GPS Technology in cellular telephones:
Does Florida's constitutional privacy protect
against electronic locating devices?

Peter Caldwell

I - INTRODUCTION

GPS technology is not new, but in the recent past has become so widespread that it now affects most everyone's life. 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 are able to locate their users wherever they may be, if required to do so.

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. On this basis, the present commentary will address whether or not individuals have an expectation of privacy in the GPS information which their cellular telephones transmit. In arriving at this objective, we will lend particular attention to the Florida Constitution's two privacy provisions, namely section 12 and 23 of article 1.

Throughout the first portion of this comment, we will therefore closely examine the rules, uses and potential applications of section 12 and 23 alone, without regard to GPS technology at first. This initial discussion will establish the framework for our subsequent hypothetical applications of section 12 and 23 jurisprudence to cellular telephone communications, contentless locational technology, and finally, to GPS itself. By considering the application of section 12 and 23 to this broad range of technology, we hope to contextualize any potential GPS privacy these two provisions might protect.

Since there is no Florida case law directly addressing the question of GPS-cellular devices under section 12 or 23, much of the following analysis will be the product of legal conjecture and prediction. However, the case law related peripherally to this subject matter

provides a strong indication of what should become the Florida courts' future position on GPS privacy, and will therefore serve as a predictor of future legal reasoning.

Yet, in order to arrive at such an advanced point in our analysis, let us first begin by elaborating the constitutional privacy framework for article 1, sections 12 and 23 of the Florida Constitution.

II - THE FLORIDA CONSTITUTION

Much like the United States Constitution, the Florida Constitution protects the privacy of its people in several ways. In addition to the constitutional privacy which protects decisional autonomy,[1] 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 1, section 12 of the Florida consitution, which states that:

> 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

[1]This references the decisional autonomy crafted by the U.S. Supreme Court in its landmark contraception rights decision, *Griswold v. Connecticut,* 381 U.S. 479 (1965), and was created as an implicit extension of constitutional substantive due process. It was also deemed to have been derived from several constitutional amendments, rather than from a single explicit constitutional provision. This type of 'privacy' protects one's personal choices from state intervention in the areas of child-rearing, contraception, marriage, and so on.

The same privacy right to decisional autonomy exists under article 1, section 23 of the Florida Constitution, as evidenced by *In re T.W.,* 551 So. 2d 1186 (Fla. 1989), in which the rights of a minor to terminate her pregnancy were analyzed by the Florida Supreme Court. However, the decisional autonomy aspect of section 23 will not be dealt with in this comment; instead, we will consider whether cellular GPS technologies, when used by government entities, could amount to a privacy violation under article 1, section 23.

> Amendment to the United States Constitution, as interpreted by the United States Supreme Court ...[2]

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

There is, however, a second type of privacy guaranteed by the Florida Constitution. This second constitutional privacy right is located in article 1, 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.[3]

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,[4] but also is invoked to prevent government disclosure of personal information[5] and the state's own acquisition of proprietary information[6] without the owner's

---

[2]Fla. Const. art I, § 12 (1994).
[3]Fla. Const. art. I, § 23 (1998).
[4]*In re T.W.,* 551 So. 2d at 1190. This case involved the personal autonomy right of a women and her fundamental right to make contraception choices.
[5]*Rasmussen v. South Florida Blood Service, 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. The privacy interests of blood donors, under section 23, article 1 of the Florida Constitution, outweighed the plaintiff's interest in receiving this information.
[6]*Mozo v. State,* 632 So. 2d 623 (Fla. 4th DCA 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). When appealed to the Florida Supreme Court, the same decision was reached. Yet, since it could be reached more simply without discussion of sections 12 and 23, the Supreme Court avoided addessing the constitutional issues: *State v. Mozo,* 655 So. 2d 1115, 1117 (Fla. 1995).

consent.[7] It is the latter (non-decisional) coverage of section 23 that will be addressed in this comment, rather than the personal autonomy scope of this provision.

Since GPS technologies may involve potential privacy invasions through warrantless government searches for criminal evidence, the possible application of section 12, article 1 will be addressed in our analysis which 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 a government entity is attempting to obtain locational information for other purposes.

Within this framework, we will consider the extent to which either section 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.

2.1 Section 12, Article 1 of the Florida Constitution: its scope

The Florida courts have re-iterated that, since the 1982 amendment of section 12, the legal analysis applied to section 12 should be the same at that used for the Fourth Amendment of the U.S. Constitution.[8] Because this is so, the Florida courts must rely on the precedential case law from the U.S. Supreme Court itself, and the developments which that court permits to evolve over time. For this reason, we shall 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)

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

whether, if a search was conducted, it was nonetheless "reasonable" enough to avoid constitutional privacy scrutiny.[9] Ordinarily, a warrant authorizing a search or the consent of the searched individual will render the search "reasonable."

The Fourth Amendment and section 12, article 1 of the Florida Constitution both require freedom from unreasonable government intrusion into the constitutionally protected areas of a citizen's life,[10] including one's private home, car, hotel room, phone booth, locker, and so on. For this reason, a warrantless search of one's home or car is unconstitutional in Florida, absent the owner's consent.[11] 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.[12] Thus, mere visual surveillance of the exterior of one's home or car does not constitute an intrusion or search and is therefore lawful.[13]

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 to not 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]

---

[8]*Madsen v. Florida,* 502 So. 2d 948, 949 (Fla 4th DCA 1987).
[9]*Kyllo v. United States,* 533 U.S. 27 (2001).
[10]*Silverman v. United States,* 365 U.S. 505, 511 (1961) states this value for the Fourth Amendment. Section 12 of the Florida Constitution similarly states this principle. Fla. Const. art I, § 12 (1994).
[11]*Illinois v. Rodruigez,* 497 U.S. 177, 181 (1990); *Tollett v. State,* 272 So. 2d 490, 493 (Fla. 1973).
[12]*Silverman,* 365 U.S. at 510-12.
[13]*Boyd v. United States,* 116 U.S. 616, 628 (1986).
[14]*Minnesota v. Carter,* 525 U.S. 83, 104 (1998) (Breyer, J., concurring in judgment).
[15]In *Dow Chemical v. United States,* 476 U.S. 227, 235-35 (1986), the U.S. Supreme Court ruled that the government had not illegally searched a manufacturer's private curtilage areas when using satellite aerial imaging. 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.

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, and the presence of a suspect inside.[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 a word, 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]

2.2 Section 23, Article 1 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 ruled to the contrary.[21] On the sum of these

[16] *Kyllo,* 533 U.S. at 34.
[17] *Id.*
[18] *Id.*
[19] *Id.* at 40.
[20] As Professor Robert Whorf has noted:

> Florida courts have generally endeavored to minimize confusion created by the apparent overlap of section 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.

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. Let us 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, phone booth, and so on. Like sectionn 12, section 23 also requires an expectation of privacy, but does not mandate that he 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, unlike section 12 privacy. Chapter **2.3** 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 section 12 and 23 privacy, there is indeed a zone of overlap where both section 12 and 23 can protect a citizen's personal information under the

---

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). Professor Whorf makes this latter remark while 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,' " citing *State v. Hume,* 512 So. 2d 185, 188 (Fla. 1987). The 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. This is the underlying rationale for keeping sections 12 and 23 as separate as possible in scope.

[21]For instance, in *Mozo v. State,* 632 So. 2d at 631-38, Justice Anstead of the 4th District Court of Appeal reasoned that both section 12 and 23 of the Florida Constitution, Article 1, should apply to cordless telephone conversations electronically intercepted by police, without a warrant, from outside a suspect's home. 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. *Id.* Nor did the fact that the matter was one of a criminal nature.

Additionally, in *Winfield v. Division of Pari-Mutuel Wagering,* 477 So. 2d 544 (Fla. 1985), the government had subpoenaed a citizen's banking records for a criminal investigation. Section 23 of the Florida Constitution, article 1, 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

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, Department of Business Regulation is the leading case in Florida establishing the legal parameters of section 23, article 1.[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 United States 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 the section 23, article 1 analysis is for the court to determine whether or not the individual actually has a "legitimate expectation of privacy."[27] In *Winfield,* the Supreme Court of Florida recognized that the petitioners did have a valid expectation of privacy in their personal banking records, and the maintenance of their confidentiality. If the individual relying on section 23 does not possess this reasonable expectation, the court will not pursue the analysis further, and the government may obtain access to the personal information it seeks.[28]

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 to obtain the individual's personal information.[29] This 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 of the individual must be weighed against the

---

zone of overlap which entails the privacy protections of both sections 12 and 23 of the Florida Constitution, article 1.

[22]*State v. Hume,* 512 So. 2d 185 (Fla. 1987).

[23]*Winfield,* 477 So. 2d at 546-48.

[24]*Id.* at 547.

[25]*Roe v. Wade,* 410 U.S. 113, 152 (1973).

[26]*Id.*

[27]*Id.*

public interest."[30] 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.[31]

Finally, the third prong of the *Winfield* test requires the government to show that it obtained or attempted to obtain the private information concerned through the least intrusive means.[32] If this prong is met, the government's compelling interest will successfully outweigh the section 23 privacy interest of the citizen in question.[33] 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.[34]

2.2.1 What does section 23 cover?

Although the foregoing three-part test has been set out clearly in *Winfield,* there remains much which we do not know about section 23, article 1 of the Florida Constitution. For our purposes, it would be useful to understand how broadly section 23 can be applied to personal information, and to what range of information types. Section 23's scope is particularly important, since understanding it may assist us in determining how, analogously, its scope might translate into any potential GPS privacy protection.

---

[28] *Id.*
[29] *Id.*
[30] *Forsberg,* 455 So. 2d. 373, 379 (Fla. 1984) (Overton, J., concurring in judgment).
[31] *Winfield,* 477 So. 2d at 548.
[32] *Id.* at 547.
[33] *Id.*
[34] *Id.* at 548.

The Florida case law tells us that section 23 can form a legitimate expectation of privacy surrounding the following personal information: personal banking privacy and records,[35] personal autopsy records,[36] cordless telephone communications intercepted by the police,[37] the private data emanating from a telephone pen register (ie. intercepted "caller ID"),[38] the private identification information of blood donors, even in the face of a subpoena,[39] and medical and other personal information contained in the files of judicial proceedings, unless a formal "sealing" has been ordered.[40]

On the other hand, section 23 does not create a legitimate expectation of privacy in the following areas: personal information, such as private email found in a government computer,[41] records providing the personal information of tenants and all other persons who ever applied to live in public housing complexes,[42] the contentless private data emitted from a personal pocket pager or "beeper," when intercepted by the police,[43] privileged medical or psychiatric reports, when disclosed to the state bar for admission to practice,[44] and personal information regarding one's smoking habits.[45]

Thus, the classes of personal information which can be protected by section 23 are, at the present time, not defined by any precise rule. To date, what constitutes a reasonable expecation of privacy for section 23 has been a matter of judicial discretion in Florida. Until many more

---

[35]*Id.*
[36]*Campus Communications v. Earnhardt,* 821 So. 2d 388 (Fla. 5th DCA 2002).
[37]*Mozo v. State,* 632 So. 2d 623 (Fla. 4th DCA 1994). On appeal, this case was decided by the Florida Supreme Court on a non-constitutional basis: *State v. Mozo,* 655 So. 2d 1115 (Gla. 1995). However, the fact that this matter was ruled on by the Supreme Court on different grounds does not rule out the otherwise valid constitutional legal analysis made by Justice Anstead in his decision from the 4th District Court of Appeal.
[38]*Shaktman v. State,* 529 So. 2d 711 (Fla. 3rd DCA 1988); *Shaktman v. State,* 553 So. 2d 148 (Fla. 1989).
[39]*Rasmussen v. South Florida Blood Service, Inc.,* 500 So. 2d 533 (Fla. 1987).
[40]*Barron v. Florida Freedom Newspapers, Inc.,* 531 So. 2d 113 (Fla. 1988); *Cape Publications, Inc., v. Hitchner,* 549 So. 2d 1374 (Fla. 1989).
[41]*State v. City of Clearwater,* 863 so. 2d 149 (Fla. 2003).
[42]*Forsberg,* 455 So. 2d at 374.
[43]*Dorsey v. State,* 402 So. 2d 1178 (Fla. 1981).
[44]*Florida Board of Bar Examiners Re: Applicant,* 443 So. 2d 71 (Fla. 1984).
[45]*City of North Miami v. Kurtz,* 653 so. 2d 1025 (Fla. 1995).

cases have been tried by the Florida courts, the defining threshold between unprotected privacy and protected subject matter shall remain a blurred line.

What is clear is that section 23, article 1 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,[46] U.S. constitutional cases show considerable reticence to recognize the discosural 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.[47] 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."[48] 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.[49]

---

[46]*Forsberg,* 455 So. 2d at 374-80 (Overton, J., concurring in judgment); *Forsberg* set the stage for *Winfield,* which immediately followed it and adhered largely to Overton's concurrence in *Forsberg. Winfield,* 477 So. 2d at 547-48.

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 which section 23 guarantees. *Id.* at 546. He remarked that those federal Supreme Court cases should be limited to privacy in connection with personal autonomy, stating that "[o]ther 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." *Id.*

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

[47]*Whalen v. Roe,* 429 U.S. 589, 605 (1977).

[48]*Id.* at 605.

[49]In *Whalen v. Roe,* the Supreme Court ruled on a New York law requiring doctors to report patient prescription drug information to the state government. *Id.* at 589-99. 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.* The U.S. Supreme Court used the balancing test which would later be adopted into Florida's section 23 privacy analysis [*supra,* note 46], but was reluctant to formally assert a fundamental right to non-disclosural, non-invasive privacy under the U.S. constitution. *Whalen,* 429 U.S. at 605. The "penumbra" of rights underlying U.S. constitutional privacy, as espoused in prior case law, [*Griswold v. Connecticut,* 381 U.S. 479 (1965)], did not as clearly apply to the non-disclosural privacy context. *Whalen,* 429 U.S. at 605.

As professor Erwin Chemerinsky has observed, "although there is a strong argument that the [United States] Constitution should be interpreted to protect a right to control information, there is thus far little support for such a right from the [United States] Supreme Court."[50]

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.[51] 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, "[a]lthough 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."[52]

Justice Overton took this observation further in his scholarly writings, where he and Katherine Giddings wrote that, "[a]rticle I, section 23 affords greater protection from government intrusion than the federal Constitution. The privacy right is explicit, it extends to all

---

Similarly, in *California Bankers Association 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 their bank transactions being disclosed to the government. *California Bankers Association v. Schultz,* 416 U.S. 21 (1974).

[50]ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES, 2ND ED., 827.

To a certain extent, this may be regarded as an anomaly in the law's evolution, since Florida 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 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, <u>as against the Government, the right to be let alone</u>.

Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (emphasis added). Thus, the concept of a "right to be left alone" originated in U.S. Supreme Court interpretations of the federal constitution, and were later imported into the Florida state constitution's consideration of its 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. *Whalen,* 429 U.S. 589 at 605; *California Bankers Association v. Schultz,* 416 U.S. 21 (1974).

[51]*Winfield,* 477 So. 2d at 548; *Forsberg,* 455 So. 2d at 377.

[52]*Forsberg,* 455 So. 2d at 377.

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."[53]

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, notes 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 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.[54]

The judicial commentary of Justices Adkins and Overton are instructive. They aid us in determining that section 23 was intended to form a stronger right than federal constitutional

---

[53]Ben F. Overton & Katherine E. Giddings, *The Right of Privacy 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 (1997).

[54]*Winfield,* 477 So. 2d at 548.

By contrast with these remarks that section 23 privacy is stronger than the federal constitution's, Professor 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 state 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 (1997), referring to the Florida Supreme Court decision of *Shevin v. Byron, Harless, Schafer, Reid & Associates,* 379 So. 2d 633 (Fla. 1980). However, what is not apparent from Professor Lenz's observations is that the *Shevin* case is not used for section 23 disclosural privacy analysis, as it was rendered shortly before the adoption of section 23, article 1 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-

privacy, and one which could be compromised only in special circumstances. Yet these commentaries, even when accompanied by the section 23 case law, 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.

2.3. The same 'expectation of privacy' under both section 12 & 23?

As discussed in the preceding section, privacy under section 12, article 1 of the Florida Constitution is limited to places where one enjoys a reasonable expectation of privacy,[55] such as a private home, inside one's car, in their hotel room, in their private papers,[56] and so on. 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, or personal property or information which is outside one's vehicle rather than inside it.[57]

By contrast, section 23, article 1 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, Department of Business Regulation,* a citizen's private bank accounts were deemed to fall within the legitimate

---

disclosure, anti-invasiveness privacy than the highly undeveloped Federal brand discussed earlier in the cases of *Whalen* and *Schultz. Whalen,* 429 U.S. 589 (1976); *California Bankers Association v. Schultz,* 416 U.S. 21 (1974).

[55]*Kyllo,* 533 U.S. 27 at 31.

[56]*United States v. Miller,* 425 U.S. 435 (1976).

[57]The Fourth Amendment, which is analyzed in the same way as article 1, 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: *United States v. McIver,* 186 F.3d 1119 (1999).

expectation of privacy contemplated by section 23, but not the zone of privacy considered for section 12 or the Fourth Amendment.[58]

Yet while the subject matter coverage of these two privacy provisions differ, the formulas used to identify a privacy expectation under section 12 and 23 are, in many respects, related. As will be revealed below, expectations of privacy under section 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 24 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.[59] 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 its physical location.[60]

Second, section 12 (i.e. Fourth Amendment equivalent) privacy requires that the individual claiming the privacy right have, in some way, manifested their own subjective expectation of privacy with regard to their private space or information.[61] This subjective manifestation of privacy, however, must pass a second test: the information or place must be one which society would objectively regard as private.[62] For this reason, the Fourth Amendment/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 the court's equation. This additional measure avoids situations where one has subjectively manifested their

[58] *Winfield,* 477 So. 2d at 547. Although the Florida Supreme Court did acknowledge 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.*
[59] *Kyllo,* 533 U.S. 27 at 33, which was based on the Fourth Amendment, although the same analysis is in section 12, article 1 case law with respect to the Florida Constitution.
[60] *Mozo v. State,* 632 So. 2d at 633.
[61] *Id.*

expectation, but the expectation is one which clearly is 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 we 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.[63] For this reason, the case law refers to a "legitimate expectation of privacy" for section 23,[64] but a "reasonable expectation of privacy" for section 12.[65]

The Florida case law has further confirmed this distinction between section 12 and 23 expectations, and as Justice Anstead (then of the 4th District Court of Appeal) remarked in *Mozo v. Florida,* "[a] major analytical difficulty faced by the federal courts in ... the Fourth Amendment [ie. 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."[66]

Similarly, in *Shaktman v. State,* Chief Justice Ehrlich of the Florida Supreme Court explained that section 23 expectations do not have to be "reasonable" because society's endorsement of a section 23 privacy expectation is not required.[67] This is in direct contrast with the second "objective" prong of the section 12 privacy test. Justice Erlich, concurring specially, stated that "[t]he words 'unreasonable' and 'unwarranted' harken back to the federal standard of

---

[62]*Kyllo, 533* U.S. at 31, 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." *Id.*
[63]*Winfield,* 477 So. 2d at 548.
[64]*Id.*
[65]*Kyllo,* 533 U.S. 27 at 33.
[66]*Mozo,* 632 So. 2d at 633.
[67]*Shaktman,* 553 So. 2d at 153 (Ehrlich, C.J., concurring speciallly).

'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."[68]

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 that test.

In Justice Eherlich's words, "the 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."[69] Justice Ehrlich provides the third and most objective criteron, which serves to defeat the expectation of privacy (despite having passed the first two prongs) if the facts show that the disputed information is of an inherently public nature[70], or for other reason should not be deemed as private.[71]

---

[68] *Id.* (Ehrlich, C.J., concurring specially).
[69] *Id.* (emphasis added).
[70] *Id.;* The *Forsberg* decision provides an example which illustrates this final criterion. In *Forsberg,* the appellants did not have an expectation of privacy in public housing records containing personal information about them. *Forsberg,* 455 So. 2d at 379 (Overton, J., concurring). It was not that personal data was not of a private character, but 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.*
[71] In sum, Justice Eherlich'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 their 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 available "objective" manifestations ("objective" prong) or facts which support a finding of privacy or lacking privacy (e.g. the information is already highly public, which defeats the expectation of privacy claimed). *Id.*

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 (iii) objective factor brings section 23 expectations of privacy closer to the section 12 test, since both contain a subjective (individual-based) prong and an objective (factually or societally-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 which the case law pretends it represents.[72]

Despite the similarities between section 23 and 12 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 (ie. police-intercepted caller ID) does not bear a reasonable expectation of privacy under section 12.[73] However, the same pen register data was sufficiently private to present a section 23 legitimate expectation of privacy.[74] 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," the court ruled.[75]

Similarly, in *Winfield,* we reiterate that the privacy of bank records was not protected by the Fourth Amendment or article 1, section 12 of the Florida Constitution.[76] By contrast, under

[72]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; *Kyllo,* 533 U.S. 27 at 33. (ii) the claimant must have manifested his subjective expectation of privacy with regard to the disputed information ("subjective" prong); *Id.* (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). *Id.*
[73]*Shaktman,* 553 So. 2d at 151.
[74]*Id.*
[75]*Id.*
[76]*Winfield,* 477 So. 2d at 547.

Winfield a legitimate expectation of privacy was found in the same private bank records under the section 23 analysis.[77]

In short, the tests used to identify an expectation of privacy under sections 12 and 23 differ only slightly. Even so, section 25 expectations have been able to cover a broader range of subject matter because section 12 is limited where private things are located in non-private spaces.

III - SECTION 12 & 23 CONSTITUTIONAL PRINCIPLES APPLIED TO GPS

Having set out the framework and possible applications of the Florida Constitution, article 1, sections 12 and 23, it is possible at this juncture 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 comment.

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

3.1 Locating expectations of privacy in GPS: Analogies drawn from Florida & non-Florida case law

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

[77] *Id.*

3.2 Is there an expectation of privacy in cellular calls?

Before examining GPS, let us first address the issue of whether cellular telephones alone entail an expectation of privacy. That is to say, do the 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 Florida 4th District Court of Appeal, cordless telephone conversations entail an expectation of privacy under both section 12 and 23 of the Florida Constitution, article 1.[78] In the court's *Mozo* decision, Justice Anstead said that it was unimportant that cordless calls were not connected by wire to a land line telephone system.[79] 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.[80] Accordingly, the warrantless wire tap discussed in *Mozo* was held to be an unconstitutional invasion of privacy under both sections 23 and 12.[81]

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 (Fourth Amendment) privacy is strongest. Thus, the persuasive value of *Mozo* is merely analogical to the GPS scenario, and therefore *Mozo* is not a clearly binding precedent.

However, a cellular telephone system was reviewed under the federal scheme in the case of *United Stated for an Order Authorizing the Roving Interception of Oral Communications,*

---

[78] *Mozo,* 632 So. 2d at 631-38; conclusion later reviewed and affirmed by the Florida Supreme Court on non-constitutional grounds: *State v. Mozo,* 655 So. 2d 1115 (1995).
[79] *Id.*
[80] *Id.*
[81] *Id.*

referred to here as *Roving.*[82] In this case, the Ninth Circuit federal court did not use a constitutional theory for protecting privacy, but instead based its analysis on the federal wiretapping statute,[83] which (similar to the constitutional scheme in Florida) includes elements of privacy expectations, limits on government intrusion, and a narrow-tailoring requirement.

In *Roving,* the cellular telephone system under review was a built-in feature of a luxury car, giving the automobile company/cellular provider the capability of eavesdropping on its users, when authorized to do so.[84] The FBI had sought an eavesdropping order from the automobile/cellular provider in *Roving,* but was denied this privilege because cellular telephones, even when used outside one's home, involved an expectation of privacy and the order sought by the FBI could not be narrowly tailored under the circumstances.[85]

Using language which resembles Fourth Amendment/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."[86] An expectation of privacy was therefore recognized with respect to cellular telephone communications contained in a private vehicle.

According to the court, cellular telephones afforded the same degree of privacy as normal land-line telephones, because they were in fact not "wireless" at all.[87] This is because wires and

---

[82]*United States for an Order Authorizing the Roving Interception of Oral Communications,* 349 F.3d 1132 (9th Cir. 2003) [hereinafter "*Roving*"].
[83]18 U.S.C. 2510; 18 U.S.C. 2511; 18 U.S.C. 2518; 18 U.S.C. 2522. Sections 2510 and 2518 were given closest attention in this case.
[84]*Id.* at 1133-35.
[85]*Id.* at 1144-46. Rather than using the constitutional term 'narrowly-tailored' however, the court referred to compliance with the eavesdrop order "unobstrusively and with a minimum of interference." *Id.* at 1145. According to the court, minimal interference (narrow tailoring) was not met because the eavesdropping order would unduly have invaded the expectation of privacy by forcing the automobile/cellular company's employees to continue using their resources to eavesdrop, and by disabling the user's ability to make outgoing calls for four months. *Id.* at 1144-46.
[86]*Id.* at 1138.
[87]*See id.*

cables are physically part of the electronic mechanism enabling the wireless connection.[88] For this reason, the term "wireless" only relates to the end-user cellular telephone device, and does not alter the underlying wire-inherent nature of all telephone communications, including those which are cellular and portable.[89] The court phrased this 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."[90]

Thus, *Roving* states that cellular users have an expectation of privacy in the facts of the case.[91] By extension, does this mean that cellular calls have a privacy expectation when they do *not* occur in a private car or other Fourth Amendment/Section 12 private space? There is a strong argument that *Roving* can be likened to protect cellular call privacy in public places as well, given the court's observation that cellular communications are indistinguishable from ordinary wire communications,[92] insofar as wiretapping, eavesdropping and (presumably) similar government invasions of privacy are concerned.

Let us also consider the Florida 5th District Court of Appeal case, *State v. McCormick.*[93] In this matter, an interception order was sought by the police for cellular telephone calls under the Florida wiretap statute.[94] The calls intercepted were made in various locations, but not necessarily in the user's private home or car.[95] The *McCormick* court cites the New Jersey Superior Court's comments from *State v. Tango* that "a cellular phone has no fixed location,"

[88] *Id.*
[89] *See id.*
[90] *Id.*
[91] *See id.*
[92] *See id.;* the court stated that, "communications using cellular phones are considered wire communications." *Id.*
[93] *State v. McCormick,* 719 So. 2d 1220 (Fla. 5th DCA 1998).
[94] In particular, FLA. STAT. ch. 934.07 and 934.09(1)(a). The Florida wiretap statute was modeled on its federal counterpart statute discussed in *Mozo* above, and is extremely similar to it.
[95] *McCormick,* 719 So. 2d at 1221-23.

for interception (and resulting privacy) purposes.[96] Justice Goshorn of the *McCormick* court then proceeds to state 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; that is to say, the location where the police actually eavesdrop on the call.

Admittedly, this is relevant to interpreting the wiretap statute and not necessarily the Florida constitution, sections 23 and 12, article 1. However, it 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.[97] This means that, 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).[98] This is because, as *Roving* states, cellular telephones are the same as land lines for privacy-interception purposes, due to the physically wire-involved nature of *all* call connections, cellular or otherwise.[99]

In short, the law is by no means clear on this issue, but there is a strong argument that a section 12 privacy expectation may exist in cellular calls made or received outside one's private home, car, hotel room, and so on. Yet, even if there is no section 12/Fourth Amendment privacy expectation for cellular communications in public places, there is likely a privacy expectation of the broader type found under article 1, section 23 of the Florida Constitution. As our discussion in part **2.3** of this comment revealed, many private communications and information do not

---

[96]*Id.* at 1221.
[97]*Id.* at 1222. However, this seems to be at odds with the Florida Supreme Court's decision in *State v. Mozo,* 655 So. 2d 1115, 1117 (Fla. 1995), 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." *Id.* 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.
[98]*See id.;* This inference is analogical to the *McCormick* court's findings, although *McCormick* does not specifically address any constitutional issues.
[99]*Roving,* 349 F.3d at 1138.

qualify for section 12 privacy, but will satisfy section 23's less restrictive expectation of privacy standard, and thereby become shielded from government intrusion.

Do cellular calls made in public meet the privacy standard of article 1, section 23 of the Florida Constitution? To answer this question, cellular communications would have to meet the three-part *Schaktman* test discussed earlier.[100] A defendant would have to show that (a) he subjectively perceived his cellular calls would remain private and free from government intrusion; (b) that this perception was not spurious or false; and (c) that no additional circumstances existed to defeat this alleged privacy expectation.[101]

There is no concrete answer to this question, but given the foregoing criteria, it is not unlikely that cellular users have at least a section 23 privacy expectation, if not the type found in section 12.

3.3 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 23 and 12 may protect a privacy right in cellular conversations, can the same privacy expectation be claimed for contentless data? That is to say, where contentless GPS data is part of a cellular telephone's functions, can it be relied upon to claim a privacy expectation under the Florida Constitution?

Since there is no case law dealing with GPS and its relationship to sections 23 and 12, this issue will be approached by relying on the Florida and non-Florida cases addressing peripheral, yet related, privacy matters. The case law offers some, albeit limited, guidance into government intrusions on contentless technology (e.g. pocket pagers, tracking beepers, pen registers, etc.), which is instructive for our analogous GPS purposes. The cases discussed here

[100] *Shaktman,* 553 So. 2d at 153 (Ehrlich, C.J., concurring specially).
[101] *Id.*

arise in the search & seizure context, and therefore frame privacy expectations solely in the Section 12 (Florida Constitution)/Fourth Amendment sphere, but will aid us in locating section 23 privacy expectations in comparable circumstances.

As the Supreme Court of Washington recently said, "[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 game, the 'wrong' side of town, the family planning clinic, the labor rally."[102]

As these observations illustrate, GPS information is not pure data. It can disclose a great deal about one's private life and, in some situations, with much more detail than a private telephone conversation, even though the contents of a telephone conversation automatically enjoy a "reasonable expectation of privacy" under section 12/Fourth Amendment because of its personal information. The same protection, by contrast, is not so clear for GPS devices and the arguably personal information they transmit.

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

For example, people still enjoy a reasonable expectation of privacy for whatever they pursue in their homes, even though contemporary police technology can virtually "see through" their homes, in search of evidence. This was the case of thermal imaging technology used by

[102] *State v. Jackson,* 150 Wash. 2d 251, 262 (Wash. 2003).

police in *Kyllo v. United States,* which enabled law enforcement to detect drug production activity inside the petitioner's home.[103] 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.[104] Even though no physical intrusion had occurred, the home was a constitutionally protected area and therefore, " 'intrusion into a constitutionally protected area,' *Silverman,* 36 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."[105]

This was the new rule formulated by the U.S. Supreme Court 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 very least, with sense-enhancing technologies which are in widespread use.[106] To this rule, Justice Scalia added:

> [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.[107]

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.[108] Since the police would not have been able to overhear the petitioner's conversation with their normal human faculties, the "bugging"

[103] *Kyllo v. United States,* 533 U.S. 27 (2001).
[104] *Id.* at 39.
[105] *Id.* at 34.
[106] *Id.* at 39.
[107] *Id.*
[108] *Katz v. United States,* 389 U.S. 347 (1967).

technology enhancement was deemed an illegal search in violation of Fourth Amendment privacy (in the absence of a wiretap warrant).[109]

By contrast, visual enhancement technology which 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.[110] Aerial views were deemed 'public thoroughfares' on which the police were not obligated to hide their eyes, the Supreme Court ruled.[111] In response to this type of technological privacy invasion, 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 limits there are upon this power of technology to shrink the realm of guaranteed privacy.[112]

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, though extraordinary technology, to see into private homes and listen into private telephone booths to intercept *contentful* private conversations. Unlike these cases, the jurisprudence presented below analyzes *contentless* personal information and its interception which, as will be revealed, presents a lesser threat to privacy. This appears to be the case even

[109] *Id.* at 354-58.
[110] *Florida v. Riley,* 488 U.S. 445 (1989); *California v. Ciraolo,* 476 U.S. 207 (1986); *Dow Chemical Co. v. United States,* 476 U.S. 227, 234-35 (1986).
[111] *Ciraolo,* 476 U.S. at 213.
[112] *Kyllo,* 533 U.S. at 33-34 (emphasis added).

where such contentless personal information is extracted from private spaces, depending on the facts of each case.

3.4 Technologies which extract *contentless* electronic information, from private telephones in particular

Let us first consider the use of numerical detection technology in the pen register line of cases. "[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."[113] These are the remarks of the United States Supreme Court in *Smith v. Maryland,*[114] whereby the majority deduced that no reasonable expectation of privacy existed in the telephone numbers dialed by an individual in the privacy of his home.[115] In this case, the police had 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.[116] This operation was conducted without a warrant, yet even in the absence of any reasonable expectation of privacy, the intrusion was held to be lawful.[117]

At this juncture, we must ask why there is no expectation of privacy for the purely numerical data which rotary telephones generate. Why does a conversation merit an expectation of privacy, while the numbers dialed by the telephone used do not? Indeed, this point was raised by the petitioner in *Smith*: "[p]etitioner argues ... that ... he demonstrated an expectation of privacy ... since he 'us[ed] the telephone *in his house* to the exclusion of all others.' "[118]

---

[113] *Smith v. Maryland,* 442 U.S. 735, 742 (1979).
[114] *Id.*
[115] *Id.*
[116] *Id* at 737-42..
[117] *Id.* at 742-43.
[118] *Id.* at 743.

While this argument seems reasonable, the U.S. Supreme Court viewed the contentless, electronic type of private information in a different light: "[a]lthough 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."[119] Otherwise stated, 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 their home, a constitutionally protected space, is irrelevant. As the *Smith* court stated, "[t]he fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference."[120] 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."[121]

Thus, 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 they hook up a telephone and voluntarily use it. On the other hand, because one does not regularly disclose their private telephone conversations to their carrier, the conversations themselves remain within one's expectation of privacy.[122]

Therefore, despite's the court's allusion to "content" in other portions of the *Smith* judgment, as cited, 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.[123] Rather, the

[119] *Id.* (emphasis added). The court's remarks here reflect a willingness to differentiate telephone conversation content from telephone numbers dialed, for privacy purposes.
[120] *Id.*
[121] *Id.* at 743-44.
[122] *See id.*
[123] *See id.*

court's reasoning appears to dwell in the voluntariness of turning over information to third parties (i.e. to one's telephone service provider in this case).[124]

At first blush, the U.S. Supreme Court's *Smith* reasoning 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 their telephone numbers tracked by their carrier if they are to be billed for their 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 1, section 12 of the Florida Constitution, has been used to create a reasonable expectation of privacy surrouding pen register data (in *Shaktman v. State)*,[125] 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 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.[126] For this reason, one's privacy expectation is not affected by the fact that the telephone company knows what numbers an individual has dialed.[127] 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 that information."[128]

---

[124]*See id.*
[125]*Shaktman,* 553 So. 2d at 151.
[126]*Id.*
[127]*Id.*
[128]*Id.*

Here, the Florida Supreme Court chose to adopt the position of the Colorado Supreme Court in *People v. Sporleder*[129] on pen register privacy, rather than aligning itself with the U.S. Supreme Court and the existing *Smith* precedent.[130] The Supreme Court of Hawai'i has similarly held that people have a reasonable expectation of privacy for the numerical electronic data which their telephones emit, particularly the numbers they dial: *State v. Rothman*.[131] The fact that there is no traditional "content" to the numbers dialed, and no conversation intercepted, does not reduce the right of privacy attached to this electronic telephone-based data.[132]

At first impression, it therefore appears that *Shaktman* creates a divergence between article 1, section 12 of the Florida Constitution and the Fourth Amendment, insofar as electronic telephone data and its privacy is concerned. However, this is deceiving because the 1982 amendments to the Florida Constitution brought section 1 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, but not until the Florida constitutional amendments took place in 1982.

Yet, even in 1981, the retracting nature of section 12 privacy was foreshadowed by the Florida Supreme Court when, in *Dorsey v. State,* Justice Overton commented about pocket pagers: "[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."[133] This remark is instructive for Florida's position on pen registers as well, since a pocket pager is so similar to

[129] *People v. Sporleder,* 666 P.2d 135, 141 (Colo. 1983).
[130] *Shaktman,* 553 So. 2d at 151.
[131] *Hawaii v. Rothman,* 779 P.2d 1, 7 (Haw. 1989).
[132] *Id.*
[133] *Dorsey v. State,* 402 So. 2d 1178, 11880 (Fla. 1981)

a pen register in terms of retrievable data.[134] Judging from this stance, the Florida Supreme Court was not always so committed to *Shaktman'*s expectation of privacy in private telephone numbers, even though *Shaktman* would eventually lose its force as the Fourth Amendment was merged with the Florida Constitution.

3.5 Technologies which extract *contentless* electronic information: Those most analogous to GPS

As a further matter of analogy, it is worth noting that electronic pen register information is similar to GPS data in that both are contentless, electronic, generated by telephone devices and, to a certain extent, both are locational in nature. It follows that the Florida case law governing pen registers and pocket pagers is relevant to a future GPS finding by the Florida courts. For the present time, however, let us consider other telephone-based electronic data which could prove even more analogous to GPS functions, beginning with non-GPS electronic tracking devices.

Although there are no cases discussing GPS in relation to article 1, section 23 of the Florida Constitution, two prominent U.S. Supreme Court cases[135] 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."[136] 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

[134]Let us 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.
[135]*United States v. Karo,* 468 U.S. 705 (1984); *United States v. Knotts,* 460 U.S. 276 (1983).
[136]*Knotts,* 460 U.S. at 207.

as it does not reveal the contents of a constitutionally protected space[137] (e.g. a private locker, home, phone booth, etc.) and the same information could have been obtained by the government through ordinary visual surveillance.[138]

A year later, in *United States v. Karo* the United States Supreme Court clarified this issue.[139] According to *Karo,* tracking beepers do not change the fact that individuals enjoy a reasonable expectation of privacy in their constitutionally protected spaces:[140] their homes, curtilage, lockers, hotel rooms, private papers, cars, and so on. 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.[141] However, in *Karo,* the court seems to have established a lower standard for electronic tracking "searches" than physical searches: "The 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."[142]

Whether one's reasonble expectation of privacy is invaded therefore depends on whether the same information could have been obtained by the government through ordinary visual surveillance; that is to say, *ordinary* visual surveillance, and not surveillance involving the superhuman capabilities which electronic tracking devices afford. Thus, even if the police physically view an object being brought into a private home, in the absence of an attached tracking device, they could not have known how long the item remained in the home, or learned that the tracked item had not been removed.[143] This is additional information not obtainable through ordinary visual surveillance, and would therefore violate the Fourth Amendment's

[137] *Knotts,* 460 U.S. at 285.
[138] *Id.*
[139] *Karo,* 469 U.S. at 715-16.
[140] *Id.*
[141] *Id.*
[142] *Id.* at 715 (emphasis added).

privacy protections under *Karo*.[144] As the *Karo* court observed, "[f]or 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."[145]

Based on the *Karo* court's reasoning, it is therefore in the interest of government not to use tracking devices at all, since doing so will create a risk that 'superhuman' information will be extracted in violation of privacy rights. Rarely is it possible to obtain the same (ie. no more) information through visual surveillance as one would acquire with an electronic tracking device.

Let us hypothetically apply this *Karo* analysis to the context of GPS devices in cellular telephones. The facts of the cellular telephone scenario are, of course, distinguishable because the police generally do not plant GPS devices into cell phones as they planted tracking beepers in *Karo* and *Knotts.* Cellular telephones are already equipped with GPS mechanisms. Yet, if we consider *Karo* as applied to a police suspect tracked through cell phone GPS, the tracking would likely amount to the "superhuman" type and thus invade one's expectation of privacy (in one's car, house, or wherever the locational data was retrieved from). This is because, in most cases, the same tracking data would not have been possible through ordinary visual surveillance, unless conducted twenty-four hours a day. As the Washington Supreme Court commented in *State v. Jackson,* "unlike 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

---

[143] *Id.*
[144] *Id.*

unlikely that the sherriff's department could have successfully maintained uninterrupted 24-hour surveillance throughout this time by following Jackson."[146]

The *Jackson* case is instructive because, rather than concerning an outdated form of tracking beeper, it involved an actual GPS locator which the police had planted on a suspect's car. The *Jackson* court analyzed these facts using a Washington statute constitution provision similar to the Fourth Amendment and Florida's article 1, section 12. In this late 2003 case, 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*): "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."[147]

The *Jackson* court arrived at this conclusion by considering *State v. Campbell,* a tracking beeper case from the Oregon Supreme Court.[148] Referring to this judgment, 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' "[149] As addressed earlier, the *Jackson* court went to great lengths to emphasize how invasive GPS technology is on one's private life, saying that "the intrusion into private affairs made possible with a GPS device is quite extensive."[150]

---

[145]*Id.;* This is not unlike the reasoning of the Florida Court of Appeal in *Johnson v. State,* 492 So. 2d 693, 694 (Fla. DCA 1986), in which a tracking beeper had been placed on an airplane without a warrant, amounting to an "illegal entry."
[146]*State v. Jackson,* 76 P.3d at 223 (emphasis added).
[147]*Id.*
[148]*Id.* at 224, referring to *State v. Campbell,* 759 P.2d 1040 (Or. 1988).
[149]*Id.*
[150]*Id.* at 223.

The opposite approach was taken by the 9th circuit U.S. Court of Appeals in *United States v. McIver.*[151] Like *Jackson, McIver* is one of few cases directly addressing privacy rights in connection with GPS technology.[152] 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*.[153] 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, the court noted. [154] In any event, in *Jackson,* the latter question did not have to be explored further because the police had attached a GPS tracking instrument to the exterior of the defendant's vehicle.[155]

The curious pattern which the foregoing cases expose is that some courts gauge locational data based on the placement of the tracking instrument, and do not consider whether the data itself might threaten constitutional privacy.[156] By contrast, other courts consider the actual tracking data obtained, without regard to the placement of the tracking instrument.[157] It seems likely that as GPS instruments become more common, the courts will eventually harmonize their analyses. Yet, at the present time, it is unclear which model should be followed: a *Jackson*- style analysis in which the retrieved data is what constitutes a constitutional privacy invasion, or rather, the *McIver* model in which the locational data is not even considered as personal information because only the tracking device's placement inside a protected space enters the court's debate.

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. It seems likely

[151] *United States v. McIver,* 186 F.3d 1119 (9th Cir. 1999).
[152] *Id.* at 1126-27.
[153] *Id.*
[154] *Id.*
[155] *Id.*
[156] *Id.*

that *Jackon* is better adapted to the physical nature of cellular telephones, however. Since 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 much more applicable to the cellular telephone environment because *data alone* is retrieved when a government-ordered GPS wiretap occurs. Thus, with only the extracted GPS data available for the courts to examine (and no beeper placement), *Jackson'*s discussion of what government-retrieved GPS data discloses, seems far more pertinent to cellular phones than the *McIver* physical-search rationale.

Since a Fourth Amendment/Section 12 expectation was found in *Jackson* 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 specifically where 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 comment.

3.6 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* (hereinafter "*Roving*"),[158] the 9th Circuit Court of Appeal did not discuss constitutional privacy, but instead dealt with GPS cellular privacy by addressing the federal

[157] *Jackson,* 76 P.3d at 222-25.
[158] *United States for an Order Authorizing the Roving Interception of Oral Communications,* 349 F.3d 1132 (9th Cir. 2003) (hereinafter "*Roving*").

wiretapping/interception statute.[159] 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 23 and 12, and could easily be imported into this body of jurisprudence (in the current absence of other constitutional case law treating this subject matter).

In this late 2003 case, the FBI sought a federal wiretap order to intercept the cellular communications and GPS locational data of certain suspects.[160] 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.[161] The car manufacturer had a call center through which it tracked its cars' GPS location, when required, and managed all cellular calls.[162] To receive driving directions, emergency assistance, or directions to nearby restaurants and services, owners of the company's vehicles would regularly contact the call center with the internal cellular telephone, and were billed in proportion to the airtime used.[163] In the case of an airbag eruption, the cellular sytem was automatically activated to communicate with the client.[164] On this basis, 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.[165] The device in the car was similarly deemed to be like any other GPS-equipped cellular telephone.[166]

Absent a court order to track and eavesdrop on the GPS-cell phone users, did the owners have a reasonable expectation of privacy, both in their locational data and their private conversations? Treating the integrated GPS and cellular components as one unit, the court said

[159]18 U.S.C. 2510; 18 U.S.C. 2511; 18 U.S.C. 2518; 18 U.S.C. 2522. Sections 2510 and 2518 were given closest attention in this case.
[160]*Id.* at 1133-37.
[161]*Id.*
[162]*Id.*
[163]*Id.* at 1140-46.
[164]*Id.* at 1134.
[165]*Id.* at 1140.

that the users had an expectation of privacy, because "the occupants of the vehicle reasonably expected that the words spoken between them would be private."[167] Thus, an interception order was necessary before the cellular provider could listen in on ther user's private conversations, and was denied in this case.[168]

In this way, the telephone's GPS component benefited from the privacy protection of the 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 in it. The *Roving* court chose not to express an opinion on this matter and, in fact, makes very little mention of the GPS component at all.

What is clear about the GPS-cellular unit is that the car company is statutorily bound to hold its clients' locational and telephonic information in strictest confidence, thereby reinforcing the expectation of privacy underlying these 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 client's consent or when the company's GPS-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 injury to any person requires disclosure without delay of communication relating to the emergency."[169] Perhaps it is this urgency which entitles the

---

[166] *Id.*
[167] *Id.* at 1138.
[168] *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 1144-45. The minimal intrusiveness (narrow tailoring) requirement also applied to the car 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.* at 1144-46.
[169] 18 U.S.C. 2702(b).

carrier to eavesdrop on clients and locate them with GPS, every time a client's airbag is activated.

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

IV - CLOSING CONSIDERATIONS

4.1 What is the privacy trend in the Florida legislature?

Although many of the authorities discussed here suggest some degree of privacy protection in GPS information, it is worthwhile asking whether this is supported by the prevailing trends in the Florida legislature. If we assume, based on the foregoing case law and discussion, that article 1, sections 12 & 23 of the Florida Constitution support a GPS privacy expectation, would the current Florida legislature approve of this?

In fact, 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 23 or 12.

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 which removes any expectation of privacy in one's locational information, albeit only for indicted or convicted persons 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 under sections 12 or 23 of the Florida Constitution, article 1.

4.2 Observations and final remarks

As the foregoing Florida cases and discussion reveal, **section 23** of the Florida Constitution has a greater possibility of being extended to GPS subject matter than section 12. Yet, the greatest challenge to section 23 is the balancing test it entails.[170] 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 the privacy right rarely survives it. Under section 23 analysis, the compelling state interest, when balanced against the alleged privacy right, is almost always the winner.[171] 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 we have considered here attests to this fact,[172] as does the federal case law on which the Florida section 23 test was originally based.[173]

A further obstacle to section 23 protecting GPS privacy is the third prong of *Winfield* test.[174] Recall that after the claimant's privacy expectation is established, the government may show that it had a compelling state interest (balancing test) in obtaining the claimant's personal information and that it obtained that information through the "least intrusive means."[175] Unfortunately for claimants of GPS privacy (or any privacy right for that matter), the government can generally defeat a section 23 argument by meeting this "least intrusive means" prong. As many cases reveal, this is because a warrant or subpeona is generally sufficient to meet this third and final requirement of the *Winfield* test.[176] Since this is the case, presumably a

[170] *Forsberg,* 455 So. 2d at 379.
[171] *Id.* at 379-80; *Winfield,* 477 So. 2d at 548; *Shaktman,* 553 So. 2d at 152.
[172] *Id.*
[173] *Whalen v. Roe,* 429 U.S. 589 (1977); *California Bankers Association v. Schultz,* 416 U.S. 21 (1974).
[174] *Winfield,* 477 So. 2d at 548.
[175] *Id.*
[176] *Id.*

court order under Florida's wiretapping and interception statute[177] would also meet this "least intrusive means" theshold, thereby canceling out the claimant's section 23 legitimate privacy expectation.

The **section 12** test also poses barriers which may restrict the courts' ability to find an expectation of privacy in GPS locational subject matter. It is not clear that section 12 allows a privacy expectation for publicly-made cellular communications, and even less clear that section 12 might protect GPS data alone (without the cellular communication). Yet, even if there were a reasonable expectation of privacy under these tests, the courts would likely find that one's personal GPS data has not unlawfully been seized or intercepted if the government obtained a wiretap/interception court order in advance. This is because most case law recognizes a "search" as "reasonable" enough to avoid constitutional privacy scrutiny if a warrant was obtained, authorizing the police search.[178] It follows that a wiretap/interception court order would equally fulfill this "reasonableness" requirement, under section 12, article 1 of the Florida Constitution (based on Fourth Amendment analysis).

4.3 Conclusion

In short, the subject matter encompassed by section 23 disclosural privacy is part of a fluid test with few bright lines, and one which remains to be developed and expanded in the case

[177]Under FLA. STAT. ch. 934.01, "... the 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 allowed only when authorized by a court of competent jurisdiction. Interception of wire and oral communications should further be limited to certain types of major offenses and specific categories of crime ..." *Id.* (emphasis added).

However, it is not entirely clear that a court is authorized to make a GPS interception order under this statute. This is because FLA STAT. ch. 934.01 only permits interception and wiretap orders for 'wire and oral communications.' FLA STAT. ch. 934.02(1) defines 'wire communication' as a means requiring "the aid of wire, cable or other like connection." FLA STAT. ch. 934.02(2) defines '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 'electronic communication' because FLA STAT. ch. 934.12(12) explicitly prohibits this.

law. Yet both section 23, and to a lesser extent, section 12, have the potential to support an expectation of privacy in cellular telephone conversations. It is less apparent that 23 and 12 could support a privacy expectation in GPS data alone, but once a GPS device is integrated within a cellular telephone, the marriage of these two functions affords greater privacy to one's GPS information.

Having said this, even though section 23 may allow a privacy expectation in GPS data, the law will normally prevent privacy from being assured. This is because the Florida constitutional privacy rights articulated by section 12 and 23 of article 1 are so easily defeated by the presence of a search warrant or 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. Almost any state interest can be construed as compelling, as the case law presented here illustrates.

Thus, considering the totality of these factors, section 23 or 12 will likely assure GPS-cellular privacy only where a government intrusion into this domain has been made without a warrant, subpoena, or any other indicator of "minimal intrusiveness." Furthermore, a GPS-cellular privacy claimant would be more successful by relying on section 23 than the more limited section 12.

On the whole, there are still no clear answers to the questions posed in the forgoing commentary. However, several indicators relate peripherally to these questions and, arguably, they support the conclusions we have reached.

---

[178] *Kyllo v. United States,* 553 U.S. 221 (2001).