Indiana Law Review

Volume 38 **2005** **Number 1**

NOTES

GLOBAL POSITIONING SYSTEM IMPLANTS: MUST CONSUMER PRIVACY BE LOST IN ORDER FOR PEOPLE TO BE FOUND?

KRISTEN E. EDMUNDSON*

INTRODUCTION

Recent technological advances have allowed the development of a device that can determine the location of a person anywhere in the world instantly and precisely. This device, known as a Global Positioning System (GPS), is available in various shapes and sizes—from backpack-sized devices with centimeter accuracy, to hand-held devices used for navigation on hiking trails with an accuracy of a few meters. Although GPS implants for humans (termed Personal Location Devices (PLDs) by the industry) are not yet on the market, it is only a matter of time before the products will be available. The technology exists for such a device, and at least one company, Applied Digital Solutions (ADS), is poised to market it. The GPS implant device is inserted under the skin using a needle and it remains in place until surgically removed. The implant would communicate its location via radio signals to nearby cellular towers.

One may question the utility of such a device or wonder whether any person would want to have one implanted under his skin. As will be discussed below, the device is being marketed primarily as a personal safety tool—to track a kidnapped child or find an injured, lost, or incompetent adult. However, just beyond these personal safety uses lies a wealth of untapped commercial uses of which the purchaser of a GPS implant may or may not be aware. Imagine receiving a letter in the mail from a clothing store at the local mall stating, "We missed you! We noticed that you were at the mall last Tuesday at 7:14 PM but you did not have the chance to stop by our store. As an incentive to stop by next time, we have included a 10% off coupon for our entire store." This and other far more annoying commercial intrusions on private life would be available if the

* J.D. Candidate, 2005, Indiana University School of Law—Indianapolis; B.A., 2000, University of Chicago. Recipient of the Papke Prize for Best Note in Volume 38, endowed by and named in honor of David R. Papke, former R. Bruce Townsend Professor of Law and faculty advisor to the *Indiana Law Review*. I would like to thank my husband, Kevin, for his endless support, my parents for their encouragement and emphasis on education, and Papa for his urging to never stop learning. Additionally, I would like to thank WTH Engineering, my former employer, for introducing me to the possibilities of GPS.

GPS implant providers decided to sell their customers' location information.[1]

Use of the GPS implant product would create privacy issues unlike any encountered before. Who should have access to the location information of the person with the GPS implant? Will this even concern the people who have a GPS chip implanted? Or will the customers simply be anticipating the emergency uses of the technology—for example locating a kidnapped child or a lost Alzheimer's patient? Will the GPS data be encrypted so that it cannot be usefully intercepted when it is transmitted to the end user through wireless communications?

In addition to the strictly locational data generated by GPS, the potential for the type of data that could be stored in GPS implants is limitless. For example, the chip could store health information including body temperature, blood alcohol level, financial data from stores that are visited, and consumer information such as which restaurants are frequented. However, this Note focuses solely on the privacy issues surrounding the GPS data capabilities—i.e., the capacity to determine with accuracy where a person is in the world at any given time. This Note does not discuss the medical aspects of GPS implants—such as whether the implant is safe, or what effect the radio waves could have on the host. This Note does not address legal issues surrounding the use of GPS implants for prisoners or parolees. Nor does it address government use of the implants. It only addresses commercial use of the GPS implants by the public at large.

In light of the often lengthy process required to enact legislation, it is wise to address the privacy concerns surrounding this new technology now, before the product is widely marketed and used. Additionally, the potential threats to privacy are even greater than in previous technologies, such as the Internet or Enhanced 911 cell phones, because the data collected is unlike any other. It can determine the location of the person with the GPS implant with an accuracy of a few feet and the GPS implant has an element of permanency that no other technology has. Once implanted, the GPS chip would need to be removed surgically. The host of a GPS implant would not be able to simply leave the phone behind or get off the Internet to avoid someone capturing personal information.

This Note first provides a background on GPS technology, concentrating on the manner in which GPS implants for humans will function. Secondly, the Note addresses the potential privacy concerns that the use of GPS implants may create, drawing on examples in the cell phone industry and other technologies that use GPS to determine the location of their users. Thirdly, the Note analyzes the existing privacy torts and legislation that address location information privacy, interception of electronic communications, and privacy on the Internet to

---

1. The reader may recall the opening scenes of the film *Minority Report* where the characters are inundated with custom advertising based on retinal scans. MINORITY REPORT (Twentieth Century Fox 2002). Although those advertisements were generated based on personal preferences databases triggered by the retinal scan, a similar phenomenon could occur based on the transmission of GPS information.

determine whether such torts and legislation are applicable to GPS implants. After concluding that the existing legislation and privacy torts are not adequate or applicable, the Note offers suggestions for new legislation that would protect the privacy of GPS implant hosts.

I. GLOBAL POSITIONING SYSTEM (GPS) IMPLANT TECHNOLOGY—WHAT IS GPS AND HOW DOES IT WORK?

A. Overview of GPS

The Global Positioning System (GPS) was originally created by the Department of Defense for use in maneuvering of weapons and troops.[2] Numerous books and articles have been written on GPS technology in the fields of geography and satellite technology. A recent law review article gives a simple explanation of the way GPS works:

> GPS consists of three main components: a space-based component, a control component, and a receiver. The space-based component consists of twenty-four satellites, which orbit the earth while broadcasting a positioning signal. The United States Air Force operates the control component, which consists of tracking facilities that monitor and correct the position of the satellites. The receiver component, which varies greatly in size and expense, uses the GPS signal to calculate its own position.[3]

A GPS receiver takes the information broadcasted by the satellite and then determines its three-dimensional location (longitude, latitude, and elevation above sea level) through a triangulation calculation.[4] With the use of Wide Area Augmentation Systems (WAAS) or Differential GPS (DGPS), GPS receivers can calculate their location with an accuracy of a few feet.[5]

GPS receivers are available in vastly different prices and accuracies. They range from a simple hand-held GPS receiver used by hikers to navigate through the forest, to huge contraptions strapped to a person's back with antennae extending a few feet in the air. Generally, the larger and more expensive the unit, the more accurate the GPS reading will be. Extremely precise GPS receivers that have accuracy to within a few centimeters are used by the military, but also by

---

2. *See* U.S. Navy, *USNO NAVSTAR Global Positioning System at* http://tycho.usno.navy.mil/gpsinfo.html (last visited Nov. 15, 2004).

3. Jeremy Speich, Comment, *The Legal Implications of Geographical Information Systems (GIS)*, 11 ALB. L.J. SCI. & TECH. 359, 361 (2001) (footnotes omitted).

4. Robert Puterski, *The Global Positioning System—Just Another Tool?*, 6 N.Y.U. ENVTL. L.J. 93, 95 (1997) ("By transmitting synchronized digital codes with a specific frequency, and knowing the precise time it takes for that signal to travel a given distance, a position can be calculated.").

5. Garmin Ltd., *What is GPS? at* http://www.garmin.com/aboutGPS/ (last visited Nov. 15, 2004) (Garmin is a major manufacturer GPS products.).

city planners, utilities, and sanitary or sewer workers to locate buried cables or pipes. GPS receivers that have an accuracy of a few feet are frequently used for navigation, whether by boat or plane.

More recently, GPS technology has been made available to the general consumer through navigation devices in cars and inclusion in hand-held devices such as cell phones and personal digital assistants (PDAs).[6] In the case of cell phones, GPS is used to determine a 911 caller's location and allow emergency vehicles to assist the caller, whereas GPS in PDAs or OnStar is used primarily for navigation assistance, although there can be an emergency response component as well.

B. GPS Subdermal Implant

On May 13, 2003, Applied Digital Solutions (ADS) announced that it had developed a working prototype of "what the company believes is the first-ever subdermal GPS 'personal location device' (PLD[7])."[8] Although the product is not yet on the market, ADS already sells two other products commercially that demonstrate the viability of the concept. Once on the market, the PLD would likely take the form of the first product, VeriChip combined with the functionality of the second product, Digital Angel.

The first product, named VeriChip, is a "miniaturized radio frequency identification device" which is about the size of a grain of rice and is inserted underneath the skin.[9] VeriChip stores identification information that is

---

6. OnStar is the primary example of the use of GPS in vehicles for navigation and public safety purposes. For more information, see http://www.onstar.com (last visited Nov. 15, 2004).

7. Throughout this Note, the terms "GPS implant" and "PLD" will be used interchangeably.

8. Press Release, Applied Digital Solutions, *Applied Digital Solutions Announces Working Prototype of Subdermal GPS Personal Location Device* (May 13, 2003) *at* http://www.adsx.com/news/2003/051303.html.

9. *Id.* The Food and Drug Administration (FDA) declined to regulate ADS's VeriChip. Press Release, Applied Digital Solutions, *FDA Ruling—Subdermal VeriChip Is Not a Regulated Medical Device "For Security, Financial, and Personal Identification/Safety Applications"* (Oct. 22, 2002), *at* http://www.adsx.com/news/2002/102202.html; *see also* Matt Fleischer-Black, *Cosmetic Advocacy*, THE AMERICAN LAWYER, Aug. 2003, 70, 123 (discussing the decision of the FDA's chief counsel, Daniel Troy, not to regulate VeriChip).

> [T]he company formally asked the FDA to rule that the agency had no jurisdiction over its product, the VeriChip . . . [I]ts lawyers . . . argued that it shouldn't be regulated because the company hadn't claimed anything about health. Troy agreed. The product did not fall within the agency's jurisdiction of products intended "to affect the structure or function of the body," he wrote in a letter in October 2002—this despite the fact that to be used the chip must be injected. Troy's letter deemed the chip a 'consumer product,' and thus the responsibility of the Consumer Product Safety Commission—which only regulates products after they hit the market.

Id. The wisdom of this ruling, or lack thereof, is left to another author. *See also* Elaine M. Cochran, *The Unguarded Gate: The Jurisdictional Gap Within FDA "Device" Regulation*, 5 J. L.

transmitted via a radio frequency signal when a proprietary scanner is passed over the device.[10] VeriChip does not have GPS capability, so it cannot be used for locating a person. VeriChip simply stores information that can be read by the proprietary scanner. Information, such as name and address, is stored in the microchip and can be retrieved in case of emergency by anyone who has the scanning device. Although ADS does not provide the number of VeriChips it has sold, VeriChips are already being included on standardized requests for production forms, suggesting that the use of VeriChips is substantial enough to warrant attention.[11]

The second relevant product, named "Digital Angel," is a device worn like a (removable) watch which can communicate the location of the wearer to any designated person via GPS data transmitted through the wireless cell phone network and retrievable by the interested party on the Internet or by calling a designated number.[12] Digital Angel is marketed as a safety device for keeping track of elderly people and "families on the go."[13] Because Digital Angel is worn on the wrist and can be taken off at any time, it does not have the permanency that VeriChip offers.

The presence of the VeriChip and Digital Angel products on the market, along with the announcement of a working GPS implant prototype demonstrate that it is only a matter of months before PLDs are available commercially.[14] A GPS implant offered by ADS would likely be affordable and require only a brief outpatient procedure to insert, given that the VeriChip costs about $200 and the device is inserted with a large needle by a doctor.[15] A GPS implant could be marketed to the same demographic as Digital Angel—it could be marketed as a tool to keep track of elderly family members or children. However, given the rapid expansion of GPS technology from the military to the average consumer,

---

& FAM. STUD. 189, 198-99 (2003) (Although this article is outdated as it does not include discussion of the FDA's October 2002 decision, the author does discuss loopholes of medical device regulation as it would apply to VeriChip and mentions some of the potential safety risks of the product.).

10. Press Release, Applied Digital Solutions, *Applied Digital Solutions Announces Working Prototype of Subdermal GPS Personal Location Device* (May 13, 2003), *at* http://www.adsx.com/news/2003/051303.html.

11. DAVID E. KELTNER, TEXAS PRACTICE GUIDE, § 8:114 (2003) (defining "documents" to include "intra- or extra- body technological devices (including but not limited to 'Verichips' and like devices)").

12. Digital Angel Corp., *Digital Angel/Consumer at* http://www.digitalangelcorp.com/consumer.asp (on file with the Indiana Law Review). A similar watch-like device is available from another company named "Wherify." *See* http://www.wherifywireless.com/corp_home.htm (last visited Nov. 15, 2004).

13. *Id.*

14. For more information on VeriChip or Digital Angel products, see the following websites: http://www.4verichip.com and http://www.digitalangelcorp.com (last visited Nov. 15, 2004).

15. Christopher Newton, *U.S. to Weigh Computer Chip Implant*, AP ONLINE, Feb. 27, 2002, *available at* 2002 WL 14995023.

it may be only a matter of time before GPS implants are commonplace in individuals from all parts of society—not just those that are at risk for getting lost or kidnapped.[16] One could conceive a world where a parent who wishes to keep track of where his teenager goes on the weekend or where a spouse, wishing to time dinner perfectly, logs onto his computer to determine how close to home his wife is.

II. Privacy Concerns of GPS Implant Hosts—Big Business as Big Brother

A. Background on Commercial Intrusion into Private Life

In the twenty-first century the enemy in the privacy war may no longer be the government, but instead may be Corporate America. The academic literature is rich with analysis of the privacy rights that citizens hold and the limits that these rights place on government intrusion into private life.[17]

Of more recent origin is the intrusion of commercial interests into private life. The market value of location information will tempt GPS implant providers to sell their customers' location information even if, initially, this is not the primary purpose for the device. The national and state do-not-call lists are examples of how important privacy is to the general public.[18] If sales calls during

---

16. For more potential applications of VeriChip and GPS implants, see Dean Unatin, *Progress v. Privacy: The Debate Over Computer Chip Implants*, 2002 UCLA J.L. & Tech. Notes 24 (2002) (describing uses for soldiers and criminals as well as children and Alzheimer's patients).

17. This Note will not discuss an individual's right to privacy under the U.S. Constitution or state constitutions. Such constitutional privacy rights may be implicated when law enforcement officials search or require information as part of an investigation, but that is not the same privacy interest as the one at stake when companies release personal information for marketing purposes. *See* U.S. West, Inc. v. FCC, 182 F.3d 1224, 1234 n.6 (10th Cir. 1999) (explaining that the privacy interest in a case dealing with telecommunication providers' use of customers' personal call information—including location - for outside marketing was not the same as constitutional right to privacy as addressed in *Griswold v. Connecticut*, 381 U.S. 479, 484-86 (1965) or *Roe v. Wade*, 410 U.S. 113, 152-56 (1973)). For a recent decision about GPS transmitters used to track a criminal suspect, see *State v. Jackson*, 46 P.3d 257, 269 (Wash. Ct. App. 2002) (comparing the use of a GPS tracking device on a car that was lawfully searched to the use of binoculars: "[m]onitoring Mr. Jackson's public travels in his truck by use of the GPS device is reasonably viewed as merely sense augmenting, revealing open-view information of what might easily be seen from a lawful vantage point without such aids."). For a recent discussion of privacy from governmental intrusion for wearers of external personal location devices, such as wrist-watch models, see Waseem Karim, *The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntarily Availing Yourself to GPS Monitoring*, 14 Wash. U.J.L. & Pol'y 485, 501-09 (2004).

18. For information on the National Do-Not-Call Registry, see http://www.fcc.gov/cgb/donotcall/ (last visited Nov. 15, 2004). Many states have their own do-not-call lists. See, for example, Indiana's web page http://www.in.gov/attorney general/telephone/FAQs.htms (last visited Nov. 15, 2004).

the dinner hour are considered intrusive, how would the average American feel if their comings and goings were constantly monitored and sold to marketing groups to better target advertising? GPS implants may be marketed primarily as safety devices, but perhaps, as is the case with supermarket shopping cards, there is a marketing opportunity lying just beneath the surface.[19]

Privacy of a person's location information, as gathered through GPS technology, is a topic of wide-spread importance—as evidenced by the use of the topic in a recent national moot court competition.[20] The case for the John Marshall National Moot Court Competition in Information Technology and Privacy Law for 2002 concerned a student who rented a moving truck that was equipped with GPS tracking technology. The truck company used the GPS tracking to determine where the truck had traveled and the company charged the student extra fees because he had taken the truck outside the state. Additionally, the truck company called one of the student's references to report that the student might be in trouble or involved in trouble based on the fact that the truck was parked overnight in the parking lot of an adult bookstore. As a result of this call, the student lost his scholarship. The student sued based on, among other things, the privacy tort of intrusion upon seclusion and deceptive business practices.[21]

B. Comparison of Privacy Concerns of GPS Implant Hosts to Privacy Concerns Surrounding Enhanced 911

Perhaps the most direct comparison of privacy concerns regarding the use of a GPS implant can be drawn from the privacy concerns associated with Enhanced 911 service for wireless phones. The Federal Communications Commission (FCC) requires wireless telecommunications providers to equip their phones and

---

19. *See* Katherine Albrecht, *Supermarket Cards: The Tip of the Retail Surveillance Iceberg*, 79 DENV. U.L. REV. 534 (2002). Albrecht discusses shopper cards which supermarkets use ostensibly for savings opportunities for customers, but actually the

> cards allow retailers to amass unprecedented amounts of longitudinal information on consumer purchase and eating habits. Each time a shopper scans a card at the checkout lane, a record of the items purchased, the time, the store location, and the payment method are added to the shopper's profile. Along with millions of other records, this profile is stored in an enormous 'data warehouse' (frequently a secure facility run by a marketing company under contract to several different supermarkets) where it can be analyzed in detail or simply stored until a later use is found for it.

Id. at 534.

20. Charles Lee Mudd, Jr. et al., *Moot Court Competition Bench Memorandum*, 21 J. MARSHALL J. COMPUTER & INFO. L. 37, 41 (2002).

21. *Id.* at 41-43, 46, 53. *See also* South Texas College of Law, *Brief for the Petitioner*, 21 J. MARSHALL J. COMPUTER & INFO. L. 59 (2002); Texas Tech University School of Law, *Brief for the Respondent*, 21 J. MARSHALL J. COMPUTER & INFO. L. 99 (2002); Richard C. Balough, *Global Positioning System and the Internet: A Combination with Privacy Risks*, CHI. BAR ASSOC. REC. Oct. 15, 2001, at 28, 30-33 (2001) (discussing applicability of privacy torts to a rental agency's use of GPS tracking device in a rental car).

wireless networks with the technology to locate and transmit the location of a cell phone user to a public safety answering point (PSAP—commonly known as the dispatch center) whenever the caller dials 911. One possible way of complying with this requirement is to use a GPS equipped handset, although cellular network-based solutions are also permitted.[22] The location accuracy requirements and time tables for implementation have been subject to change, but, since October 1, 2001, carriers have been required to have an accuracy of "50 meters for 67 percent of calls" in the case of handset-based solutions.[23] Many wireless carriers have not complied with the deadlines and some have paid fines for their noncompliance.[24]

The reason that wireless companies are failing to comply with FCC regulations is that the cost of upgrading their systems and developing the technology required to transmit accurate location information from a cell phone is substantial: "[m]any carriers have already spent hundreds of millions of dollars to deploy location-tracking technologies. To recoup expenses, wireless carriers are exploring ways to generate new revenue from their investments in these capabilities."[25] Traupman notes:

> The same technology that alerts paramedics and police to safety emergencies, for example, can also help automobile drivers locate the nearest French restaurant or gas station. Additionally merchants will be equipped to call a frequent shopper's mobile phone and offer a time-sensitive coupon when the shopper is near the merchant's store.[26]

These uses seem relatively harmless, even if they might be deemed annoying. However there are additional potential uses that would have privacy advocates even more concerned:

> As explained by James Dempsey of the Center for Democracy and Technology, "what if your insurer finds out you're into rock climbing or late-night carousing in the red-light district? What if your employer knows you're being treated for AIDS at a local clinic? The potential is there for inferences to be drawn about you based on knowledge of your whereabouts." In short, privacy advocates are concerned that cell-phone companies will release location information to third parties—whether the third party is a marketer, a law enforcement agency, an employer, or

---

22. Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling System, 14 F.C.C.R. 17388, 17393 (1999).

23. *Id.* at 17392-93.

24. *See* Cingular Wireless LLC, 17 F.C.C.R. 8529, 8533 (2002) (proposing revised compliance dates and mandating contributions to the U.S. Treasury of up to $1.2 million for each missed deadline); AT&T Wireless Services, Inc., 17 F.C.C.R. 19938, 19938 (2002) (adopting consent decree terminating violation proceeding).

25. Ellen Traupman, *Who Knows Where You Are? Privacy and Wireless Services*, 10 COMM. L. CONSPECTUS 133, 135-36 (2001) (footnotes omitted).

26. *Id.* at 136 (footnotes omitted).

a criminal.[27]

Perhaps foreshadowing these privacy concerns, Congress passed the Wireless Communications and Public Safety Act of 1999,[28] which requires customer approval in order for wireless providers to use or disclose location information.[29] However, as will be discussed below, the customer approval process has been the subject of much debate and often leaves privacy advocates unsatisfied.[30]

One might, at first, draw a distinction between GPS equipped cell phones and GPS implants, thinking that there is no privacy issue involved with GPS implants for humans. After all, the product is being advertised for emergency uses such as locating kidnapped children or wandering Alzheimer's patients. However, the same argument could have been made for GPS technology in cell phones. Originally, GPS technology in cell phones was mandated by the FCC for use in emergency situations. But the cell phone companies and businesses realized the value of this location information for market use—and the same is likely to occur for GPS implants. As Traupman noted in her article, "[i]nformation like this is simply too good—not to mention expensive—to leave for emergencies and police work."[31] Marketing companies would love to know what time of day a customer drives by a certain coffee shop or which customers drive by an athletic store on their way to the gym. A business might want to know the location of its competition's sales personnel and the routes taken for sales calls. Certain individuals might want to purchase location information for blackmail, extortion, child custody disputes, or divorce litigation.

The chance that GPS implant providers would sell the location information of their customers to other businesses is extremely high, especially considering Digital Angel's privacy policy (Digital Angel is the wrist-watch version of the GPS personal location device). The privacy policy, as available on Digital Angel's web site, states that "[w]e may, from time to time, share, sell or rent some of your personal information with third parties with whom we have a

---

27. Aaron Renenger, Note, *Satellite Tracking and the Right to Privacy*, 53 HASTINGS L.J. 549, 553 (2002) (quoting Simon Romero, *Location Devices' Use Rises, Prompting Privacy Concerns*, N.Y. TIMES, March 4, 2001 at 25).

28. Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, § 5, 113 Stat. 1288-1289 (1999).

29. *See* 47 U.S.C. § 222(f) (2000).

30. For further discussion of the inadequacy of current protection for location information privacy, especially in the wake of the terrorist attacks of 9/11, see Aaron Futch & Christine Soares, *Enhanced 911 Technology and Privacy Concerns: How Has the Balance Changed Since September 11?*, 2001 DUKE L. & TECH. REV. 38, 23 (2001) ("Given the speed with which events are now unfolding both at home and abroad, a well reasoned, carefully considered approach to protecting privacy in the E911 system is likely to be an unfortunate casualty."); David J. Phillips, *Beyond Privacy: Confronting Locational Surveillance in Wireless Communication*, 8 COMM. L. & POL'Y 1, 7 (2003) (discussing the PATRIOT Act).

31. *See* Traupman, *supra* note 25, at 136 n.35 (quoting Alan Charles Raul, *O Customer, Where Art Thou?*, eCOMPANY NOW, Mar. 1, 2001 (no longer available at cited website)).

business relationship so long as they agree not to share, sell or rent any of your personal information with others."[32] This policy may only apply to the information required to place an order with the company (such as name, address, phone number, and e-mail), but it may also apply to the location information gathered when the consumer uses the product. The privacy policy was not explicit—which is yet another reason to be wary.

Additionally, the fact that GPS implants have yet to make an entrance on the market does not preclude the consumer privacy issue from being discussed. On the contrary, if this new technology is to be given a chance, privacy issues would best be dealt with before the GPS implant is available. Consumers must have confidence in a new technology before they will use it, and there will be no confidence if the public fears that its location information will be up for sale. At least one writer has acknowledged this necessity in the case of GPS in cell phones: "For this technology to take off, (consumers) must have a uniform expectation about their privacy, that it is the customer and not the service provider who has control over the use of their location information."[33] Speaking more generally of GPS technology, one commentator notes that the "truly beneficial uses of location technologies such as safety and search and rescue could develop into strong markets for the GPS community only if the Big Brother issues can be addressed."[34] A lack of privacy protection for consumers of new GPS products, such as the human implant, could have a disastrous effect on the predicted exponential growth of the GPS market.[35]

Besides privacy concerns, there are more serious concerns that might arise with the introduction of GPS implants to the marketplace, such as danger to the GPS implant host and liability of the GPS implant provider for bad data or breach of security. Although these issues are beyond the scope of this Note, they are worthy of brief discussion here. GPS implant providers could be held liable for injuries sustained by hosts if the product failed to emit a signal for emergency personnel to locate the host or if the data gave the wrong location.[36] If the Digital Angel product is any model for the forthcoming GPS human implant product, location information would be available for customers on Internet sites as part of the standard service. Even if this information were password protected, web sites

---

32. Digital Angel Corp., *Digital Angel Privacy Policy at* http://www. digitalangelcorp.com/about_privacy.asp (on file with the Indiana Law Review). As of March 4, 2004, the Privacy Policy contained this language, but it has since been omitted.

33. M.J. Zuckerman, *Wireless, with Strings Attached: A Cellphone Can Make You Stand Out, to Rescuers and Marketers Alike*, USA TODAY, Feb. 7, 2001, at 1D (quoting Michael Altschul, general counsel to the Cellular Telecommunications & Internet Association, an industry trade group, on the subject of location based services utilizing location information from cell phones).

34. Dee Ann Divis, *Saving Private Location*, GPS WORLD, Oct. 1, 2003.

35. The market for location based services is predicted to grow from revenues of $6 million today to revenues of $828 million in 2005. *Id.*

36. *See, e.g.*, Jennifer L. Phillips, Comment, *Information Liability: The Possible Chilling Effect of Tort Claims Against Producers of Geographic Information Systems Data*, 26 FLA. ST. U.L. REV. 743 (1999).

can be hacked and "[m]isuse of an implanted tracking device embedded in a child's shoulder and tracked by Internet access is foreseeable at the least by the criminal element of society who habitually adjusts to new technological demands."[37] Worse yet, the presence of a GPS implant in a child could put the child at further risk of harm even though the implant is billed as a safety device:

> In the case of the imbedded tracking device, when a child is abducted, the criminal is highly motivated to act out in self interest even at the child's expense. If the criminal knew the child had the device implanted in a standard location of the shoulder and it was emitting continuous information concerning the abductor's location, it is not difficult to imagine, and even foreseeable that an abductor would cut the device out of the child's shoulder.[38]

These concerns are certainly important, however, analysis of these issues would require a discussion beyond the scope of this Note.

III. Applicability (or Lack Thereof) of Existing Privacy Torts and Legislation to GPS Implants

A. Privacy Torts

One potential avenue for protection of consumer privacy is through tort claims against GPS implant providers. All modern day privacy torts find their birth in Warren and Brandeis' influential nineteenth century article where the authors noted that

> The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.[39]

Although Warren and Brandeis' article was principally aimed at the press and the "invention" they referred to was the photograph, which could then be taken instantly rather than requiring one to consciously sit for the photograph, their words could be applied to businesses and modern day technologies like GPS.

Warren and Brandeis' theories did not go unnoticed and have given rise to four generally recognized privacy torts today: intrusion upon seclusion, false

---

37. Cochran, *supra* note 9, at 198-200 (discussing potential lack of Food & Drug Administration (FDA) oversight in the use of VeriChip).

38. *Id.* at 199 (discussing ADS's GPS implant in the context of where it would fit into FDA regulation).

39. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 196 (1890).

light, misappropriation of publicity, and publicity of a person's private life.[40] If these torts were applied to the use of GPS location information, the success of the privacy tort claim would be unlikely. However, the tort claims discussed below could be brought against the GPS implant provider. Claims brought against an eavesdropper who obtained information location by intercepting the GPS signal would be covered under the Electronic Communications Privacy Act, which will be discussed below.[41]

The false light and misappropriation torts would not provide consumer privacy protection because they are not applicable to GPS information. The false light tort would not be applicable because "[t]he potential privacy invasion concerning the use of GPS . . . is not based on falsity, but on dissemination of truthful information that a consumer would prefer to keep private."[42] Likewise, the misappropriation tort is not applicable to the use of GPS information because this use does not involve "a person's name or image, but knowledge of that person's precise whereabouts."[43]

Public disclosure of private facts may at first seem to apply to disclosure of GPS location information, but the tort is limited because "if an event takes place in a public place, the tort is unavailable."[44] Courts generally find that when a person travels over public streets, he voluntarily conveys his location information.[45] However, there are some limitations to the public place exception. For example, even though women could be observed entering and leaving a public Women's Clinic, this was held not a defense to the tort of public disclosure of embarrassing personal facts where abortion protesters had placed the names of the women on protest signs, implying that they were about to undergo an abortion.[46] The court reasoned that "merely because plaintiffs' 'comings and goings' may have been visible to members of the public does not mean that the public was aware of the precise purpose of those 'comings and goings.'"[47] Following that reasoning, if a GPS implant provider were to sell or

---

40. RESTATEMENT (SECOND) OF TORTS §§ 652A, 652E (1977).

41. *See* discussion *infra* Part III.C.

42. Renenger, *supra* note 27, at 556.

43. *Id.*

44. *Id.* at 557 (citing RESTATEMENT (SECOND) OF TORTS § 652D cmt. b. (1977)).

45. United States v. Knotts, 460 U.S. 276, 281-82 (1982) (finding suspect had no reasonable expectation of privacy while driving on public roads, so use of tracking device was not a violation of the Fourth Amendment).

> A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the defendant] traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.

Id.

46. Doe v. Mills, 536 N.W.2d 824, 832 (Mich. App. 1995).

47. *Id.*; *see also* Nader v. Gen. Motors Corp., 255 N.E.2d 765, 771 (N.Y. 1969) ("A person

disclose customer location information (without the customer's consent), and that information was publicly displayed, then conceivably the provider could be held liable for the wrongful disclosure of these private facts. A GPS situation analogous to the abortion case might be a GPS implant customer whose trips to an AIDS clinic or male strip club were disclosed to a conservative group that listed the customer's name as a homosexual on protest signs.

Finally, the intrusion upon seclusion tort, which is often applied in cases of eavesdropping, might be applicable to the GPS information situation; however the gathering of such information in a public space provides an exception to the tort just as it does for public disclosure of private facts.[48] Yet, the 2002 John Marshall National Moot Court Competition in Information Technology and Privacy Law felt the intrusion upon seclusion tort in the GPS context had enough merit to include the issue in its moot court case.[49]

Torts are one possible way of protecting the privacy of GPS implant hosts. However, there are other more proactive rather than reactive measures that can be taken such as legislation preventing the disclosure of location information by companies providing location services to consumers.

B. Telecommunications Act of 1996 and Wireless Communications and Public Safety Act of 1999

Although regulation of GPS implants may not fall under the Telecommunications Act of 1996 (hereinafter Telecom Act),[50] it is still useful to undertake a detailed analysis of how the Telecom Act protects consumer privacy because it may serve as a model for legislation tailored specifically for GPS implants. The Telecom Act appears to be the only legislation that addresses consumer privacy concerning an individual's location information and therefore deserves in depth attention. The purpose of the Telecom Act was to update the Communications Act of 1934 so that it could handle new technologies such as the Internet, cable, cellular phones, and other types of communication available in the digital age.[51] Although Congress' "central ambition" may have been to "permit more competition into telecommunications markets," the Telecom Act also contained privacy legislation aimed at protecting consumers.[52]

1. Protection for Consumers.—The Telecom Act protects consumers from unauthorized release of their personal information. It restricts the use of consumer information by telecommunications carriers:

---

does not automatically make public everything he does merely by being in a public place. . . .").

48. Renenger, *supra* note 27, at 558.

49. Mudd et al., *supra* note 20, at 41.

50. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified in scattered sections of 47 U.S.C. §§151-710 (2000)).

51. *See* Michael I. Myerson, *Ideas of the Marketplace: A Guide to the 1996 Telecommunications Act*, 49 FED. COMM. L.J. 251, 252 (1997).

52. Glen O. Robinson, *The "New" Communications Act: A Second Opinion*, 29 CONN. L. REV. 289, 304 (1996).

> Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.[53]

The Telecom Act protects "customer proprietary network information," which is defined as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications services subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[54]

The Telecom Act did not originally include location information, but was amended to explicitly include "location" in the definition of customer proprietary network information (CPNI) by the Wireless Communications and Public Safety Act of 1999.[55] This 1999 Act also added subsection (f) to section 222, which is focused on location information exclusively and states:

> For purposes of subsection (c)(1) of this section, without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to—(1) call location information concerning the user of a commercial mobile service . . . other than in accordance with subsection (d)(4) of this section . . . .[56]

Notice that this part refers to "express prior authorization" rather than "approval of the customer" in the CPNI section. As will be discussed below, these seemingly similar approval requirements are in fact vastly different.

2. FCC's First Attempt at Providing Guidance for Telecommunications Providers.—The Telecom Act did not explain the manner in which telecommunication providers were to obtain consent from customers to use their CPNI and location information. In response to telecommunication providers' requests, the FCC issued an order in February 1998 ("1998 CPNI Order") under which the FCC adopted an "opt-in" approach, requiring providers to obtain customer permission before releasing their CPNI to companies for purposes

---

53. 47 U.S.C. § 222(c)(1) (2000). The privacy of consumer information is discussed in 47 U.S.C. § 222. Telecomm. Act of 1996 § 702, 47 U.S.C. § 222.

54. *Id.* § 222(h)(1)(A).

55. Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, § 5, 113 Stat. 1288-1289 (1999).

56. 47 U.S.C. § 222(f). Subsection (d)(4) creates an exception for the release of customer location information in the case of an emergency and limits this release to emergency personnel and family members. *Id.* § 222(d)(4).

outside the customer's existing relationship with the provider.[57] "Opt-in" consent means that "one's prior, express approval must be obtained before personal information is used for purposes beyond those associated with the initial collection purpose."[58] In contrast, an "opt-out" system "allows approval to be inferred from the customer-data processor relationship unless an individual specifically requests limits on further use."[59]

3. Telecommunications Backlash: The U.S. West *Case.*—The telecommunications provider, U.S. West, was not satisfied with the FCC's selection of the opt-in approach "rather than its suggested opt-out approach (which is allegedly cheaper and results in a higher 'approval' rate than the opt-in approach)."[60] So, the company filed suit against the FCC alleging that the opt-in standard adopted in the 1998 CPNI Order was an arbitrary and capricious interpretation of 47 U.S.C. § 222 and violated the First and Fifth Amendments of the Constitution.[61] The court reached only the First Amendment claim and found that the FCC's opt-in regulation violated the First Amendment under the *Central Hudson* analysis for commercial speech.[62]

The court described the *Central Hudson* test as first presenting a threshold question of "whether the commercial speech concerns lawful activity and is not misleading."[63] No one disputed that the commercial speech based on CPNI was lawful and non-misleading, so the court addressed only the remaining prongs of the *Central Hudson* test whereby "the government may restrict the speech only if it proves: '(1) it has a substantial state interest in regulating the speech, (2) the regulation directly and materially advances the interest, and (3) the regulation is no more extensive than necessary to serve the interest.'"[64]

---

57. Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 13 F.C.C.R. 8061, 8066-67 (1998) [hereinafter 1998 CPNI Order].

58. Paul M. Schwartz, *Charting a Privacy Research Agenda: Responses, Agreements, and Reflections*, 32 CONN. L. REV. 929, 934 (2000).

59. *Id.*

60. U.S. West, Inc. v. FCC, 182 F.3d 1224, 1240 (10th Cir. 1999) (Briscoe, J., dissenting), *cert. denied,* 530 U.S. 1213 (2000).

61. *Id.* at 1228 (majority).

62. *Id.* at 1240. It is important to note that the court did not find § 222 itself to be unconstitutional—that claim was not alleged by U.S. West.

63. *Id.* at 1233 (citing Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 566 (1980)).

64. *Id.* at 1233 (quoting Revo v. Disciplinary Bd. of the Sup. Ct. for the State of N.M., 106 F.3d 929, 932 (10th Cir. 1997) (citing *Central Hudson*, 447 U.S. at 564-65)). Another Supreme Court case holds that the third prong of the *Central Hudson* test is not entirely accurate. *See* Bd. of Trs. of State Univ. of N.Y. v. Fox, 492 U.S. 469, 478, 480 (1989) (holding the "no more extensive than reasonably necessary" test to be incompatible with the subordinate position of commercial speech in the free speech hierarchy and designating a "means narrowly tailored to achieve the desired objective" test). The *Fox* test is more lenient to government regulation of commercial speech than the *Central Hudson* test, and the *U.S. West* court did take this new test into consideration when it discussed the third prong in depth. *U.S. West*, 182 F.3d at 1238.

The court expressed doubt whether there was a substantial state interest in regulating the use of CPNI: "[a]lthough we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely."[65] The court required "a more empirical explanation and justification" than simply the concern that disclosure of CPNI could prove embarrassing.[66] Assuming for the sake of appeal that the government had met the substantial state interest requirement, the court found that the government failed to show that the regulation materially advanced the interest because it presented "no evidence showing the harm to either privacy or competition is real."[67] The court reasoned that there was no indication that disclosure of CPNI might actually occur, while acknowledging that "protecting against disclosure of sensitive and potentially embarrassing personal information may be important in the abstract."[68]

Lastly, the court found that FCC rules requiring opt-in approval were not narrowly tailored.[69] The court found that the FCC rejected an opt-out approval process on mere speculation that "there are a substantial number of individuals who feel strongly about their privacy, yet would not bother to opt-out if given notice and the opportunity to do so. Such speculation hardly reflects the careful calculation of costs and benefits that our commercial speech jurisprudence requires."[70] The court was careful to caution that it was not using a least restrictive means test, but "merely recognize[d] the reality that the existence of an obvious and substantially less restrictive means for advancing the desired government objective indicates a lack of narrow tailoring."[71] This obvious and substantially less restrictive means was the opt-out approval mechanism.[72]

4. Current Limitations on the Release of Location Information.—In response to the *U.S. West* case, the FCC issued a further order stating what the approval standard should be for § 222.[73] In this document, the FCC adopted an opt-out standard for intra-company use of CPNI and for "sharing of CPNI with, and use by, a carrier's joint venture partners and independent contractors in connection with communications-related services that are provided by the carrier (or its

---

65. *Id.* at 1235.

66. *Id.*

67. *Id.* at 1237.

68. *Id.* (Apparently, the court did not deem the fact that the telecommunication industry cared enough about the standard to go to court as evidence that the industry intended to disclose CPNI for marketing purposes to third parties.).

69. *Id.* at 1238 (citing *Fox*, 492 U.S. at 480; Florida Bar v. Went For It, Inc., 515 U.S. 618, 632 (1995)).

70. *Id.* at 1239.

71. *Id.* at 1238 n.11.

72. *Id.* at 1239.

73. Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 17 F.C.C.R. 14860 (2002) [hereinafter 2002 CPNI Order].

affiliates) individually, or together with the joint venture partner."[74] However, in the case of disclosure to third parties and affiliates that provide no communications-related services, the FCC determined that an opt-in standard was appropriate even in light of the *U.S. West* case.[75] The FCC reasoned:

> [C]onsumers say that their privacy interest is substantially greater when asked about releasing information to third parties or for uses beyond their expectations based on the existing relationship with their chosen carrier. Furthermore, once such information leaves the hands of the customer's carrier, the customer loses her ability to limit further dissemination, and section 222 and the Commission's rules concerning use of CPNI are not applicable to those unknown third parties that receive the customer's personal information. For these reasons, there is a greater need to ensure express consent from an approval mechanism for third party disclosure. Opt-in directly and materially advances this interest by mandating that carriers provide prior notice to customers and refrain from disclosing CPNI unless a customer gives her express consent by written, oral, or electronic means.[76]

In the 2002 CPNI Order, the FCC established the customer consent standards for CPNI, which in its statutory definition includes the word "location."[77] However, wireless location information is also protected by § 222(f) and the standard for disclosure of or access to this information is "express prior authorization."[78] Ellen Traupman argues that Congress' choice of words in this section "means clear, unmistakable customer approval is required before using or disclosing location information relating to wireless subscribers," thus requiring an opt-in standard.[79] However, Traupman wrote her article before the FCC released its 2002 CPNI Order.

Yet, the FCC noted that "section 222 adopts a different standard for use of wireless location information than for use of other kinds of CPNI. The standard for use of wireless location information will be addressed in a separately docketed proceeding."[80] As promised, the FCC returned to this issue, however the FCC declined to commence a rulemaking on § 222(f), reasoning that "[b]ecause the statute imposes clear legal obligations and protections for consumers and because we do not wish to artificially constrain the still-developing market for location-based services, we determine that the better

---

74. *Id.* at 14875.

75. *Id.* at 14883.

76. *Id.* at 14885-86 (footnotes omitted).

77. 47 U.S.C. § 222(h)(1) (2000).

78. *Id.* § 222(f).

79. Traupman, *supra* note 25, at 144.

80. 2002 CPNI Order, *supra* note 73, at 14865 n.20 (referring to Wireless Telecommunications Bureau Seeks Comment on Request to Commence Rulemaking to Establish Fair Location Information Practices, WT Docket No. 01-72, Public Notice, DA 01-696 (rel. March 16, 2001)).

course is to vigorously enforce the law as written, without further clarification of the statutory provision by rule."[81]

Although the FCC has deemed § 222(f) self-explanatory, others have warned that telecommunication providers may decide for themselves whether the section could ever allow implied consent and what is included in the definition of location information.[82] Should a telecommunications provider ignore the consent requirements or interpret them in a manner that the FCC deems inappropriate, the telecommunications provider would be subject to an enforcement action by the FCC, which could include fines in the million-dollar range.[83]

In summary, the existing protection for customer location information under the Telecom Act varies depending upon what part of § 222 is used (either CPNI or 222(f) location information) and to whom the information is being given (joint venture and independent contractors or third parties). If the CPNI protection of § 222 is used, then the FCC applies an opt-out approach for use by the company and its partners in communications-related services. If the CPNI is passed to a third party, however, the FCC has ordered an opt-in approach. Likewise, disclosure of wireless location information under § 222(f) requires "express prior authorization," although the FCC has declined to make explicit the meaning of this phrase for fear of discouraging further development of location based-services.[84]

5. Whether ADS or Other GPS Implant Providers Would Be Covered by the Telecom Act.—Now that the reader has a basic understanding of the Telecom Act and its implications for consumer privacy of location information, the question remains whether the Telecom Act is applicable to GPS implant providers. Traupman argues that "non-carrier application providers and content developers" who use location information gathered by the telecommunications providers are not governed by the § 222 CPNI restrictions.[85] Additionally, Reneger argues that the Telecom Act "offers no protection for people whose privacy is violated through non-cell-phone-based collections of location information" and cites the

---

81. *In re* Request by Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Location Information Practices, 17 F.C.C.R. 14832, 14832 (2002) [hereinafter Request for Location Information Practices].

82. "For example, some carriers have asserted that the location of the cell tower nearest a customer is not 'location information.'" Phillips, *supra* note 30, at 14 (citing Request for Location Information Practices, *supra* note 81, at 14839) (statement of Commissioner Michael J. Copps, dissenting)).

83. "[T]he holder of CPNI, the customer's existing telecommunications provider (including its telecommunications affiliates), is subject to enforcement action by the Commission for any failure to abide by the notice rules regarding planned use, disclosure, or permission to access a customer's CPNI." 2002 CPNI Order, *supra* note 73, at 14878 (footnotes omitted); *see, e.g.*, Cingular Wireless LLC, 17 F.C.C.R. 8529, 8533 (2002) (mandating "contributions" to the U.S. Treasury of up to $1.2 million for each missed deadline).

84. *See supra* text accompanying note 81.

85. Traupman, *supra* note 25, at 146.

use of GPS in rental cars to track customer speeding as an example.[86]

In order to determine whether the Telecom Act could apply to GPS implant providers, we must look to the definitions of certain terms used in the Act. A recent case provides guidance for applying the Telecom Act to new technology.[87] In *AT&T v. City of Portland*, the court considered whether the Telecom Act applied to cable broadband internet access and stated that "'we look first to the plain language of the statute, construing the provision of the entire law, including its object and policy.'"[88] This case is particularly helpful as a statutory interpretation standard since the FCC has not offered a construction, in the form of a substantive or interpretive rulemaking, of the Telecom Act relating to GPS implant providers.

Many cases emphasize judicial deference to an administrative agency's (like the FCC's) statutory construction, however in *AT&T*, the court disagreed with the FCC's interpretation and instead performed its own interpretation of the Telecom Act.[89] Since the FCC's interpretation was not arrived at through rulemaking, but instead was developed for the purposes of the litigation, the court did not feel bound to defer to the agency's litigating position.[90] Thus, this case provides insights into the process that a court might undertake if a GPS implant provider case were to arise under the Telecom Act in the current situation with an absence of an official FCC ruling on GPS implants.

The contested issue in *AT&T* was whether the local cable franchising authority could "condition a transfer of a cable franchise upon the cable operator's [AT&T's] grant of unrestricted access to its cable broadband transmission facilities for Internet service providers other than the operator's proprietary service ["@Home"]."[91] This issue turned on two determinations: 1) whether @Home was a "cable service" as defined in the Communications Act (the act which the Telecom Act supplements) and 2) whether @Home, as operated by AT&T, was merely an "information service" or also a telecommunications service.[92]

When examining the cable service issue, the court looked both at the definition in the statute and the practicality of treating @Home as a cable service. The court reasoned that the @Home internet service provider was not a cable

---

86. Renenger, *supra* note 27, at 562.

87. AT&T Corp. v. City of Portland, 216 F.3d 871 (9th Cir. 2000). *See also* Brand X Internet Servs. v. FCC, 345 F.3d 1120, 1131 (9th Cir. 2003) (upholding AT&T decision even in light of contrary ruling by the FCC); Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities, 17 F.C.C.R. 4798, 4802 (2002) (finding "cable modem service, as it is currently offered, is properly classified as an interstate information service, not as a cable service, and there is no separate offering of telecommunications service").

88. *AT&T Corp.*, 216 F.3d at 876 (quoting United States v. Mohrbacher, 182 F.3d 1041, 1048 (9th Cir. 1999)).

89. *Id.* at 876.

90. *Id.*

91. *Id.* at 873.

92. *Id.* at 876-77.

service under the statutory definition because "Internet access is not one-way and general, but interactive and individual beyond the 'subscriber interaction' contemplated by the statute."[93] Additionally, the court reasoned that "applying the carefully tailored scheme of cable television regulation to cable broadband Internet access would lead to absurd results, inconsistent with the statutory structure," for example requiring @Home to carry the signals of local commercial and non-commercial educational television stations.[94]

For the second issue, the FCC argued that a cable broadband internet service provider (ISP) was merely an information service, defined as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications."[95] The FCC maintained:

> ISPs are themselves users of telecommunications when they lease lines to transport data on their own networks and beyond on the Internet backbone. However, in relation to their subscribers, who are the "public" in terms of the statutory definition of telecommunications service, they provide "information services," and therefore are not subject to regulation as telecommunications carriers.[96]

However, the court found that the telephone service linking the user and the ISP was a telecommunications service as defined under the Act because it "control[led] all of the transmission facilities between its subscribers and the Internet."[97] So this particular ISP had both elements of an information service and a telecommunications service by virtue of its ownership by AT&T. Therefore, the court concluded that AT&T did not need to obtain a franchise to offer cable broadband through its ISP because the service was a telecommunications service and not a cable service.[98]

There are three possible scenarios under which GPS implant providers could be covered by the Telecom Act. A GPS implant provider could come within the scope of the Telecom Act if it was defined as a telecommunications carrier, a commercial mobile service, or a joint venture partner. Yet, as will be shown below, even if these scenarios existed, other considerations would make it more likely that the FCC would either fail to enforce the privacy rules or a reviewing court would not interpret the Telecom Act as pertaining to GPS implant providers.

a. ADS as a telecommunications carrier.—First, ADS (as a prototypical GPS implant provider) could be considered a telecommunications carrier for purposes of the CPNI privacy protection under 47 U.S.C. § 222(c). Section 153 of the Telecom Act defines "telecommunications" as "the transmission, between

---

93. *Id.* at 876.
94. *Id.* at 877.
95. *Id.* (quoting 47 U.S.C. § 153(20) (1996)).
96. *Id.*
97. *Id.* at 878.
98. *Id.* at 878-79.

or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received."[99] A telecommunications carrier is simply a provider of telecommunication services and those services are defined as "the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used."[100]

Under this broad definition of "telecommunications," GPS data might qualify as "information of the user's choosing," unchanged in form or content. The GPS data is transmitted from the implant to the provider's data warehouse via the wireless network, which would qualify as "between or among points specified by the user." Once the telecommunications definition is satisfied, GPS implant providers could satisfy the definition of "telecommunications carrier"—one who provides telecommunications services for a fee to the public.

However, regulating GPS implant providers was not the purpose that Congress had in mind when it enacted these statutes in 1996.[101] Additionally, when compared to the ISP in the *AT&T* case, ADS would not have control over the transmission facilities between its implant hosts and the GPS satellite or computer database storing the location information. The *AT&T* court's determination of the ISP as a telecommunications service is distinguishable from the GPS implant scenario because ADS is not owned or operated by the telephone company that is providing the transmission facilities. Furthermore, in *AT&T*, the FCC argued that the ISP was not a telecommunications service, and if the FCC were asked to determine the applicability of the Telecom Act to GPS implant providers, it would likely refrain from extending the Telecom Act to GPS technology which is even more distant from a traditional telephone company.[102] Finally, even if GPS implant providers were considered telecommunications providers and thus subject to the privacy restraints of § 222(c), this protection for CPNI does not carry the more protective "express prior authorization" standard that is applied to wireless location information.[103]

b. ADS as a commercial mobile service.—Second, GPS implant providers could be considered "commercial mobile services" and thus subject to the location information privacy protection under 47 U.S.C. § 222(f). "Commercial mobile service," as used in § 222(f), is defined as, "any mobile service . . . that is provided for profit and makes interconnected service available (A) to the public or (B) to such classes of eligible users as to be effectively available to a substantial portion of the public, as specified by regulation by the

---

99. 47 U.S.C. § 153(43) (2000).

100. *Id.* § 153(44), (46).

101. *See supra* text accompanying notes 51-52. Although this point is not decisive by itself, a court would consider Congress' intent in the passing of the Telecom Act when determining whether to extend protection to a new technology.

102. The argument would have more force if a GPS implant provider first asked the FCC for an interpretation of the applicability of the Telecom Act to its service, rather than waiting until the point when litigation was inevitable.

103. *See supra* Part III.B.4.

Commission."[104] "Interconnected service" is defined as "service that is interconnected with the public switched network (as such terms are defined by regulation by the Commission) or service for which a request for interconnection is pending."[105] Furthermore, the term "mobile service" is defined as:

> [A] radio communication service carried on between mobile stations or receivers and land stations, and by mobile stations communicating among themselves, and includes (A) both one-way and two-way radio communication services, (B) a mobile service which provides a regularly interacting group of base, mobile, portable, and associated control and relay stations (whether licensed on an individual, cooperative, or multiple basis) for private one-way or two-way land mobile radio communications by eligible users over designated areas of operation . . . .[106]

Concentrating on the first part of this definition, in order for GPS implant providers to be considered commercial mobile services, they must provide a radio communication service, that could be one-way only, and that is carried on between mobile stations and land stations. Although ADS has not released the mechanics of how its subdermal GPS personal location device would transmit the host's coordinates to the company's monitoring station, it is safe to assume that it would behave in a similar manner to ADS's existing Digital Angel product. The Digital Angel product's "[a]lert transmissions are contingent on operation in areas providing network service and strong CDPC (Cellular Digital Packet Data) wireless network coverage. In areas with weak or no coverage, alerts cannot be sent from the wearer's monitor. Digital Angel's services require the network service provided by AT&T Wireless."[107] So, the location information would be transmitted over the wireless network (cellular phones transmit using radio) between the mobile human host and the company's monitoring station. Plus, the fact that the GPS implant may not receive information via the wireless network (since it relies on satellites to determine its GPS coordinates) does not matter since one-way communication is permitted.

Yet, application of the label "commercial mobile service" to GPS implant providers leads to the same limitation as the telecommunications provider—the fact that transmission facilities, in the form of cell towers and the associated technology, are operated by the cell phone companies themselves—in this case AT&T. Defining ADS as a "commercial mobile service" ignores the common sense meaning of the term in favor of a blind reading of the statutory definition. Furthermore, even if ADS was considered a commercial mobile service and therefore subject to the privacy limitations of § 222(f), the statute only protects the call location information (as monitored by AT&T—likely the nearest cell

---

104. 47 U.S.C. § 332(d)(1) (2000).

105. *Id.* § 332(d)(2).

106. *Id.* § 153(27). For a definition of personal communication service, see 47 C.F.R. § 24.5 (2003).

107. Digital Angel Corp., *Digital Angel/Consumer*, *supra* note 12.

tower location), but not necessarily the content of the message being sent from the implant to the data warehouse, which includes the exact GPS coordinates.

c. ADS as a joint venture partner.—Third, ADS could be considered a joint venture partner with its cellular network provider—AT&T Wireless.[108] The FCC gave examples of joint venture partners that provide "information services typically provided by telecommunications carriers, such as Internet access or voice mail services."[109] If ADS used the same wireless internet technology in its GPS implants, then its use of customer location information might be constrained by the FCC's guidelines.[110]

However the relationship between the joint venture (ADS) and the telecommunications provider (AT&T) is not of the same type described in the 2002 CPNI Order. ADS would not be using CPNI from the telecommunications provider to market its GPS implants. Instead, ADS would be using its own location information generated from the GPS implants and then in turn sharing or selling this location information to other companies that might be communications or safety related, or could be completely unrelated in terms of products or services. This sort of relationship was not anticipated by the FCC, meaning that the opt-out requirement and joint venture safeguards are not applicable to ADS or AT&T in that capacity.

6. Conclusion: The Telecom Act Would Not Apply to GPS Implant Providers.—As discussed above, the Telecom Act is unlikely to provide privacy constraints for GPS implant providers since the providers do not meet the definitions or the purposes of the Act. Although public opinion may cry out for some sort of privacy protection of location information when GPS implants arrive on the market, the FCC would be unlikely to extend the protection of the Telecom Act to the new technology and a reviewing court will be unable to find such protection in the Act, because the court's task is not to consider what policy

---

108. *See id.* (directing the web page visitor to click on "Wireless Internet" on the AT&T Wireless web site to determine whether his or her area was covered by Cellular Digital Packet Data wireless network coverage required for Digital Angel to work).

109. 2002 CPNI Order, *supra* note 73, at 14881.

110. *See supra* Part III.B.4. For guidelines, see 2002 CPNI Order, *supra* note 73, at 14881-82:

> We require that carriers that allow access to or disclose CPNI to independent contractors or joint venture partners under an opt-out regime assure that certain safeguards are in place to protect consumers' CPNI from further dissemination or uses beyond those consented to by the consumer. In particular, we require carriers, at a minimum, to enter into confidentiality agreements with independent contractors or joint venture partners that: (1) allow the independent contractor or joint venture partner to use the CPNI only for the purpose of marketing the communications-related services for which that CPNI has been provided; (2) disallow the independent contractor or joint venture partner from using, allowing access to, or disclosing the CPNI to any other party, unless required to make such disclosure under force of law; (3) require that the independent contractor or joint venture partner have appropriate protections in place to ensure the ongoing confidentiality of consumers' CPNI.

should be.[111] Furthermore, even if GPS implant providers were considered telecommunication providers, "the FCC has broad authority to forbear from enforcing the telecommunications provisions if it determines that such action is unnecessary to prevent discrimination and protect consumers, and is consistent with the public interest."[112] The FCC might determine that GPS implant use (when the implants first reach the market) is so minor as to make any rulemaking or enforcement based on an extension of the Telecom Act not worthwhile. For the aforementioned reasons, privacy protection for consumers using GPS implants must be found somewhere other than the Telecom Act.

C. Legislation Aimed at Eavesdropping and Internet Web Sites

1. Electronic Communications Privacy Act.—In addition to the possibility that GPS implant providers might attempt to sell their customers' location information to marketers and other businesses, there remains the concern that third parties might try to gain this information for themselves directly. For example, a person might intercept the radio signal that is broadcast from the GPS implant on its way through the wireless network and then be able to retrieve the location information from the transmission. An analogous concept would be an eavesdropper using a high-powered microphone to overhear someone's conversation. This type of access to a GPS implant host's location information would be a clear violation of the law, although it is unlikely that a GPS implant provider would engage in this type of activity against its customers' wishes. However, GPS implant providers might still need to address this issue, e.g., by providing encryption of the signal broadcasting the GPS coordinates of the host in order to deter others from eavesdropping.

Under the Electronic Communications Privacy Act (ECPA), interception of electronic communications is punishable by fines and incarceration.[113] The transmission of GPS coordinates by the GPS implant through the wireless network would likely fit into the definition of "electronic communications" set forth in the ECPA, because the implant would likely operate like the Digital Angel product, which uses radio to transfer the data from the GPS device to the nearest cell phone tower.[114] "Electronic communication" is defined as:

> [A]ny transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire,

---

111. *See AT&T Corp.*, 216 F.3d at 876:

> The parties, and numerous amici, forcefully urge us to consider what our national policy should be concerning open access to the Internet. However, that is not our task, and in our quicksilver technological environment it doubtless would be an idle exercise . . . . Like Heraclitus at the river, we address the Internet aware that courts are ill-suited to fix its flow; instead, we draw our bearings from the legal landscape, and chart a course by the law's words.

112. *Id.* at 879. *See also* 47 U.S.C. §160(a) (2000).

113. 18 U.S.C. § 2511 (2000); *see generally id.* §§ 2510-2520.

114. *See supra* text accompanying note 107.

> radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—
>
> (A) any wire or oral communication;
>
> (B) any communication made through a tone-only paging device;
>
> (C) any communication from a tracking device (as defined in section 3117 of this title); or
>
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.[115]

There is an exception to the electronic communications definition above for "tracking device[s]." A "tracking device" is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[116] On its face, this definition appears to describe the function of a GPS implant. However, the definition of a tracking device appears in the part of Title 18 that discusses search and seizure limitations on law enforcement, so this exception may be limited to law enforcement use. In light of the tracking device exception, the interpretation of the ECPA is unclear, and as another commentator has suggested, perhaps Congress should clarify the application of the tracking device exception to "ensure that anyone who wrongfully obtained location information and abused personal privacy could not hide under the tracking device exception found in the ECPA."[117]

2. Children's On-line Privacy Protection Act.—Although this Note has not concentrated on protection available for personal information that is gathered on the internet, one law that applies to websites' collection and disclosure of personal information warrants special attention because it is tailored to one of the targeted users of the GPS implant—children. The Children's On-line Privacy Protection Act requires the FTC to promulgate regulations that "require the operator of any website or online service directed to children that collects personal information from children or the operator of a website or online service that has actual knowledge that it is collecting personal information from a child" to take a number of precautions.[118] Among other things, the operator must give notice of the information it collects from children at the website and what its disclosure policy is, "obtain verifiable parental consent for the collection, use, or disclosure of personal information from children," and "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."[119] The definition of "personal information" includes the standard information such as name, address, phone number, and social security number, but it also includes "any other identifier that the [FTC] determines permits the physical or online contacting of a specific

---

115. 18 U.S.C. § 2510(12).

116. *Id.* § 3117(b).

117. Traupman, *supra* note 25, at 151.

118. 15 U.S.C. § 6502 (2000).

119. *Id.* § 6502(b)(1).

individual."[120] Location information in the form of GPS coordinates could be considered identifying information that would permit the physical contact of that child.

GPS implant providers would likely slip through the requirements of the Children's On-line Privacy Protection Act because they are not collecting location information from children on the internet. Rather, they would simply be displaying location information obtained through a device that the child's parents had implanted. Additionally, if the parent asked for the child to have a GPS implant inserted, then the parent has given permission for the GPS implant provider to track that child and store this information, at least for the parent's access.

Although the Children's Online Privacy Protection Act may not apply to GPS implant providers, the Act is still useful to keep in mind as a model for legislation that might be developed to protect the location privacy of GPS implant users. Additionally, there could be varying levels of privacy protection for GPS implant users—perhaps more protection for children using the GPS implant than for adults. The Children's Online Privacy Protection Act is such an example of differential privacy protection.

IV. Suggestions for New Legislation

Since the Telecom Act and other legislation discussed above either does not apply to GPS implants or provides inadequate protection, it is clear that new legislation is needed to protect hosts of the implants from intrusive commercial use of their location information. Legislation to protect the disclosure of location information from GPS human implants is perhaps more vital than the legislation that has already been enacted in the Telecom Act for GPS in cell phones. After all, location information for cell phones was an afterthought brought about because of the increase in 911 calls originating from cell phones, whereas location information is the primary purpose of GPS implants.

A. Pending Legislation

There are several bills pending in Congress that relate to the privacy of personal and location information that warrant discussion. House Bill 1636 is termed the "Consumer Privacy Protection Act of 2003," and it proposes to regulate data collection organizations with a requirement that

> A data collection organization shall provide to the consumer, without charge, the opportunity to preclude any sale or disclosure for consideration of the consumer's personally identifiable information, provided in a particular data collection, that may be used for a purpose other than a transaction with the consumer, to any data collection organization that is not an information-sharing affiliate of the data

120. *Id.* § 6501(8).

collection organization providing such opportunity.[121]

This bill does not focus on location information. Indeed it does not even mention such information in its definition of personally identifiable information.[122] Additionally, the bill proposes an opt-out requirement for data collection organizations' use of personal information, which, as discussed below, may not be an adequate protection for the more invasive location information disclosure.[123]

Although the protections for location information disclosure by cell phone providers are not likely to apply to GPS implant providers,[124] it is worth noting that there is a bill entitled "Wireless Privacy Protection Act of 2003" proposing to further restrict the disclosure of such information.[125] The bill defines the process of what it would mean to give "express prior authorization" under 47 U.S.C. § 222(f). The proposed bill states that

> [A] customer shall not be considered to have granted express prior authorization for purposes of subsection (f) unless—
>
> (1) the carrier has provided the customer in writing a clear, conspicuous, and complete disclosure of the carrier's practices with respect to the collection and use of location information, transaction information, and automatic crash identification information, before any such information is disclosed or used, and such disclosure includes—
>
> (A) a description of the specific types of information that is collected by the carrier;
>
> (B) how the carrier uses such information; and
>
> (C) what information may be shared or sold to other companies and third parties;
>
> (2) the customer has agreed in writing to the collection and use of such information, or has agreed in writing to such collection and use subject to certain limitations; and
>
> (3) the carrier has established and maintains reasonable procedures to protect the confidentiality, security, and integrity of the information the carrier collects and maintains in accordance with such customer consents.[126]

This bill appeared in a previous session of Congress as well.[127]

The language of this bill is rigorous in its prerequisites for disclosure. Not

---

121. Consumer Privacy Protection Act of 2003, H.R. 1636, 108th Cong. § 103(a) (2003).

122. *Id.* § 3(4).

123. For a competing bill with principally the same aims, i.e, privacy of personally identifiable information, see S. 745, 108th Cong. (2003).

124. *See supra* Part III.B.5

125. Wireless Privacy Protection Act of 2003, H.R. 71, 108th Cong. (2003).

126. *Id.* § 2.

127. *See* H.R. 260, 107th Cong. (2001).

only does it require prior permission in writing, but it requires minimal privacy procedures on the part of the carrier. These specific requirements for the term "express prior authorization" should serve as a model for any GPS implant legislation because they would give the GPS implant consumer adequate information to make an informed decision about allowing the GPS implant provider to disclose his or her location information.

B. Opt-in Versus Opt-out

As discussed above,[128] the implications of an opt-in versus an opt-out system of consent to release of private location information can have enormous effects on the likelihood that consumers will in fact opt for the protection. In an opt-out system many consumers will allow the disclosure of their location information because they did not bother to read the fine print in the contract for their technology. Although GPS implant consumers will be well aware of the location capabilities of the technology they are purchasing (unlike many cell phone purchasers) and may pay closer attention to the paperwork accompanying their purchase, an opt-in requirement for release of location information is preferable.[129]

An example of legislation that uses the opt-in mechanism for privacy protection is the Driver's Privacy Protection Act of 1994 (Driver's Act).[130] The Driver's Act imposes an opt-in requirement on state departments of motor vehicles before they may disclose or sell drivers' information for marketing use. The requirement used to be opt-out, but was changed to opt-in in 1999.[131]

Conceivably, a person's location information (in mass, available twenty-four hours a day, seven days a week through the GPS implant) would be as private if not more private than the information listed on a driver's license and the associated driver's information such as speeding tickets. Thus, any legislation aimed at the privacy of consumers with GPS implants should have an opt-in mechanism.

Perhaps GPS implant legislation should prohibit release of location information for GPS implant hosts because the device is so permanent and safety driven. Customers might not even fathom how their location information could be used, and perhaps they should be given greater protection. After all, if

---

128. See *supra* text accompanying notes 58-59 for definitions of the opt-in and opt-out standards.

129. The Digital Angel privacy policy available on its internet site offers customers "the opportunity to opt-out of receiving communications from us or others." Digital Angel Corp., *Digital Angel Privacy Policy*, *supra* note 32. This demonstrates, that if left to their own devices, ADS and other GPS implant providers likely would at most provide opt-out privacy protection.

130. 18 U.S.C. §§ 2721-2725 (2000).

131. Pub. L. No. 106-69, §§ 350(c), (d), and (e), 113 Stat. 986 (1999); *see also* Reno v. Condon, 528 U.S. 141, 145 (2000) (upholding requirement that states obtain "a driver's affirmative consent to disclose the driver's personal information for use in surveys, marketing, solicitations, and other restricted purposes" against Commerce Clause attack).

customers want to take advantage of location based services (the primary purpose for which companies would want to buy the location information), they could always use a cell phone that is equipped with GPS for 911 purposes and utilize the services that wireless providers will be developing in the coming years.

Even if Congress deems it inappropriate to have a prohibition on the release of all customers' location information, there is one type of customer that Congress would be likely to protect with a blanket prohibition—children. There should be a blanket prohibition on release of a child's location information to third parties besides law enforcement. A child's whereabouts are not likely to interest a third party marketing or sales company as much as an adult's whereabouts, so in the interest of protection from the criminal elements of society,[132] location information from children should be prohibited from disclosure. This would be an even harsher measure than that taken in the Children's On-line Privacy Protection Act.[133]

C. Limitations on Legislation

Any suggestions for new legislation would be incomplete without a discussion of Constitutional and other limitations on such legislation. In order for such legislation to be effective, it would have to withstand challenges in court regarding Congress' authority to pass such legislation and First Amendment challenges to the restriction of commercial speech.

Congress would likely have the authority to make privacy law for GPS implants under the Commerce Clause.[134] The information contained on driver's licenses has been considered an article of commerce subject to federal regulation.[135] Likewise, GPS implants would presumably be used across states lines, although their use in commerce would not be nearly as pronounced as in driver's licenses, at least if the privacy advocates have their way. Congress might even be able to regulate location information by virtue of the fact that the implant providers would be using federal government data generated from the GPS satellites.

One might think that Congress could simply pass a law that prohibits GPS implant providers from using their customer's location information to sell other products or from selling the location information itself to third party companies. However, such legislation might not be possible because of Constitutional constraints. As discussed above,[136] the FCC was prohibited from requiring an

---

132. *See supra* text accompanying notes 37-38.

133. *See supra* Part III.C.2.

134. U.S. CONST. art. I, § 8, cl. 3.

135. In *Reno v. Condon*, the court reasoned that driver's information is an article of commerce because it "is used by insurers, manufacturers, direct marketers, and others engaged in interstate commerce to contact drivers with customized solicitations. The information is also used in the stream of interstate commerce by various public and private entities for matters related to interstate motoring." *Reno*, 528 U.S. at 148.

136. *See supra* Part III.B.3.

opt-in system for telecommunications providers' use of CPNI for services outside the scope of the existing service relationship.[137]

If *U.S. West* were to be applied to GPS implant customer privacy legislation, it might limit the protections available for implementation based on the second prong of *Central Hudson*. The court in *U.S. West* found that the government failed to prove that the regulation directly and materially advanced the state's interests.[138] The court reasoned that "while protecting against disclosure of sensitive and potentially embarrassing personal information may be important in the abstract, we have no indication of how it may occur in realty with respect to CPNI" since the government failed to present evidence "regarding how and to whom carriers would disclose CPNI."[139]

This requirement of evidence regarding disclosure of the information sought to be protected could be a significant problem for privacy legislation covering GPS implants. GPS implants are not even on the market yet, and when they are available they may be slow to gain in popularity and acceptance. Under the standard articulated in *U.S. West*, legislators may have to wait until disclosure of GPS hosts' location information becomes a problem before they could justify privacy restrictions of an opt-in sort. Yet, a lack of legislation or rulemaking could dampen the market for GPS implants and even the federal government acknowledges this risk:

> We should do this [privacy rulemaking] *before* location technology investments are made, so that industry isn't forced to retool later, at far more expense. We should do so before consumers make up their minds about whether they trust location practices, rather than fighting an uphill battle to regain consumer confidence after it has been lost.[140]

Thus, Congress is faced with a Catch-22. Its legislation may be subject to invalidation by the courts if it legislates before the privacy problem has been made manifest, but if it waits to legislate, the market for the new technology may be suppressed because consumers are afraid to buy the new technology without legislative safeguards. Yet, perhaps a reviewing court would lean in favor of privacy given that the information at issue in the case of GPS implants is accurate location information rather than the more generalized CPNI which includes names and addresses—information for which consumers have less of a privacy expectation.

Any new legislation aimed at consumer privacy for GPS implants will need to have its purpose defined in each of the provisions of the legislation. Courts are unwilling to apply broad purposes of acts to individual provisions because "blind adherence to broad purposes can obfuscate Congress' true intent regarding

---

137. U.S. West, Inc. v. FCC, 182 F.3d 1224, 1240 (10th Cir. 1999).

138. *Id.* at 1237.

139. *Id.*

140. Request by Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Location Information Practices, 17 F.C.C.R. 14832, 14839 (2002) (Statement of Commissioner Michael J. Copps, dissenting) (emphasis in original).

a particular provision."[141] For example, Congress might pass a bill regulating GPS implants that was aimed at the health and safety of the wearer since the FDA declined to regulate VeriChips as medical devices.[142] This bill could also include consumer privacy measures, but Congress would need to rearticulate the purpose of such sections to avoid confusion and possible weakening of the measures when courts are called upon to interpret the legislation in light of free speech challenges.

It is possible that federal legislation could leave the door open for states to create their own legislation. However, given the borderless operation of GPS, perhaps federal legislation should expressly state that it fills the field and preempts any attempts at state legislation.

D. Alternatives to Legislative Protection of Privacy

An alternative to legislation to protect consumer privacy of location information is industry self-regulation.[143] In this manner, GPS implant providers could regulate consumer privacy on their own by providing privacy policies for consumer review and abiding by those policies. However, "[s]ince the economic incentive to provide strong privacy protections is either weak, nonexistent, or at least nonuniformily distributed among all participants in the marketplace, most serious proposals for self-regulation among market participants rely on the threat of government regulation if the data collectors fail to regulate themselves sufficiently."[144]

Additionally, the GPS implant industry may be an imperfect market in which to apply self-regulation of privacy. There is only one company—ADS—poised to enter the GPS implant market. Consequently, there would be a lack of choice and bargaining power that is the hallmark of a functioning market approach (assuming customers have enough information to realize the potential abuses of their privacy).[145] Therefore, self-regulation is not an adequate remedy to consumer privacy concerns surrounding location information.

CONCLUSION

The potential applications for GPS personal location devices are limitless. Such devices could track a lost or kidnapped child, locate an adult with

---

141. *U.S. West*, 182 F.3d at 1237 n.10 (finding that Congress' primary purpose in the CPNI provision was customer privacy, not the broader purpose of increasing competition that was expressed in the Telecom Act).

142. *See* Press Release, Applied Digital Solutions, FDA Ruling—Subdermal VeriChip Is Not a Regulated Medical Device "For Security, Financial, and Personal Identification/Safety Applications" (Oct. 22, 2002), *at* http://www.adsx.com/news/2002/102202.html.

143. Frank Douma & Milda K. Hedblom, *Wireless Communication Applications for Transportation: User Boon or Booby Trap?*, 27 WM. MITCHELL L. REV. 2163, 2173 (2001).

144. A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1524 (2000).

145. *See* Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 890-903 (2002) (discussing market failures in self-regulation of privacy).

Alzheimers who has wandered off, or simply allow family members to keep track of each other's whereabouts. But along with these benefits come some unforeseen risks. These risks become apparent when looking at a similar location technology—Enhanced 911 cell phones. As Enhanced 911 cell phones have shown, location information providers have realized that the information they are collecting is valuable to third parties,[146] and, as a result, personal location information can end up in the hands of marketers and businesses—contrary to the expectations of consumers.

Congress saw the need for statutory protection of location information gathered from cell phones and responded with the Telecommunications Act of 1996 and the Wireless Communications and Public Safety Act of 1999.[147] However, the current privacy requirements are not adequate because so many consumers will not read the fine print or understand the implications of allowing their location information to be sold to third party marketing firms and other types of companies.

Even the inadequate protection for location information from cell phones would not apply to the new personal location devices proposed by ADS.[148] Currently, no laws would prevent ADS from selling location information to marketing firms or any other interested parties, and no laws would even require consumer consent before the release of this information.

Privacy legislation is needed to protect GPS implant consumers' location information from disclosure to third parties. Although GPS implants are not yet on the market, legislators should act now if they wish to encourage the use of this fascinating new technology. Without privacy protections in place, consumers may be too afraid to use the new technology.

The protection for cell phone users' location information can serve as a guide for new legislation, but the protection for GPS implants must be stronger than that for information gathered from a cell phone because the of the permanency of the implant—implant hosts would be unable to turn their GPS device off or leave it at home since the GPS device is surgically implanted under their skin. Even if the potential disclosure of sensitive location information has not crossed the mind of the average consumer, legislators should act quickly to protect consumers from this danger by creating an opt-in mechanism for the release of location information from GPS implants. Not only will the opt-in mechanism create a default rule of protection, but it will also require education of the consumer by the GPS implant provider about the potential uses for location information should the consumer be willing to allow disclosure of location information.

---

146. *See supra* note 25 and accompanying text.

147. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified in scattered sections of 47 U.S.C. §§151-710 (2000)); Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, § 5, 113 Stat. 1288-1289 (1999). *See supra* Part III.B.

148. *See supra* Part III.B.6.