, cars, hotel rooms, and their private papers.[57] This is therefore a limited zone of privacy, and one which does not easily protect personal documents, an individual's location in public view, medical records, personal property, or information that is outside one's vehicle rather than inside it.[58]

By contrast, article I, section 23 of the Florida Constitution allows for a broader zone of privacy than section 12, and is not limited to information or people located in private homes or cars. For instance, in *Winfield v. Division of Pari-Mutuel Wagering,* a citizen's private bank accounts were deemed to fall within the legitimate expectation of privacy contemplated by section 23, but not the zone of privacy considered for section 12 or the Fourth Amendment.[59]

Yet while the subject matter coverage of these two privacy provisions differ, the formulas used to identify a privacy expectation under sections 12 and 23 are in many respects related. As will be revealed below, expectations of privacy under sections 12 and 23 are remarkably similar despite what judicial commentary purports to the contrary.

There are two notable traits which distinguish section 12 and section 23 expectancies, and they are as follows: First, a section 12 privacy expectation can only be claimed for the interior of a house, car, hotel room, telephone booth, locker, private apartment, or similar private space.[60] By contrast, a section 23 privacy expectation can be claimed anywhere without restriction, since it is the subject matter of the information which denotes its private character, rather than the physical location.[61]

---

56. Kyllo v. United States, 533 U.S. 27, 33 (2001).

57. United States v. Miller, 425 U.S. 435, 440 (1976).

58. United States v. McIver, 186 F.3d 1119, 1127 (1999). The Fourth Amendment, which is analyzed in the same way as article I, section 12 of the Florida Constitution, does not guarantee a reasonable expectation of privacy for GPS tracking devices placed by police on the outside of a vehicle, as opposed to inside. *Id.*

59. *Winfield,* 477 So. 2d at 548. Although the Florida Supreme Court acknowledged a reasonable expectation of privacy for one's personal bank accounts under section 23, ultimately the account information had to be disclosed because the government's compelling interest outweighed Winfield's privacy right. *Id.*

60. *Kyllo,* 533 U.S. at 32-33.

61. *See* Mozo v. State, 632 So. 2d 623, 633 (Fla. 4th Dist. Ct. App. 1994).

Second, section 12 (i.e. Fourth Amendment equivalent) privacy requires that the individual claiming the privacy right has, in some way, manifested his own subjective expectation of privacy with regard to his private space or information.[62] However, this subjective manifestation of privacy must pass a second test: the information or place must be one which society would objectively regard as private.[63] For this reason, the Fourth Amendment and section 12 case law refers to a "reasonable expectation of privacy," since society's "reasonable" and objective perception of the privacy claimed is factored into a court's equation. This additional measure avoids situations where one has subjectively manifested his expectation, but the expectation is one which is clearly not private and should not receive protection from government intrusions.

This differs from section 23 privacy because a section 23 expectation does not have to be "reasonable" or pass any objective standard. Earlier, this Article addressed Justice Adkins' remarks from *Winfield,* in which Adkins recalled the section 23 drafters' intentions to exclude a "reasonableness" standard from the section 23 expectation of privacy.[64] For this reason, the case law refers to a "legitimate expectation of privacy" for section 23,[65] but a "reasonable expectation of privacy" for section 12.[66]

The Florida case law has further confirmed this distinction between sections 12 and 23 expectations, and as Justice Anstead (then of the 4th District Court of Appeals) remarked in *Mozo v. Florida*:

> A major analytical difficulty faced by the federal courts in . . . the Fourth Amendment [i.e. Section 12 equivalent] appears to be applying the objective prong of the *Katz* formula: i.e., whether the defendant was reasonable in his belief of privacy. But . . . under the Florida right of privacy [i.e. Section 23], although the subjective belief must be legitimate, the separate and distinct test of a reasonable expectation of privacy is eliminated.[67]

Similarly, in *Shaktman v. State,* Chief Justice Ehrlich of the Florida Supreme Court explained that section 23 expectations do not have to be

---

62. *Id.* at 634.

63. *Kyllo,* 533 U.S. at 33 (where the court noted that "when the government violates a subjective expectation of privacy that society recognizes as reasonable . . . search does not occur . . . unless 'the individual manifested a subjective expectation of privacy' . . . 'society is willing to recognize that expectation is reasonable'").

64. *Winfield,* 477 So. 2d at 548.

65. *Id.*

66. *Kyllo,* 533 U.S. at 33.

67. *Mozo,* 632 So. 2d at 633.

"reasonable" because society's endorsement of a section 23 privacy expectation is not required.[68] This is in direct contrast with the second "objective" prong of the section 12 privacy test. Justice Ehrlich, concurring specially, stated that "[t]he words 'unreasonable' and 'unwarranted' harken back to the federal standard of 'reasonable expectation of privacy,' [used for section 12] which protects an individual's expectation of privacy only when society recognizes that it is reasonable to do so . . . . [T]he Florida right of privacy was intended to protect an individual's expectation of privacy regardless of whether society recognizes that expectation as reasonable."[69]

Justice Ehrlich further established the test used in assessing a section 23 expectation of privacy. According to Ehrlich, society's recognition of certain personal information as private was irrelevant, since it was the individual whose own expectations of privacy were to be taken into account. When enunciating the three-part test for determining a section 23 expectation of privacy, Justice Ehrlich articulated the "spurious or false" standard, which has become part of the test.[70]

In Justice Ehrlich's words, "[T]he zone of privacy covered by article I, section 23, can be determined only by reference to the expectations of each individual, and those expectations are protected provided they are not spurious or false."[71] Justice Ehrlich provides the third and most objective criterion, which despite having passed the first two prongs, serves to defeat the expectation of privacy if the facts show that the disputed information is of an inherently public nature,[72] or for other reasons should not be deemed private.[73]

---

68. Shaktman v. State, 553 So. 2d 148, 153 (Fla. 1989) (Ehrlich, C.J., concurring specially).

69. *Id.* (Ehrlich, C.J., concurring specially).

70. *Id.* (Ehrlich, C.J., concurring specially).

71. *Id.* (Ehrlich, C.J., concurring specially) (emphasis added).

72. *Id.* (Ehrlich, C.J., concurring specially). The *Forsberg* decision provides an example that illustrates this final criterion. Forsberg v. Hous. Auth. Of Miami Beach, 455 So. 2d 373, 379 (Fla. 1984) (Overton, J., concurring). In *Forsberg,* the appellants did not have an expectation of privacy in public housing records containing personal information about them. *Id.* It was not that personal data was not of a private character, but that the public housing records were, by their very nature, public government documents. *Id.* Thus, this defeated any legitimate expectation of privacy which otherwise might have been found in the content of those documents. *Id.*

73. In sum, Justice Ehrlich's test for section 23 expectations amount to the following three steps: (i) the information claimed as private must be assessed according to the individual's own personal expectations; accordingly, the privacy would depend on whether the individual subjectively perceived his information as private and shielded from government intrusion ("subjective" prong); (ii) however, even if the first criterion is met, the information will not be deemed private if the claimant's privacy expectation appears to be "spurious or false;" (iii) in order to assess both of the foregoing factors, all circumstances must be considered, including any

The latter factor (iii) reveals that the section 23 test for expectations of privacy is more objective and susceptible to society's general privacy view than the courts would like to admit. In this regard, the objective factor (iii) brings section 23 expectations of privacy closer to the section 12 test, since both contain a subjective (individual-based) prong and an objective (factual or societal-based) prong. In other words, section 23 may do no more than denote a hidden "reasonable expectation of privacy" test, rather than the "legitimate expectation of privacy" standard that the case law pretends it represents.[74]

Despite the similarities between sections 12 and 23 expectations of privacy, the case law reveals that sometimes personal information is not private enough to satisfy section 12, but will nonetheless meet the requirements of a section 23 expectation. For instance, in *Shaktman,* the majority specifically stated that data collected from a pen register (i.e. police-intercepted caller ID) does not bear a reasonable expectation of privacy under section 12.[75] However, the same pen register data was sufficiently private to present a legitimate expectation of privacy under section 23.[76] The *Shaktman* court ruled that data including the telephone numbers one has dialed "represents personal information which, in most circumstances, the individual has no intention of communicating to a third party."[77]

Similarly, in *Winfield,* the privacy of bank records was not protected by the Fourth Amendment or article I, section 12 of the Florida Constitution.[78] By contrast, under *Winfield,* a legitimate expectation of privacy was found in the same private bank records under the section 23 analysis.[79]

In short, the tests used to identify an expectation of privacy under sections 12 and 23 differ only slightly. Even so, section 23 expectations

---

available "objective" manifestations ("objective" prong) or facts that support a finding of privacy or a lacking of privacy (e.g., the information is already highly public, which defeats the expectation of privacy claimed). *Shaktman,* 553 So. 2d at 153 (Ehrlich, C.J., concurring specially).

74. To demonstrate this point, let us review the section 12 expectation of privacy test once again, in its three-prongs: (i) a section 12 privacy expectation can only be claimed if the information is located in the interior of a house, car, hotel room, telephone booth, private apartment, or similar private space; (ii) the claimant must have manifested his subjective expectation of privacy with regard to the disputed information ("subjective" prong); (iii) even if this preceding prong is met, the information or place in which the information was found must nevertheless be one which society would objectively regard as private ("objective" prong). Kyllo v. United States, 533 U.S. 27, 32-33 (2001).

75. *Shaktman,* 553 So. 2d at 151.

76. *Id.*

77. *Id.*

78. Winfield v. Div. of Pari-Mutuel Wagering, 477 So. 2d 544, 547 (Fla. 1985).

79. *Id.*

have covered a broader range of subject matter because section 12 is limited to situations where private possessions are located in non-private spaces.

III. APPLICATION OF SECTIONS 12 & 23 OF THE FLORIDA CONSTITUTION

Having set out the framework and possible applications of the Florida Constitution, article I, sections 12 and 23, it is now possible to apply these principles to concrete problems. In particular, the applicability of sections 12 and 23 to GPS-equipped cellular telephones will be the focus of the following portion of this Article.

To reiterate, applying sections 12 and 23 necessitates that an expectation of privacy should exist first. The analysis therefore largely depends on one crucial factor: do users of GPS-equipped cellular telephones have an expectation of privacy?

The application which follows is necessarily speculative, since there is no Florida case law dealing with sections 12 or 23 and the relationship of these provisions to GPS subject matter. In fact, even the case law from other jurisdictions on this topic is sparse, and it deals only peripherally with the specific GPS issues. Therefore, this case law contributes nothing to our knowledge of the GPS-section 23 interface. Thus, the following predictions are based on the incomplete set of tools currently at our disposal.

A. *Is There an Expectation of Privacy in Cellular Calls?*

Before examining GPS, the issue of whether cellular telephones alone entail an expectation of privacy must be addressed. The issue is whether cellular calls themselves support a privacy right, in the absence of any GPS system within the telephone apparatus. If so, does this cellular privacy right exist when the calls are made in a public place outside the home or car?

According to the Fourth District Court of Appeals of Florida, cordless telephone conversations entail an expectation of privacy under both sections 12 and 23 of the Florida Constitution, article I.[80] In the *Mozo* court's decision, Justice Anstead stated that it was unimportant that cordless calls were not connected by wire to a land line telephone

80. Mozo v. State, 632 So. 2d 623, 631-38 (Fla. 4th Dist. Ct. App. 1994). The conclusion was later reviewed and affirmed by the Florida Supreme Court on non-constitutional grounds. State v. Mozo, 655 So. 2d 1115 (1995).

system.[81] The fact that cordless telephones were mobile and, in addition, could be intercepted more easily by the use of radio waves, did not lower the expectation of privacy associated with private telephone conversations.[82] Accordingly, the warrantless wire tap discussed in *Mozo* was held to be an unconstitutional invasion of privacy under both sections 12 and 23.[83]

Admittedly, cordless telephones are not the same as cellular phones, as they are less likely to be used in the privacy of one's home where section 12's Fourth Amendment expectation of privacy is strongest. Thus, the persuasive value of *Mozo* is merely analogical to the GPS scenario, and *Mozo* is not a binding precedent.

However, a cellular telephone system was reviewed under the federal scheme in the case of *United States for an Order Authorizing the Roving Interception of Oral Communications,* referred to here as *Roving.*[84] In this case, the Ninth Circuit did not use a constitutional theory for protecting privacy, but instead based its analysis on the federal wiretapping statute.[85] This statute, which is similar to the constitutional scheme in Florida, includes elements of privacy expectations, limits on government intrusion, and a narrowly-tailored requirement.

In *Roving,* the cellular telephone system under review was a built-in feature of a luxury car, giving the automobile cellular provider access to eavesdrop on its authorized subscribers.[86] The FBI sought an eavesdropping order from the automobile and cellular provider in *Roving,* but was denied this privilege because cellular telephones, even when used outside one's home, involve an expectation of privacy. Additionally, the order sought by the FBI could not be narrowly tailored under the circumstances.[87]

---

81. *Mozo*, 632 So. 2d at 634.

82. *Id.* at 634-35.

83. *Id.* at 632, 634.

84. United States for an Order Authorizing the Roving Interception of Oral Commc'ns, 349 F.3d 1132 (9th Cir. 2003).

85. *Id.* at 1136. 18 U.S.C. § 2510 (2002); 18 U.S.C. § 2511 (2002); 18 U.S.C. § 2518 (1998); 18 U.S.C. § 2522 (1994). Sections 2510 and 2518 were given closest attention in this case.

86. *Roving*, 349 F.3d at 1133-35.

87. *Id.* at 1144-46. Rather than using the constitutional term "narrowly-tailored," the circuit court referred to compliance with the eavesdropping order "unobtrusively and with *a minimum of interference.*" *Id.* at 1145. According to the circuit court, minimal interference (narrow tailoring) was not met because the eavesdropping order would unduly have invaded the expectation of privacy by forcing the automobile and cellular company's employees to continue using their resources to eavesdrop, and by disabling the user's ability to make outgoing calls. *Id.* at 1144-46.

Using language that resembles Fourth Amendment and section 12 (Florida Constitution) reasoning, the *Roving* court remarked that "the occupants of the vehicle reasonably expected that words spoken between them would be private, not subject to interception or transmission."[88] Therefore, an expectation of privacy was recognized with respect to cellular telephone communications within a private vehicle.

According to the circuit court, cellular telephones afforded the same degree of privacy as normal land-lines because they were in fact not "wireless" at all.[89] This is because wires and cables are physically part of the electronic mechanism enabling the wireless connection.[90] For this reason, the term "wireless" only relates to the end-user cellular telephone device, without altering the underlying wire-inherent nature of all telephone communications, including those that are portable.[91] The circuit court phrased its opinion in the following manner: "Despite the apparent wireless nature of cellular phones, communications using cellular phones are considered wire communications under the statute, because cellular telephones use wire and cable connections when connecting calls."[92]

Since cellular users have an expectation of privacy within the *Roving* context,[93] do cellular callers have a privacy expectation when they are not in a private car or other Fourth Amendment and section 12 private space? There is a strong argument that, as an extension of *Roving*, privacy in cellular calls made in public places may similarly be protected, given the *Roving* court's observation that cellular communications are indistinguishable from ordinary wire communications insofar as wiretapping, eavesdropping, and arguably similar government invasions of privacy are concerned.[94]

Also consider the Fifth District Court of Appeals of Florida case, *State v. McCormick*.[95] In *McCormick*, an interception order was sought by the police for cellular telephone calls under the Florida wiretap statute.[96] The calls intercepted were made in various locations, but not always in the

88. *Id.* at 1138.

89. *See id.*

90. *Id.*

91. *See Roving*, 349 F.3d at 1138.

92. *Id.*

93. *See id.*

94. *See id.* The circuit court stated that "communications using cellular phones are considered wire communications . . . ." *Id.*

95. State v. McCormick, 719 So. 2d 1220 (Fla. 5th Dist. Ct. App. 1998).

96. *Id.* at 1221; *see* FLA. STAT. ch. 934.07 (2002) & 934.09(1)(a) (2004). The Florida wiretap statute was modeled after its federal counterpart statute discussed in *Mozo* above, and is extremely similar to it.

user's private home or car.[97] The *McCormick* court reproduced the New Jersey Superior Court's comments from *State v. Tango* that "a cellular phone has no fixed location" for interception (and resulting privacy) purposes.[98] In *McCormick*, Justice Goshorn stated that an interception takes place both where the telephone is located (i.e. the cellular user's current location) and where the physical wiretap takes place.[99]

This analysis is relevant to interpreting the wiretap statute and not necessarily article I of the Florida Constitution, sections 12 and 23. However, *McCormick* reveals that a government intrusion into one's private cellular space occurs both at the cellular user's location and the wire-bound location where the government listens in.[100] Therefore, even if there is no privacy expectation where the cellular user is located, the user may still have a privacy expectation in the place where the wiretap occurs (even though the user is not physically present there).[101] As *Roving* states, cellular telephones are the same as land lines for privacy-interception purposes, due to the wire-bound nature of all telephone connections, cellular or otherwise.[102]

In short, the law is by no means clear on this issue. Yet a strong argument exists that cellular communications could entail privacy expectations under section 12, even when made or received outside one's private home, car, or hotel room. Even in the absence of a Fourth Amendment and section 12 privacy expectation, publicly made cellular calls may enjoy a broader privacy expectation found under article I, section 23 of the Florida Constitution. As discussed in Part II.C of this Article, many private communications and information types do not qualify for section 12 protection. However, these communications will satisfy section 23's less restrictive expectation of privacy standard, and thereby be shielded from government intrusion.

Accordingly, how can one determine whether cellular calls made in public meet the privacy standard of article I, section 23 of the Florida

---

97. *McCormick*, 719 So. 2d at 1221-23.

98. *Id.* at 1221.

99. *Id.* at 1222.

100. *Id.* However, this seems to be at odds with the Florida Supreme Court's decision in *State v. Mozo*, in which it was determined that "[t]he actual 'interception' of a communication occurs not where such is ultimately heard or recorded but where the communication originates." State v. Mozo, 655 So. 2d 1115, 1117 (Fla. 1995). In either case, the cellular user could argue that he had a constitutional expectation of privacy in the place where his calls were physically tapped.

101. *See Mozo*, 655 So. 2d at 1117. This inference is analogical to the *McCormick* court's findings, although *McCormick* does not specifically address any constitutional issues.

102. United States for an Order Authorizing the Roving Interception of Oral Commc'ns, 349 F.3d 1132, 1138 (9th Cir. 2003).

Constitution? To answer this question, cellular communications would have to meet the three-part *Shaktman* test discussed earlier.[103] A defendant would have to show that: (a) he subjectively perceived his cellular calls would remain private and free from government intrusion; (b) this perception was not spurious or false; and (c) no additional circumstances existed to defeat this alleged privacy expectation.[104]

There is no concrete answer to this question given the open-ended flexibility of the *Shaktman* test. Yet, taking the foregoing into account, it is not unlikely that cellular users have at least a section 23 privacy expectation, if not the more restrictive section 12 type.

B. *Technologies Which Extract Contentful Personal Information*

The legal principles addressed thus far become more complicated when a new variable is introduced into the equation: even though sections 12 and 23 may protect a privacy right in cellular conversations, can the same privacy expectation be claimed for contentless data? In other words, where contentless GPS data is part of a cellular telephone's functions, can it be relied on to claim a privacy expectation under the Florida Constitution?

Since there is no case law dealing with GPS and its relationship to sections 12 or 23, this issue will be approached by relying on case law from Florida and other jurisdictions addressing related privacy matters. The case law offers some, albeit limited, guidance into government intrusions on contentless technology (i.e., pocket pagers, tracking beepers, pen registers), which is instructive for our analogous GPS purposes. The cases discussed here arise in the search and seizure context, and therefore frame privacy expectations solely in the more restrictive section 12 (Fourth Amendment) sphere. These cases will nonetheless aid in locating privacy expectations in comparable circumstances under section 23.

The Washington Supreme Court recently commented,

> [T]he intrusion into private affairs made possible with a GPS device is quite extensive as the information obtained can disclose a great deal about an individual's life. For example, the device can provide a detailed record of travel to doctors' offices, banks, gambling casinos, tanning salons, places of worship, political party meetings, bars, grocery stores, exercise gyms, places where children are dropped off for school, play, or day care, the upper scale restaurant and the fast food restaurant, the strip club, the opera, the baseball

103. Shaktman v. State, 553 So. 2d 148, 153 (Fla. 1989) (Ehrlich, C.J., concurring specially).
104. *Id.* (Ehrlich, C.J., concurring specially).

> game, the "wrong" side of town, the family planning clinic, the labor rally.[105]

These judicial observations illustrate that GPS information does not constitute solely raw data. Indeed, GPS transmissions can disclose a great deal about one's private life and, in some situations, more detail than a private telephone conversation. This is despite a telephone conversation's content automatically enjoying a "reasonable expectation of privacy" under section 12 (Fourth Amendment) because of its inherently personal nature. Paradoxically, the same legal protection is not clearly afforded for GPS devices and the personal information GPS equipment transmits to others, including government authorities.

New technologies can detect private information about individuals which, until recently, was undetectable through ordinary human faculties. Keeping this in mind, the courts have sought to preserve the privacy expectations citizens previously enjoyed in the absence of these invasive new technologies.

For instance, people enjoy a reasonable expectation of privacy in whatever activity they pursue at home, even though police technology can virtually "see through" their homes to search for evidence. This was exemplified in *Kyllo v. United States,* where the police used thermal imaging technology that enabled them to detect drug activity inside the petitioner's home.[106] Police exploitation of this new technology was seen as a form of cheating, and on this basis, the Supreme Court found the police had conducted an illegal and warrantless search, violating petitioner's reasonable expectation of privacy.[107] Additionally, the Court stated even though no physical intrusion had occurred, the home was a constitutionally protected area and therefore, "'intrusion into a constitutionally protected area,' *Silverman,* 365 U.S., at 512, 81 S.Ct. 679, constitutes a search — at least where (as here) the technology in question is not in general public use."[108]

Accordingly, the U.S. Supreme Court formulated a new rule in 2001: the government can only conduct warrantless searches of constitutionally private information and places if it does so with unenhanced human senses or, at the very least, with sense-enhancing technologies which are in widespread use.[109] To this rule, Justice Scalia added:

---

105. State v. Jackson, 76 P.3d 217, 223 (Wash. 2003).
106. Kyllo v. United States, 533 U.S. 27 (2001).
107. *Id.* at 40.
108. *Id.* at 34.
109. *Id.* at 40.

> [I]f, without technology, the police could not discern volume without being actually present in the phone booth, Justice STEVENS should conclude a search has occurred. Cf. *Karo,* 468 U.S., at 735, 104 S.Ct. 3296 (STEVENS, J., concurring in part and dissenting in part) . . . . The same should hold for the interior heat of the home if only a person present in the home could discern the heat.[110]

Here, Justice Scalia refers to *Katz v. United States,* in which the technological enhancements of a "bug" permitted the government to listen in on the petitioner's private conversation while he was in a telephone booth.[111] Since the police would not have been able to overhear the petitioner's conversation with their normal human faculties in the absence of a wiretap warrant, the "bugging" technology enhancement was deemed an illegal search in violation of the petitioner's Fourth Amendment right to privacy.[112]

By contrast, visual enhancement technology that merely offers a better vantage point does not violate a person's expectation of privacy. As such, satellite aerial imaging in *Dow Chemical Co. v. United States* and airplane-view imaging in *California v. Ciraolo* and *Florida v. Riley* were deemed permissible searches by the U.S. Supreme Court, provided they did not invade areas immediately adjacent to a private home or peer into the home itself.[113] The Supreme Court ruled aerial views were "public thoroughfares" on which the police were not obligated to hide their eyes.[114] Additionally, referring to technological privacy invasions generally, the *Kyllo* Court critically remarked:

> It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology. For example, as the cases discussed above make clear, the technology enabling human flight has exposed to public view (and hence, we have said, to official observation) uncovered portions of the house and its curtilage that once were private. . . . The question we confront today is what

---

110. *Id.* at 39.

111. Katz v. United States, 389 U.S. 347 (1967).

112. *Id.* at 354-59.

113. Florida v. Riley, 488 U.S. 445, 450 (1989); California v. Ciraolo, 476 U.S. 207, 215 (1986); Dow Chem. Co. v. United States, 476 U.S. 227, 236-39 (1986).

114. *Ciraolo,* 476 U.S. at 213.

limits there are upon this power of technology to shrink the realm of guaranteed privacy.[115]

What distinguishes these cases, however, from the ones which follow is the contentful nature of the information retrieved by technological means. The foregoing cases generally recognize a section 12 (Fourth Amendment) privacy expectation where the government enables itself, through extraordinary technology, to see into private homes and listen into private telephone booths to intercept contentful private conversations. In order to frame these cases in contrast with others, the jurisprudence discussed in Part III.C below analyzes contentless personal information and its interception which, as will be revealed, presents a lesser threat to privacy. Even where contentless personal information is extracted from private spaces, it will be shown that a lesser expectation of privacy still exists.

C. *Technologies Which Extract Contentless Electronic Information*

First consider the use of numerical detection technology in the pen register line of cases. In the words of the U.S. Supreme Court, "[W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company . . . and similar devices are routinely used by telephone companies."[116] In *Smith v. Maryland*,[117] the U.S. Supreme Court majority deduced that no reasonable expectation of privacy existed in the telephone numbers dialed by an individual in the privacy of his home.[118] In *Smith*, police asked the local telephone company to electronically trace all telephone numbers dialed by a suspect, and the telephone provider did so using a pen register device which identified the clicking patterns of rotary telephones.[119] This operation was conducted without a warrant, yet in the absence of any reasonable expectation of privacy, the intrusion was held to be lawful.[120]

At this juncture, one must inquire as to why there is no expectation of privacy for the purely numerical data which rotary telephones provide. In other words, why does a telephone conversation merit a constitutional expectation of privacy, whereas the numbers dialed by the telephone do

115. *Kyllo*, 533 U.S. at 33-34.
116. Smith v. Maryland, 442 U.S. 735, 742 (1979).
117. *Id.*
118. *Id.*
119. *Id.* at 737-42.
120. *Id.* at 742-45.

not? This very point was raised by the petitioner in *Smith*. The Court observed, "Petitioner argues . . . that . . . he demonstrated an expectation of privacy . . . since he '[used] the telephone *in his house* to the exclusion of all others' [when the police recorded the telephone numbers he dialed]."[121]

While the petitioner's argument in *Smith* seems reasonable, the U.S. Supreme Court viewed this contentless, electronic type of private information in a different light. The Court stated, "Although petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct . . . could not . . . preserve the privacy of the *number* he dialed."[122] In other words, the content of telephone conversations is granted a higher status than numerical, non-content telephone data, regardless of how private in nature the latter may be.

Further, the fact that one's telephone information is extracted from the privacy of his home, a constitutionally protected space, is irrelevant. As the Supreme Court in *Smith* stated, "The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference."[123] One might ask why privacy is so easily discarded from a constitutionally protected space, such as one's private home, in these unique circumstances. The *Smith* Court explained that it is because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third persons."[124] According to the Court's reasoning, because telephone companies regularly track the numbers people dial for billing purposes, an individual is effectively forfeiting any privacy right once he hooks up a telephone and voluntarily uses it. On the other hand, because one does not regularly disclose his private telephone conversations to his carrier, the conversations themselves remain within one's expectation of privacy.[125]

Therefore, despite the Court's allusion to "content" in other portions of the *Smith* judgment, the underlying rationale for the Court's reasoning has little to do with the fact that phone conversations are contentful, while mere phone numbers are not.[126] Rather, the Court's reasoning appears to

---

121. *Smith*, 442 U.S. at 743.

122. *Id.* (citing Brief for Petitioner at 6). The Court's remarks here reflect a willingness to differentiate telephone conversation content from telephone numbers dialed for privacy purposes.

123. *Id.*

124. *Id.* at 743-44.

125. *See id.*

126. *See Smith*, 442 U.S. at 743-44.

depend on the *voluntariness* of turning over otherwise "private" information to third parties.[127]

At first blush, the U.S. Supreme Court's reasoning in *Smith* seems flawed because there is an absence of voluntariness and choice on the part of the telephone service subscriber. After all, one has no option but to have his telephone numbers tracked by his carrier if he is to be billed for his calls.

The U.S. Supreme Court's reasoning seems additionally dubious when the case law of Florida and other states is taken into account. Florida's equivalent to the Fourth Amendment, namely article I, section 12 of the Florida Constitution, has been used to create a reasonable expectation of privacy surrounding pen register data (e.g., *Shaktman v. State*),[128] in direct contrast to the *Smith* holding. Thus, as the *Shaktman* case exposes, the view of the Florida Supreme Court regarding pen register data and its privacy differs sharply from that of the U.S. Supreme Court.

Furthermore, the Florida Supreme Court's reasoning in *Shaktman* completely undermines that of the U.S. Supreme Court in *Smith*, by pointing out that individuals do not voluntarily surrender their numbers to their telephone company.[129] It follows that, in Florida, one's privacy expectation is not affected by the fact that the telephone company knows what numbers an individual has dialed.[130] When commenting on the privacy invasion potential of pen register technology, the Florida Supreme Court noted that "[t]he telephone numbers an individual dials . . . represent personal information which . . . the individual has no intention of communicating to a third party. This personal expectation is not defeated by the fact that the telephone company has access to that information."[131]

Here, the Florida Supreme Court chose to adopt the position of the Colorado Supreme Court in *People v. Sporleder*[132] on pen register privacy, rather than aligning itself with the U.S. Supreme Court and the existing *Smith* precedent.[133] The Supreme Court of Hawaii has similarly held that people have a reasonable expectation of privacy in the numerical electronic data that their telephones emit, particularly in the numbers they dial, as per *State v. Rothman*.[134] The fact that there is no traditional

127. *See id.*
128. Shaktman v. State, 553 So. 2d 148, 151 (Fla. 1989).
129. *Id.*
130. *Id.*
131. *Id.*
132. People v. Sporleder, 666 P.2d 135, 141 (Colo. 1983).
133. *Shaktman*, 553 So. 2d at 151.
134. Hawaii v. Rothman, 779 P.2d 1, 7 (Haw. 1989).

"content" to the numbers dialed, and no conversation intercepted, does not reduce the right of privacy attached to this electronic telephone-based data.[135]

At first impression, it appears that *Shaktman* creates a divergence between article I, section 12 of the Florida Constitution and the Fourth Amendment, insofar as electronic telephone data and its privacy is concerned. However, this appearance is deceiving because the 1982 amendments to the Florida Constitution brought section 12 in line with the Fourth Amendment, and thereafter prohibited Florida from providing any greater privacy than the Fourth Amendment afforded. In other words, Florida's expectation of privacy in electronic, contentless telephone data (under *Shaktman*) was likely overturned by the U.S. Supreme Court's 1979 *Smith* decision after the Florida constitutional amendments in 1982.

Even in 1981, the shrinking scope of section 12 privacy protection was foreshadowed by the Florida Supreme Court in *Dorsey v. State*. In *Dorsey*, Justice Overton commented on pocket pagers stating that "[w]e . . . hold that there can be no expectation of privacy in 'beeper' messages sent over the airwaves and that these messages are not protected by Florida's wiretap law."[136] This remark is instructive of Florida's position on pen registers as well, since a pocket pager is so similar to a pen register in terms of retrievable data.[137] Judging from this stance, the Florida Supreme Court has not always been committed to preserving *Shaktman*'s expectation of privacy in telephone numbers (and similar numerical communications), and *Shaktman* would eventually lose its legally binding character as the Fourth Amendment was merged with the Florida Constitution.

D. *Technologies Which Extract Contentless Electronic Information: Those Most Analogous to GPS*

Pen register data and GPS are similar in that both are contentless, electronic, often generated by telephones and, to a certain extent, both are locational in nature. It follows that the Florida cases on pen registers and pocket pagers are relevant to any future GPS-related decisions by the Florida courts since, to date, there are no existing Florida authorities on GPS privacy.

---

135. *Id.*

136. Dorsey v. State, 402 So. 2d 1178, 1180 (Fla. 1981).

137. Note, for analogy's sake, that the type of information retrieved from pocket pagers is similar to that extracted from a pen register, since both electronic instruments permit the interception of telephone numbers dialed, but do not retrieve the conversational content of the calls.

Yet, in addition to the pen register and pocket pager cases, this Article will consider other telephone-based electronic data which could prove analogous to GPS. One could consider, for instance, the case law pertaining to non-GPS electronic tracking devices. There are no cases discussing GPS in relation to article I, section 23 of the Florida Constitution, yet two prominent U.S. Supreme Court cases[138] address the Fourth Amendment privacy implications of "tracking beepers." These devices are defined as "a radio transmitter, usually battery operated, which emits period signals that can be picked up by a radio receiver."[139] Thus, the tracking beepers referred to in this line of cases are a close cousin of modern GPS trackers, and provide similar locational information about private individuals.

United States v. Knotts stands for the principle that a tracking beeper can be planted freely on private individuals, since the beeper does not invade any expectation of privacy so long as it does not reveal the contents of a constitutionally protected space[140] (i.e. a private locker, home, or phone booth) and the same information could have been obtained by the government through ordinary visual surveillance.[141]

A year later, in *United States v. Karo*, the U.S. Supreme Court clarified this issue.[142] According to *Karo,* tracking beepers do not change the fact that individuals enjoy a reasonable expectation of privacy in their constitutionally protected spaces.[143] Thus, a tracking beeper which reveals information about a constitutionally protected private space amounts to a "search," and therefore violates one's reasonable expectation of privacy.[144] Nonetheless, the Court in *Karo* established a lesser standard for electronic tracking "searches" than physical searches, observing that "[t]he monitoring of an electronic device such as a beeper is, of course, *less intrusive* than a full-scale search, but it does reveal a critical fact about the interior of the premises that the Government . . . could not have otherwise obtained without a warrant."[145]

Therefore, whether one's reasonable expectation of privacy is invaded depends on whether the same information could have been obtained by the government through ordinary visual surveillance. Ordinary visual

138. United States v. Karo, 468 U.S. 705 (1984); United States v. Knotts, 460 U.S. 276 (1983).
139. *Knotts,* 460 U.S. at 277.
140. *Id.* at 285.
141. *Id.*
142. *Karo,* 468 U.S. at 715-16.
143. *Id.*
144. *Id.*
145. *Id.* at 715 (emphasis added).

surveillance does not include surveillance involving superhuman capabilities that electronic tracking devices afford. Even if the police physically view an object being moved into a private home from the exterior, in the absence of an attached tracking device, the police could not have known how long the item remained in the home, or that the tracked object had not been removed.[146] This additional information is not obtainable through ordinary visual surveillance and government acquisition of it would therefore violate the Fourth Amendment's privacy protections under *Karo*.[147]

As the Court in *Karo* insisted,

> For the purposes of the [Fourth] Amendment, the result is the same where, without a warrant, the Government surreptitiously employs an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house . . . . Even if visual surveillance has revealed that the article to which the beeper is attached has entered the house, the later monitoring . . . also establishes that the article remains on the premises.[148]

Based on the Court's reasoning in *Karo*, government entities should not use tracking devices at all, since doing so would create a risk that "superhuman" information will be extracted in violation of constitutional privacy. Rarely is it possible to obtain the same information through visual surveillance as one would acquire with an electronic tracking device.

Hypothetically, apply the *Karo* reasoning to GPS devices in cellular telephones. The facts of the cellular telephone scenario are distinguishable because the police generally do not plant GPS tracking devices into cell phones. Cellular telephones are already equipped with GPS locators when voluntarily purchased. Yet, considering *Karo* as applied to a police suspect tracked through cell phone GPS, the tracking would likely amount to the "superhuman" type of surveillance the U.S. Supreme Court condemned in *Karo,* namely the type which invades a person's expectation of privacy (in a private car, home, or wherever the locational data was retrieved). Concededly, the same tracking data would not have been possible through

---

146. *Id.*

147. *Karo*, 468 U.S. at 715.

148. *Id.* This is not unlike the reasoning of the Fifth District Court of Appeals of Florida in *Johnson v. State,* in which a tracking beeper had been placed on an airplane without a warrant, amounting to an "illegal entry." Johnson v. State, 492 So. 2d 693, 694 (Fla. Dist. Ct. App. 1986).

ordinary visual surveillance, unless conducted twenty-four hours a day. As the Washington Supreme Court commented in *State v. Jackson*,

> [U]nlike binoculars or a flashlight, the GPS device does not merely augment the officer's senses, but rather provides a technological substitute for traditional visual tracking. Further, the devices in this case were in place for approximately two and one-half weeks. It is unlikely that the sheriff's department could have successfully maintained uninterrupted 24-hour surveillance throughout this time by following Jackson.[149]

Jackson is instructive because, rather than concerning the outdated form of a tracking beeper, it involved an actual GPS locator that the police had planted on a suspect's car. The *Jackson* court analyzed these facts using a Washington State constitution provision similar to the Fourth Amendment and Florida's article I, section 12. In *Jackson,* the privacy invasion was clear. There was indeed an expectation of privacy in one's locational data, and invasive GPS tracking should not be viewed on the same plane as harmless visual surveillance (contrary to the approach taken in *Knotts*).[150] The Washington Supreme Court stated, "We do not agree that the use of the GPS devices to monitor Mr. Jackson's travels merely equates to following him on public roads where he has voluntarily exposed himself to public view."[151]

The *Jackson* decision was reached through consideration of *State v. Campbell,* a tracking beeper case from the Oregon Supreme Court.[152] Referring to *Campbell*, the *Jackson* court observed that "use of a device that enabled the police to locate a person within a 40-mile radius day or night 'is a significant limitation on freedom from scrutiny' and 'a staggering limitation upon personal freedom.'"[153] *Jackson* emphasized the invasiveness of GPS technology on personal privacy, stating that "the intrusion into private affairs made possible with a GPS device is quite extensive."[154]

The opposite approach was taken by the Ninth Circuit U.S. Court of Appeals in *United States v. McIver.*[155] Like *Jackson, McIver* is one of the

---

149. State v. Jackson, 76 P.3d 217, 223 (Wash. 2003) (emphasis added).
150. *Id.* at 223-24.
151. *Id.*
152. *Id.* at 224 (referring to State v. Campbell, 759 P.2d 1040 (Or. 1988)).
153. *Id.*
154. *Jackson*, 76 P.3d at 223.
155. United States v. McIver, 186 F.3d 1119 (9th Cir. 1999).

few cases directly addressing privacy rights in connection with GPS technology.[156] Yet, unlike *Jackson,* the *McIver* court found no privacy invasion in GPS locational data, so long as the government's GPS instrument was attached to the exterior of one's car and not the car's interior.[157] The circuit court noted that a government intrusion into the interior of one's private car would be an entirely different matter and would indeed have raised Fourth Amendment concerns.[158] In *McIver,* the Fourth Amendment question did not require further analysis because the police GPS device had been attached to the exterior of the defendant's vehicle.[159]

The curious pattern which *McIver* reveals is that some courts gauge locational data relative to the placement of the tracking instrument, without considering whether the data itself might threaten constitutional privacy.[160] By contrast, *Jackson* shows that some courts consider the actual data obtained and its relation to privacy, without regard to the placement of the tracking instrument.[161] It seems likely that, as GPS instruments become more common, the courts will eventually harmonize these two contrasting analyses. Yet, at the present time, it is unclear which model should be followed. In the *Jackson* type of analysis, the retrieved data is what constitutes a constitutional privacy invasion. Only the tracking device's placement inside a protected space has entered the court's debate since the *McIver* model. The locational data is not even considered as personal information.

Applying these two contrasting models to the GPS data of cellular telephones is challenging because it is not clear which type of legal reasoning is appropriate. However, *Jackson* is arguably better adapted to the physical nature of cell phones because government action in the cellular telephone realm is largely limited to wiretapping, including the court-ordered interception of GPS locational data. The government will almost never physically plant a tracking device in one's telephone. This important fact virtually eliminates the utility and applicability of the *McIver* analysis to cell phone GPS.

By contrast, the *Jackson* reasoning remains relevant to the cellular telephone environment because only data is retrieved when a government-ordered GPS wiretap occurs. Thus, with only the extracted GPS data

156. *Id.* at 1126-27.
157. *Id.*
158. *Id.*
159. *Id.*
160. *McIver,* 186 F.3d at 1126-27.
161. State v. Jackson, 76 P.3d 217, 222-25 (Wash. 2003).

available for the courts to examine (and no beeper placement), *Jackson*'s discussion of what government-retrieved GPS data discloses is more pertinent to cell phones than the *McIver* physical-search rationale.

Finally, since the *Jackson* court found a Fourth Amendment (article I, section 12 of the Florida Constitution) expectation with respect to GPS locational information, it follows that the broader section 23 type of privacy almost certainly would exist.

To date, there is only one American case which considers the privacy of GPS data based specifically on whether the GPS device in question is part of a cellular telephone. For guidance and clarification, this case is examined more closely in the following section of this Article.

E. *Technologies Which Extract Contentless Electronic Information: When GPS is Part of the Cellular Telephone*

In *United States for an Order Authorizing the Roving Interception of Oral Communications* (*Roving*),[162] the Ninth Circuit Court of Appeals did not discuss constitutional privacy, but instead dealt with GPS cellular privacy by addressing the federal wiretapping and interception statute.[163] This wiretapping analysis is nonetheless pertinent to the constitutional debate on GPS cellular privacy. In fact, the *Roving* court makes various assertions about GPS cellular privacy which coincide with the Florida courts' own constitutional reasoning for sections 12 and 23. They could easily be imported into this body of Florida jurisprudence in the current absence of constitutional cases addressing GPS subject matter.

In *Roving*, the FBI sought a federal wiretap order to intercept the cellular communications and GPS locational data of certain suspects.[164] These suspects were known to own a particular luxury vehicle, and all models of this luxury car were equipped internally with a GPS-cellular device.[165] The car company had an independent manufacturer for the GPS devices, which had a call center through which it tracked its cars' GPS location, when required, and managed all cellular calls.[166] Owners of the company's vehicles would regularly contact the call center with their internal cellular telephone to receive driving directions, emergency assistance, or directions to nearby restaurants and services, and were billed

---

162. United States for an Order Authorizing the Roving Interception of Oral Commc'ns, 349 F.3d 1132 (9th Cir. 2003).

163. 18 U.S.C. § 2510 (2002); 18 U.S.C. § 2511 (2002); 18 U.S.C. § 2518 (1998); 18 U.S.C. § 2522 (1994). Sections 2510 and 2518 were given closest attention in this case.

164. *Roving*, 349 F.3d at 1133-37.

165. *Id.*

166. *Id.*

in proportion to the airtime used.[167] In case of an airbag eruption, the car's cellular sytem was automatically activated to communicate with the client and ensure safety.[168] On the basis of these facts, the *Roving* court determined that the car company was a cellular service provider, offering a "wire or electronic communications service," much like any other cellular telephone company.[169] The device in the car was similarly deemed to be like any other GPS-equipped cellular telephone.[170]

The question raised in *Roving* is whether, absent a court order to track and eavesdrop on the GPS-cell phone user, does the owner of the device have a reasonable expectation of privacy, both in his locational data and private conversations. Treating the integrated GPS and cellular components as one unit, the circuit court said that the users indeed had an expectation of privacy, because "the occupants of the vehicle reasonably expected that the words spoken between them would be private."[171] Thus, an interception order was necessary before the cellular provider, on behalf of police, could listen in on the user's private conversations. In *Roving*, the police were denied such an interception order.[172]

In this way, the telephone's GPS element enjoyed the privacy protection afforded to personal conversations. Had the GPS unit been part of a separate, non-telephonic device, it is unclear that any expectation of privacy would have been recognized by the court. The *Roving* court chose to remain silent on this specific issue, however, and mentioned little of the GPS component at all.

What was clear about the GPS-cellular unit was that the car company was statutorily bound to hold its clients' locational and telephonic information in strict confidence, thereby reinforcing the expectation of privacy underlying the GPS devices and the data they transmit. The federal statute, 18 U.S.C. § 2702(b), provides that carriers cannot disclose their clients' GPS-cellular information in the absence of a government warrant, unless they do so with the clients' consent or when the company's GPS-

---

167. *Id.* at 1133-34.

168. *Id.* at 1134.

169. *Roving*, 349 F.3d at 1140-41.

170. *Id.*

171. *Id.* at 1138.

172. *Id.* at 1144-47. The interception order was denied because it could not have been accomplished "with a minimum of interference," under the circumstances. *Id.* at 1144. This is because the clients, while being eavesdropped on, could not make any outgoing communications to the call center, and therefore would not benefit from the cellular service they had paid for. *Id.* at 1144-46. The minimal intrusiveness (narrow tailoring) requirement also applied to the GPS manufacturer, whose resources and personnel would have been drained by carrying out the FBI's interception order for 4 months of 24-hour surveillance. *Id.*

cellular data shows that a crime is underway. This statute states that a carrier may disclose a client's GPS or cellular communications information "to a Federal, State, or local government entity, if the provider, in good faith, believes that an emergency involving danger or death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."[173] Although purely speculative, it may be this urgency which entitles the carrier to eavesdrop on clients and locate them with GPS every time an airbag is activated.

In short, even though a court does not engage in constitutional analysis, *Roving* supports a presumption that there is a privacy expectation in GPS, provided that the GPS apparatus is integrated into a cellular telephone.

IV. CLOSING CONSIDERATIONS

A. *What Is the Privacy Trend in the Florida Legislature?*

Although the authorities discussed here generally suggest some degree of privacy protection in GPS information, whether there is a trend in the Florida legislature supporting this protection is a separate question. Assuming, based on the foregoing case law and discussion, that article I, sections 12 and 23 of the Florida Constitution support a GPS privacy expectation, would the current Florida legislature agree?

There are two GPS bills which have been proposed in the Florida legislature. Although they do not address personal GPS location data in cellular telephones, and may never become law, both bills illustrate a trend to remove GPS privacy protection, rather than expand it under sections 12 or 23.

In brief, House Bill 1283 has been introduced to require the 24-hour GPS monitoring of certain types of sex offenders. There is also House Bill 0943, which will require bail bond agents to enforce the GPS locational tracking of any pre-trial releasees. Both bills are intended to use GPS technology in a way that removes any expectation of privacy in one's locational information, albeit only for indicted or convicted persons *already* in some form of detention. Nonetheless, if the Florida legislature has any concerns about the use or abuse of spreading GPS technologies, its concern does not seem to be directed at the privacy threat which GPS might pose constitutionally under sections 12 or 23 of article I.

---

173. 18 U.S.C. § 2702(b) (2002).

B. *Observations and Final Analysis*

1. Section 23

As the foregoing Florida cases and discussion suggest, section 23 (article I) of the Florida Constitution has a greater possibility of extension to GPS subject matter than section 12. Yet, the greatest challenge to section 23 is the balancing test it entails.[174] That is to say, while section 23 may support an expectation of privacy in some GPS subject matter, the applicable balancing test is so restrictive that a privacy right rarely survives it. Under section 23 analysis, the compelling state interest frequently wins out when balanced against the alleged privacy right.[175] This is not surprising since very little can be expected to take precedence over a compelling state interest, including a fundamental constitutional right. The Florida case law considered here attests to this fact,[176] as does the federal case law which originally inspired the creation of Florida's section 23.[177]

There is one further obstacle to section 23's protection of GPS privacy, and that is the third prong of the *Winfield* test.[178] After the claimant's privacy expectation is established, the government may show that it had a compelling state interest in obtaining the claimant's personal information, and that it obtained such information through the "least intrusive means."[179] Unfortunately for claimants of GPS privacy or any privacy expectation, the government can often defeat a section 23 argument by meeting this "least intrusive means" prong. As many cases show, this is because a search warrant or subpoena is the "least intrusive means" and therefore meets the third and final requirement of the *Winfield* test.[180] Similarly, a court order under Florida's wiretapping and interception statute[181] would presumably meet the "least intrusive means"

---

174. Forsberg v. Hous. Auth. of Miami Beach, 455 So. 2d 373, 379 (Fla. 1984).

175. *Id.* at 379-80; Winfield v. Div. of Pari-Mutuel Wagering, 477 So. 2d 544, 548 (Fla. 1985); Shaktman v. State, 553 So. 2d 148, 152 (Fla. 1989).

176. *See* cases cited *supra* note 175.

177. Whalen v. Roe, 429 U.S. 589, 602-06 (1977); California Bankers Ass'n v. Schultz, 416 U.S. 21, 52-54 (1974).

178. *Winfield,* 477 So. 2d at 548.

179. *Id.*

180. *Id.*

181. Under Florida Statutes chapter 934.01,

> [T]he Legislature makes the following findings: . . . (4) To safeguard the privacy of innocent persons, the interception of wire or oral communications when none of the parties to the communication has consented to the interception should be

threshold, thereby canceling out the claimant's section 23 legitimate privacy expectation.

2. Section 12

The section 12 test also poses barriers which may restrict the courts' ability to find an expectation of privacy in GPS locational subject matter. As summarized above, the law does not clearly show that section 12 supports a privacy expectation for publicly-made cellular communications. It is even less clear that section 12 might protect GPS data alone (in the absence of cellular communication).

Yet, even if there were a reasonable expectation of privacy under these tests, a court could find that one's personal GPS data was not unlawfully seized or intercepted if the government obtained a wiretap or interception order in advance. Most cases recognize searches as "reasonable," avoiding constitutional scrutiny, where a warrant has been obtained to authorize a police search.[182] It follows that a wiretap or interception court order would similarly fulfill this "reasonableness" requirement under article I, section 12 of the Florida Constitution (Fourth Amendment).

C. *Conclusion*

In short, the subject matter covered by section 23's disclosural privacy cannot be delineated with a simple, bright-line test. Admittedly, the reach of Florida Constitution article I, section 23 remains to be developed and expanded in the case law. However, both section 23 and, to a lesser extent, section 12 have the potential to support an expectation of privacy in purely cellular telephone conversations. It is less apparent that sections 12 and 23

> allowed only when authorized by a court of competent jurisdiction . . . . Interception of wire and oral communications should further be limited to certain major types of offenses and specific categories of crime . . . .

FLA. STAT. ch. 934.01 (2002). However, it is not entirely clear that a court is authorized to make a GPS interception order under this statute. This is because Florida Statutes chapter 934.01 only permits interception and wiretap orders for "wire and oral communications." FLA STAT. ch. 934.02(1) (defining "wire communication" as a means requiring "the aid of wire, cable or other like connection"). FLA STAT. ch. 934.02(2) (2002) (defining "oral communication" as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation and does not mean any public oral communication uttered at a public meeting or any electronic communications"). However, GPS data cannot qualify as an "electronic communication" because Florida Statutes chapter 934.02(12) explicitly prohibits it.

182. Kyllo v. United States, 533 U.S. 27, 40 (2001).

could support a privacy expectation in GPS data alone. Yet, once a GPS device is integrated within a cellular telephone, the marriage of these two functions affords greater privacy to one's GPS information. The case law reviewed above supports this view.

Having made this assertion, one must consider that even where section 23 may allow a privacy expectation in GPS data, the law may prevent a constitutional privacy interest from being assured. This is because Florida's constitutional privacy under article I, sections 12 and 23 is so easily defeated by a police search warrant or an interception order.

The section 23 balancing test is also a barrier, since this test prioritizes the state's compelling interest ahead of the individual's constitutionally guaranteed rights. As the case law presented here illustrates, many state interests can be construed as compelling, certainly where crime prevention is the state interest at issue.

Considering the totality of these factors, section 12 or 23 may assure GPS-cellular privacy only where government intrusion into GPS data has been made without a warrant, subpoena, or any other indicator of "minimal intrusiveness." Furthermore, as argued here, a GPS-cellular privacy claimant would have greater success relying on section 23 than the more restrictive section 12.

Although there are no firm answers to these privacy questions in the Florida cases, all hope is not lost for GPS privacy and its potential for constitutional protection. Future Florida jurisprudence will bear important landmarks in the use and privacy of locational GPS, a technology which has suddenly become widespread and whose role in public life is expanding at an alarming rate. At present, the Florida legislature may not recognize an expectation of privacy in GPS data. However, the fundamentals exist for the Florida Supreme Court to conclude otherwise, paving the way for other states to follow.