

19

The Evolution of Global Positioning Systems

Blair Krause and Ryan Murray

Introduction

Global Positioning Systems (GPS) are evolving and new breakthrough products are constantly emerging on the market. The most recent breakthroughs are now readily available to consumers in the form of vehicle navigation and communication devices, theft protection and global surveillance. These technologies offer many benefits to the common user, but also raise security and privacy issues by permitting a high level of misuse. The monitoring and exploitation of one's driving habits, patterns and history can take place. The invasion of the public's privacy happens every day due to a lack of regulation concerning the access and use of GPS data.

GPS 101

GPS satellites circle the globe, hone in on transmitting devices through a series of signals, and then record data such as driving speed and travel routes. GPS devices work by 'listening' for the radio signals from satellites and calculating how long the signals take to arrive. The result of that calculation provides a highly accurate estimation of latitude and longitude. The information transmitted by the GPS tracking device beams back to a user's computer through the cellular network and records in the company's database. Elaborate individual GPS tracking systems are rapidly becoming a standard part of vehicles' onboard computer systems, along the side of seatbelt usage and which passenger's door is open. This developing technology is quickly changing the way users drive and the future of many industries.

Vehicle Tracking GPS

The most advanced GPS products on the market today are vehicle transmitter systems such as LoJack™, and navigation devices such as OnStar™. These systems are available to consumers for only a few hundred dollars and include online services that can instantly map where a car is in real-time. This provides a great service for anyone

protective of their car. The return rate for vehicles with the LoJack™ theft prevention system is 90%, and the car is typically located and returned within two hours (LoJack Homepage). These systems may have many great benefits, but how much privacy do people sacrifice by using GPS?

Private Vehicle Tracking Systems

Vehicle Global Positioning Systems are mainly used for theft prevention, but new functions of the systems open the product to a wide variety of alternative uses and misuses. Systems such as LoJack™ were originally built solely for theft prevention, but have evolved into multi-use systems. As mentioned earlier, the monitoring and recording a driver's location, route, speed, and even seatbelt use can take place. These monitoring functions offer valuable benefits to a growing number of innovative industries. New users of these systems include employers, marketing researchers, insurance companies, and the police. These new GPS users may validate their reasons for using the products, but the question of how much privacy the user of the vehicle sacrifices still remains. Situations involving the new uses of GPS systems on vehicles have been questioned because they raise many personal privacy and security issues.

Company Vehicle Tracking

The new Global Positioning Systems have a high potential for misuse. After installing a GPS product in a vehicle, the device begins tracking and recording everywhere it goes. Depending on who the actual owner of the vehicle is, such as an employer, drivers may not know whether a device is monitoring their movements or not. In a CNBC special, Jim Joyce, the Vice President of Nabet stated, "we were concerned about privacy issues and how this information might be used to monitor the employees in a big brother situation" (Joyce). Many employees do not know a GPS device could be monitoring them throughout the workday. Employers can survey online where their company vehicle is and when it has been dispatched. Information is even available on how long an employee is at each location and how fast they are driving. As a benefit to the employer, "dispatchers can see on the map where the closest technician is out in the field, and they can push a job to that particular employee" (Onley). Many say this is an invasion of privacy, but employers justify it as another productivity management system. Jim Joyce points out that his company's productivity has increased significantly since the installation of GPS on their vehicles (Joyce).

Laws already allow employers to monitor employee's Internet and e-mail usage at a computer related job and other industries are beginning to incorporate this productivity measurement method into their businesses. Employers may encounter ethical issues when using GPS, but the law allows them to do so. For example, state surveillance laws now say, "the only person legally allowed to secretly hide a GPS tracking device in a car is the registered owner of the vehicle" (Bohan). This law encompasses the business that owns the vehicle the employee drives. It is up to the employer whether they want to inform the

employee about the tracking device. This may seem deceptive, but recent court cases have made it common law. In California, a state with some of the strictest GPS tracking laws, "informing the driver or passengers about the presence of the device isn't required when the unit is placed there by the car's legal owner" (Bohan). Employees still question the use of GPS as an invasion of their privacy. Many compare it to having a boss hovering over one's shoulder at a desk job. Others see the use of these devices as a trust issue with their employer. Whatever the argument, GPS causes a loss in privacy in the working world, but there are currently no solutions unless a court decision is overturned.

Other vehicle-based companies are starting to install GPS into their cars. The trend is most prevalent in the rental industry. Rental car companies, dissatisfied with the treatment of their vehicles, are taking preventative measures to stop the problem. Rental car companies say they "have used GPS devices since the mid-1990s, installing systems to give drivers directions while they're on the road" (Lemos). However, there are many reasons for installing these systems other than navigation.

There have been numerous cases brought to court about rental companies charging penalty fees to drivers for breaking company policies, which they observed through GPS. For example, in a case that could help set the bar for the amount of privacy drivers of rental cars can expect "a Connecticut man is suing a local rental company, Acme Rent-a-Car, after it used GPS technology to track him and then fined him \$450 for speeding three times" (Lemos). The man had no idea a device was monitoring him. The main argument concerns disclosing the use of GPS, even though "the policy is stated in bold at the top of the rental agreement" (Lemos). Currently, there are no recent court decisions defining this policy enforcement as legal or illegal. Presently, "Acme has left the decision in the hands of the Department of Consumer Protection (DCP). The judge in the small claims court case has delayed hearing the claim until the department has issued a ruling" (Lemos). For now, the only solution for car renters is to follow company policies and sacrifice their privacy until the DCP makes a decision.

Malicious Intent

Anyone can buy a vehicle GPS tracker and install it on any car they have access to, making it possible to track anyone without his or her knowledge. GPS raises many personal security issues with the threat of stalking or other malicious intent. For example, "in 2001, a man was arrested in Menlo Park in Oakland for using a GPS monitoring device to stalk a woman" (Bohan). In another case, a man in Colorado was convicted of tracking his wife with a GPS bug after she began divorce proceedings against him (McCullagh). These may be extreme examples, but these systems are becoming more prevalent on the market and many consumers are still unaware of the capabilities GPS products possess.

GPS on vehicles is steadily incorporating itself into everyday life. For example, parents are starting to use GPS to keep tabs on their driving teens. In a recent article, a stepfather installed a GPS in his son's car, unbeknownst to him. The stepfather reported "he was running 60 miles per hour up Concannon Street in a 35 mile an hour zone. Data

gathered by the device showed that Corey drove from school to friends' homes, indicating that he was carrying passengers in violation of DMV rules for drivers under 18" (Bohan). After the son was confronted he naturally felt betrayed and thought his privacy had been violated. Having one's parents know of their whereabouts may not matter to some, but the thought of someone else using the device illegally, such as an ex-partner, may seem scarier.

The Government has no restrictions on who can buy these systems and there is little or no registration process for the vehicle to which it is attached. These monitoring systems are very small and can be hidden anywhere in one's vehicle. "The Lojack transponder is about the size of a deck of cards. It's small enough to be hidden in dozens of locations inside a vehicle" (Lojack Homepage). The only way to prevent these types of misuses from continuing is for all companies to implement a vehicle owner verification process. This would help to ensure that the owner of the vehicle is the same person who purchased and installed the GPS. Otherwise, it is up to the government to take action. For example, California legislators determined that "the increasing use of electronic surveillance is eroding personal liberty" and that "electronic tracking without the person's knowledge violates that person's reasonable expectation of privacy" (Bohan). This law is one step in the right direction for privacy advocates. Further Governmental legislation is predicted to take place as the frequency of misuse continues to rise.

Public Perception Survey

One group of Americans that are greatly affected by the advances in GPS vehicle navigation tracking are school aged children and young adults. This demographic is often tracked by their parents with or without their knowledge. To test the awareness level regarding GPS vehicle tracking we administered a survey to high school students in the Midwestern US. After reviewing the responses to the questions, we broke the students down into three groups. Depending on which and how many questions they answered correctly, the respondents were placed in with either the Genuine Knowledge Group, General Knowledge Group, or Little or No Knowledge Group. Of 67 surveys returned, only 13% possessed genuine knowledge with regard to GPS tracking capabilities. Of the remaining 87%, only 32% possessed general knowledge of the tracking capabilities of GPS tracking systems, leaving an astounding 40 people, or 60%, with little or no knowledge of their vulnerability. We must also take into consideration the possibility that the respondents did not take the survey seriously, although the numbers were so skewed towards the Little or No Knowledge Group, that we do not believe this to be a strong factor. With this demographic being one of the most affected by this type of technology, such a high lack of knowledge leaves this group open to be tracked by their parents or someone with less honorable intentions.

Marketing Research Uses

The data obtained by a vehicle's GPS is stored in the servicing company's database system. So, what could anyone do with the driving records about thousands of random and innocent consumers?

Companies pay good money to conduct marketing research about people's driving habits. For example, one company deciding on where to place expensive advertising billboards will find prime exposure locations based on GPS traffic data. Soon, enough relevant data will be mined and prove to be a beneficial research source. Recently, the Department of Transportation tested the research capabilities of GPS data archives. The results show that "GPS technologies are able to better capture variability in travel behavior across multiple days. It also offers detailed route choice, spatial location and travel itinerary information not available in other travel survey data sets" (Measuring). With this high level of accuracy, marketing research companies could identify someone and abstract information, such as the shopping centers or restaurants they frequent. Based on this information, consumers would be directly marketed. This method is very similar to e-mail SPAM received based on the Internet websites visited. Depending on the service provider and its privacy agreement, people may not have a choice whether their data reaches the hands of marketing researchers. Since the data is compiled on the company's system, they legally own it. In order for consumers to protect their privacy, extensive research of the company's privacy of information policy must take place to ensure selling of database records does not occur.

Insurance Uses

The release of GPS driving records to insurance companies containing data on how often one speeds or if they frequent high crime rate areas, could be financially damaging for drivers. There are currently no laws regulating the access of this data by a third party. Insurers are beginning to use the technology and will "offer a discount to LoJack™ owners. In fact, some insurance companies offer up to 35% off the comprehensive portion of your insurance premium for equipping your vehicle with LoJack™ and an alarm" (LoJack Homepage). Insurance companies incur these discounts because of the perceived risk reduction related to auto theft. Now, imagine how much the company's perception of risk would rise if they actually saw all the poor driving habits of many Americans.

Companies are starting to recognize the opportunity for better risk assessment through using GPS. "In fact, one of the largest insurance companies in the United States, Progressive Auto Insurance, has already tested policies in Texas that tied insurance rates to car usage as monitored by global positioning" (Schwart). Insurers could use this data to find reckless drivers. Soon after, insurance rates begin to rise and some drivers might end up paying even more than the initial discount could save them. A Yale University law professor, who is examining the issue, predicts that "within a decade all our car insurance companies will be offering us discounts if we will commit to Acme-like contracts - if we agree not to speed. The use of tracking technology will grow, even if they don't give us a discount" (Schwart). Many feel that policies like these are a direct exploitation of personal privacy and companies are taking on a "big brother" role. Unless the DCP creates a policy banning the use of this information, drivers are at risk for potential insurance rate hikes due to the exploitation of personal GPS data.

Governmental Uses

GPS technology is becoming a valuable asset to police departments across the country. Not only are these systems significantly reducing the rate of auto thefts, but they also aid the authorities in tracking and prosecuting suspects and offenders. Recently:

A federal judge in New York ruled that police did not need court authorization when tracking from afar. Law enforcement personnel could have conducted a visual surveillance of the vehicle as it traveled on the public highways. The driver had no expectation of privacy in the whereabouts of his vehicle on a public roadway (McCullagh).

The statement "tracking from afar" entails monitoring using GPS. Without the need for a court authorization, police can track any possible suspect for whatever reason. Reports show there is an "increasingly popular law enforcement practice of secretly tagging Americans' vehicles without adhering to the procedural safeguards and judicial oversight that protect the privacy of homes and telephone conversations from police abuses" (McCullagh). U.S. State departments are even misusing GPS products and many feel that this directly violates reasonable expectation of privacy. "I think they should get court orders," said Lee Tien, staff counsel for the Electronic Frontier Foundation. "We're in a world where more and more of our activities can be viewed in public and, perhaps more importantly, be correlated and linked together" (McCullagh). Some could consider this a violation of the Fifth Amendment that addresses self-incrimination. Shouldn't there be at least some type of probable cause for monitoring a driver?

Since laws are not current enough to include GPS technology, police can use it for any type of law enforcement. For example, "police used a GPS tracking device on a suspect's car to track his movements and accumulate evidence against him. The suspect was ultimately convicted of methamphetamine manufacture based on the evidence police discovered by tracking his car. He appealed on Fourth Amendment grounds" (Berkeley Intellectual Property Weblog). The defendant believed GPS tracking violated laws relating to a reasonable search and seizure, since police had little evidence before the tracking began. The court deemed it constitutional and found the defendant guilty. Cases similar to this are beginning to pop up all over the country. Soon, this technology will become an unregulated and frequently used tool of the police. Police departments will have the power to find vehicles in the vicinity of a crime and pursue the owners as possible suspects. This type of mass surveillance will place police in an extreme "big brother" situation unless Government restrictions are put in place. "Mass surveillance could possibly raise a Fourth Amendment issue, but the 7th Circuit Court declined to comment" (Recent). Soon the Government will be forced to make a decision as the frequency of misuses continues to rise.

Even though a small percentage of cars on the road have GPS, the auto industry is considering incorporating these devices into the car manufacturing process. In the future, "one can even imagine a law requiring all new cars to come equipped with the device so that the

government can keep track of all vehicular movement in the United States” (Berkeley Intellectual Property Weblog). There are numerous ethical issues with the Government having this much power over privacy. However, “some legal scholars fear that when the U.S. Supreme Court eventually weighs in on GPS tracking, it will side with police over privacy” (McCullagh). Consumers and companies only see the tip of the iceberg with this technology. It possesses many benefits now, but unforeseen privacy risks lie ahead. James E. Hall, a transportation lawyer and former chairman of the National Transportation Safety Board, states, “we are moving toward a kind of automobile that nobody’s ever known. It’s mostly good news, but there are negative things that we will have to work through” (Schwart). The issue rests on how much privacy consumers are willing to sacrifice for the luxuries of GPS.

GPS Navigation Systems & Privacy

The term “*Privacy Policy*” is usually a misnomer, and its use in the GPS Vehicle Navigation industry is no exception. GPS navigation companies like OnStar and many others provide eager customers with in-car navigation services. These services include, among others, map oriented navigation screens and roadside emergency assistance. Simple navigation devices typically tell the customer where they are, but systems like OnStar offer a variety of services and are much more invasive.

GPS Navigation Privacy

Of the top GPS navigation companies, OnStar's unique customer interaction platform makes their system the most susceptible to privacy problems. Although OnStar's privacy practices are suspect, the company is among the few who have a detailed Privacy Policy available online that outlines the information collected from their customers.

OnStar Overview

OnStar began as an emergency assistance program for General Motors (GM) vehicles that allowed customers to push a button on the dashboard to call for emergency assistance. When a customer pushed the button, the GPS receiver on the car would register the vehicle's location and transmit it to the OnStar call center via wireless cell phone networks. Also, OnStar connects the distressed motorist with a customer assistance representative when the OnStar button is pushed. The OnStar systems today are very similar to the original, and only recently has OnStar expanded their existing services, and ventured into the realm of map oriented navigation screens and turn-by-turn navigation assistance.

OnStar Privacy

OnStar's vehicle navigation and roadside assistance technology is available on 50 GM models, which include vehicle lines such as Chevrolet, GMC, Pontiac, Cadillac, Buick, Saturn, Hummer, and Saab (OnStar Vehicles, GM Vehicle Showroom Online). The noticeable difference between OnStar and other GPS navigation companies is that OnStar establishes direct communication with the customer via a wireless cell signal. This means that customers can contact OnStar personnel at the push of a button at anytime. As we know, information goes both ways, and OnStar's creature comforts are also what make it a potential security and privacy concern.

OnStar differs from other GPS systems in more ways than one. The OnStar system is available from the GM factory, and it often comes preinstalled on vehicles. This means OnStar customers did not make a conscious decision to go out and buy GPS technology, and thus they might not be aware of its capability. In addition, GM often gives car buyers free trials of OnStar as a bonus for purchasing a car. Most customers take this bonus at face value not understanding the implications stemming from such technology (GM Online).

OnStar is in a unique position to collect information from millions of people, and they can easily profit from it by selling their customer's data. In its Privacy Policy, OnStar states:

Information we collect about you includes: contact information (such as name, mailing address, email address, phone number and language preference); credit card and billing information (such as cardholder name, card number and subscription package and OnStar Hands-Free Calling minute purchases); and other personal information that helps us customize our

services, such as your requests for emergency assistance or driving directions (OnStar Privacy).

This statement allows OnStar to store any of the information described above. To help put their customers at ease, OnStar insists that their information transferring capabilities are not always on, and the system is only active when needed for emergencies (OnStar Privacy). However, there is a small sentence later on the privacy statement that allows OnStar to turn itself on when "... your OnStar equipment calls OnStar with data updates" (OnStar Privacy). This means an OnStar system can call to "update" anytime, and thus transmit information to OnStar anytime.

Once OnStar has a customer's driving habit information, they can use it for approved uses such as, "to perform market research" (OnStar Privacy). Again, this is a broad term allowing OnStar to use a customer's information in any way they please. The Privacy Policy does not specify who is doing the market research, so third party contracting is possible. This policy also mentions that OnStar may share information with the maker of the car, its wholly owned subsidiaries and its suppliers. The above statement is referring to GM, which has thousands of suppliers and hundreds of subsidiaries. The Privacy Policy goes even further, saying OnStar can give your personal and contact information to car dealers, wireless companies, and XM Radio for promotional purposes (OnStar Privacy).

The most blatant lack for customer privacy concern is in the following statement:

Your contact information, information about your current OnStar services and certain information from your car (i.e., odometer reading) may be shared with our business partners exclusively to conduct joint marketing programs with OnStar or to *confirm eligibility in car insurance discount programs* (our emphasis). We may also share information with our business partners in other circumstances with your permission..." (OnStar. Privacy)

This excerpt illustrates that the Privacy Statement is not really protecting OnStar's customers' privacy, but simply outlines that they have customers' information, and that they are going to use it regardless of the customer's wishes.

Current Government Use

OnStar lists in its privacy statement that if the government serves them with a legal warrant for a person's information, they will turn over personal and car information. This information has been collected many times by police trying to track down criminals who have cars with OnStar. One example is a case in North Carolina where a man had purchased a 2000 Chevrolet Suburban with a fake certified check. The police activated the OnStar system and tracked the man down (McCullagh). This type of use has been permitted by courts several

times, and it makes many privacy advocates wonder where the line will be drawn.

Future Government Use

Many fear that OnStar could be manipulated by the government and turned into what is called a roaming bug. The government's use of a roaming bug means that they activate a customer's asset (car or phone) microphone and listen in on conversations that they believe are important. Concerns over the use of roaming bugs are also being raised in reference to other devices like cell phones whose microphones can also be remotely turned on and off. Luckily for current OnStar customers, the roaming bug is not an issue at present time. The 9th Circuit Court ruled that the FBI's use of OnStar in this way is not permitted since it would render OnStar useless in the case of an emergency (McCullagh). It is important to note that this government use was not overturned for privacy reasons, but rather for safety concerns, and this worries many privacy advocates because the government could easily engineer a fix to this problem. If there is a way around the safety issue roaming bugs may soon become a reality.

Using GPS Information: Google Earth

In the past, if someone were to obtain the vehicle information addressed in this chapter, they would have had a hard time getting an up-to-date photo of all the locations that were listed on a person's vehicle location report. Yet, recent technological advances such as Google Earth make such tracking almost elementary. Google Earth allows customers to see up-to-date images of the entire planet, free of charge. Major cities have higher resolution than rural areas, but the quality level in these outlying areas is still high and improving daily. If a data thief, OnStar, or their competitors wanted to get a visualization of the locations described in a vehicle location report, it would be very easy using Google Earth. This creates even more privacy and security invasion concerns since the whereabouts of a customer's house, children's school and other private information could easily be discerned from their vehicle information.

Google Earth customers can also subscribe to enhanced versions of the program that allows access to extremely high resolution images of the globe (Google Earth Online). These advanced versions are making it even easier to accurately track a person's vehicle history and current whereabouts. The images on Google Earth have reached a level of such high quality that police are now using them to look for illegal marijuana fields. In Racine, Wisconsin, the police did just that to catch a man harvesting marijuana (Late Night). As the quality of Google Earth's images increases, the public's vulnerability to tracking through their vehicles increases along with it.

Conclusion

Vehicles are such a necessity in the lives of Americans that the related privacy issues affect nearly every American. If consumers do not stand up for their rights, companies and the government will be able to

freely know anyone's whereabouts. The practice of tracking people without their consent is already becoming a reality with GPS navigation companies selling personal vehicle location information and employers tracking their employees every move. This problem is not limited solely to GPS navigation companies and employers, but with the decreasing prices for this technology, consumers are at risk of being tracked by one another. The GPS units described in this chapter offer convenience to both consumers and employers for a high price tag, but money is not the only cost. These technologies may soon carry the heavy cost of a complete loss of privacy.

Works Cited

- "2007 OnStar-Equipped Vehicles." OnStar Vehicles Online. 2007. 15 Feb. 2007 <http://www.onstar.com/us_english/jsp/equip_vehicles/07_vehicles.jsp>.
- Bohan, Suzanne. "GPS devices offer peace of mind, but at what price?" Oakland Tribune. 2006. WRITERFind. 20 February 2007 <http://www.findarticles.com/p/articles/mi_qn4176/is_20060904/ai_n16708035/pg_1>.
- "Frequently Asked Questions." LoJack Homepage. 2007. FAQ. 23 February 2007. <<http://www.lojack.com/faq>>.
- "General Motors Corporate Website." GM Online. 2007. GeneralMotors.com. 15 Feb. 2007. <<http://www.GM.com>>.
- "GM Vehicle Showroom." GM Online. 15 Feb. 2007 <<http://www.gmbuypower.com/index.jsp?&partnerId=900014>>.
- "Google Earth. Explore, Search, and Discover." Google Earth Online. 2007. Earth.Google.Com. 15 Feb. 2007 <<http://earth.google.com>>.
- Joyce, Jim. "Conspiracy Goes Mainstream." CNBC. 2006. YouTube. 20 February 2007 <<http://www.youtube.com/watch?v=bmCjoNNkUfg>>.
- Last Night in Little Rock. "A new GPS privacy issue, and Google Earth used to find marijuana patches." Crime In News, Talk Left Online. 2006. Talkleft.com. 15 Feb. 2007. <<http://www.talkleft.com/story/2006/10/18/24911/289>>.
- Lemos, Robert. "Car spy pushes privacy limit." ZDNet News. 2006. Technology News. 20 February 2007 <http://news.zdnet.com/2100-9595_22-530115.html>.
- McCullagh, Declan. "Snooping by satellite." CNET News.com. 2005. Staff Writer. 22 February 2007 <http://news.com.com/2100-1028_3-5533560.html>.
- "Measuring Day-to-Day Variability in Travel Behavior Using GPS Data." U.S. Department of Transportation. 2006. Federal Highway Administration. 23 February 2007 <http://www.usa.gov/dot/highway/2033/gps/ad_152/index=2wm>.
- Onley, Dawn. "Technology Gives Big Brother Capability." HR Magazine. 2005. Vol.50, Iss. 7. 25 February 2007 <<http://proquest.umi.com/pqdweb?index=0&did=864066741&SrchMode=1&sid=3&Fmt=3>>.
- "OnStar Privacy Statement." OnStar Online. 2007. OnStar.com. 15 Feb. 2007. <http://www.onstar.com/us_english/jsp/privacy_policy.jsp>.

“Recent Decision about GPS, Privacy, and the Fourth Amendment.”
Berkeley Intellectual Property Weblog. 2007. Boalt Organization. 22
February 2007 <www.boalt.org/biplog/archives/659>.
Schwart, John. “This Car Can Talk. What It Says May Cause Concern.”
2003. The Newyork Times. 22 February 2007
<[http://www.nytimes.com/2003/12/29/
technology/29car.html?ex=1388120400](http://www.nytimes.com/2003/12/29/technology/29car.html?ex=1388120400)>.

Appendix A

GPS Vehicle Tracking Survey

The following is a survey to ascertain your knowledge of GPS Vehicle Tracking capabilities. Please answer the following questions to the best of your ability.

1. Which of the following GPS tracking companies have you heard of (choose all that apply)
 - a. OnStar
 - b. Garmin
 - c. TomTom
 - d. Kenwood
 - e. MicroTech

2. Which of the following are GPS tracking systems capable of (choose all that apply):
 - a. knowing your speed
 - b. knowing your location
 - c. knowing whether you are wearing your seat belt
 - d. recoding where you have been
 - e. who is driving

3. For which of the following uses are GPS tracking systems allowed to gather and distribute customers’ information (choose only one):
 - a. Marketing research
 - b. Give customer’s driving records to government with no warrant
 - c. Sell/Give to affiliates or anyone they do business with
 - d. All of the above
 - e. Only a & b

4. Under which of the following circumstances can someone track a vehicle without the driver’s knowledge?
 - A. If the tracker knows the driver
 - B. If the tracker owns the car
 - C. If the tracker is renting the car to the driver

5. Is it legal for your parents to track you without your knowledge if they are on the car’s registered title? Yes No

6. Do you have a GPS navigation or tracking system in your car (that you are aware of)? Yes No

7. If yes to 6, do you think that your driving habits are being tracked and stored? Yes No

8. How would you rank your knowledge of GPS navigation systems (1-10, with one be the lowest level of knowledge and 10 the highest). _____

