CONSUMER PRIVACY & IDENTITY QUARTERLY

VOL N°2 ISSUE N°3

DISCLAIMER

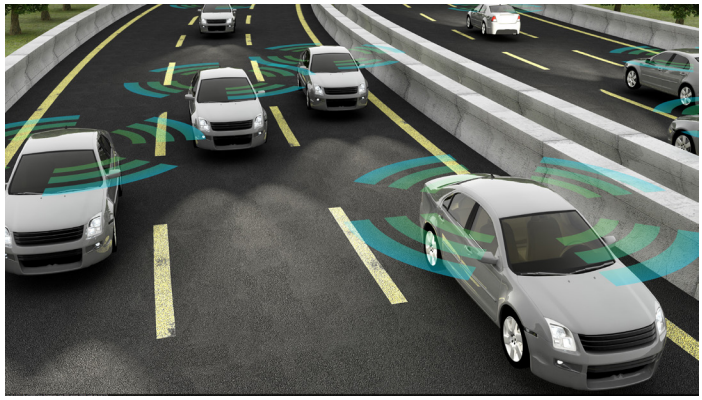
The Department of Defense (DoD) expressly disclaims liability for errors and omissions in the contents of this publication. No warranty of any kind, implied, expressed, statutory, including but not limited to warranties of non-infringement of third party rights, titles, merchantability, or fitness for a particular purpose is given with respect to the contents of this guide or its links to other Internet resources. The information provided in this guide is for general information purposes only. Reference in this guide to any specific commercial product, process, or service, or the use of any trade, firm or corporation name is for the information and convenience of the public and does not constitute endorsement, recommendation or favoring by DoD or the U.S. Government. DoD does not control or guarantee the accuracy, relevance, timeliness, or completeness of information contained in this guide; does not endorse the organizations or their websites referenced herein; does not endorse the views they express or the products/services they offer; cannot authorize the use of copyrighted materials contained in referenced websites. DoD is not responsible for transmissions users receive from the sponsor of the referenced website and does not guarantee that non-DoD websites comply with Section 508 (Accessibility Requirements) of the Rehabilitation Act.

FOR MORE INFORMATION OR QUESTIONS EMAIL osd.ncr.osd.mbx.dodsmartcards@mail.mil

IN THIS ISSUE:

TECHNOLOGY AND TRANSPORTATION

Over the years, technological advances have essentially transformed how Americans travel. The price of convenience is not free. Your personal information and data may be at risk as a result of advanced technology.- *Page 4*



GPS SECURITY: WHAT YOU SHOULD KNOW

GPS (Global Positioning System) has become not just a useful technology but an everyday part of our lives. However, it also comes with security risks. -*Page 5*

ALSO INSIDE:

THE RISE OF AUTOMATIC LICENSE PLATE READERS - *Page 6*

CAR HACKING: IT COULD HAPPEN TO YOU *- Page 7*

THE FUTURE: AUTONOMOUS DRIVING *- Page 12*

INTRODUCTION: TECHNOLOGY & TRANSPORTATION

Over the years, technological advances have essentially transformed how Americans travel. Long gone are the days of printed directions, stand-alone navigation systems, extending your hand to hail a taxi, or gathering that last bit of change to pay a toll. These things sound archaic in today's society as various technologies have gained popularity in recent years. However, the price of convenience is not free. As this issue will detail further, your personal information and data may be at risk as a result of advanced technology.

Global Positioning System (GPS) has become so widespread it can be found in cellular telephones, wrist watches, and vehicles. Being constantly connected certainly has its perks. You can easily navigate a new city with ease, find the fastest route based on real-time traffic, and even track your children's whereabouts. However, this constant connectivity impedes on your privacy as these devices can be manipulated by hackers to gain access to your personal information and data.

With the help of cellular telephones fitted with GPS, the use of ridesharing applications such as Uber and Lyft has skyrocketed, given their sheer convenience and cash-less approach. Uber, in particular, has had its share of controversial policies and strategies over the years. It was revealed that Uber monitors customers for nearly five minutes after the ride is complete. While this was defended by Uber as minimizing driver fraud and increasing location accuracy, it is still a concerning policy that puts your privacy at risk.

Travelling got a little less stressful with the creation of the E-ZPass, a radio frequency identification (RFID) device that helps drivers breeze through toll plazas with little to no wait time. Studies show that these devices have also been used to gather traffic data away from toll plazas and unknowing to users. While these devices do not carry any personal information, they can easily be used to piece together one's travel habits.

The use of the aforementioned technologies is completely up to the user. However, one technology that has gained popularity among law enforcement agencies is Automatic License Plate Readers (ALPRs). These readers are mounted on the back of patrol cars and stationary objects, generally collecting data from users without their knowledge. While there is no way to opt out of this data collection and it was created with the purpose of keeping us safe, everyone should still be aware about the kind of data collected and how it is used.

With the constant advancement of technology, vehicles are now equipped with high-tech capabilities like Bluetooth and cellular radio, which have made cars more susceptible to hacking. If hackers gain access to a vehicle's electronic control unit (ECU), they can suddenly accelerate, manipulate the steering wheel, or slam on the brakes. Autonomous driving is continuing to develop. These self-driving vehicles are outfitted with GPS systems that make them susceptible for hacking. Hackers can conceivably manipulate autonomous vehicles based on their will, placing the vehicle's security and the passengers' safety at risk.

The purpose of this issue is not to deter you from using these devices or make you paranoid about being tracked, but rather to make you aware of the privacy and security risks you may face. Our goal is to help inform you about the advantages and disadvantages of transportation related technologies and how they may affect you. We hope this issue leaves you a more informed and safe traveler for years to come.

GPS SECURITY: WHAT YOU SHOULD KNOW

The days of needing to look up directions before you get in the car and head to your destination are long gone, and an even more distant memory is needing to use a crinkly, folded-up map pulled from your glove compartment. GPS (Global Positioning System) has become not just a useful technology but an everyday part of our lives. However, it also comes with security risks, which will be covered here.

Most smartphones offer various GPS apps for driving, including not just location services and turn-by-turn instructions, but also directions for the quickest route based on real-time traffic, road hazards, and location of speed traps, often ending with arrival times pinpointed to the minute. This shows how advanced GPS technology has become and how important it is to protect yourself from potential dangers associated with broadcasting your precise location.

We are increasingly relying on GPS not only for driving and road awareness, but parents are also entrusting it with their children's safety. Wearable technology in the form of a children's smartwatch uses GPS technology to keep track of their location when out of sight, giving parents peace of mind. There are multiple versions of GPS "Kid Trackers" available on the market today, containing safety zones, video calling, and "listen-in" technology, the capability to press a button and hear what is going on around your child at that moment. There is even a GPS watch that lets the child also track his or her parents when feeling panicked or scared, a two-way surveillance for comfort on both ends. Another feature is a "friend list" to connect with other watch users of the same brand, which parents can monitor, but is a disturbing fact to know that a stranger can gain access to your child.

From our phones, to tracker devices, to GPS systems built into cars, we are constantly being monitored. Smart phones and other personal technologies continually expose your location, leaving you vulnerable to inherent risks if the data lands in the wrong hands. Even photographs taken by your cell phone can quickly pin and share your coordinates with hackers or anyone on social media who views a posted photograph. Any geolocation tag can be linked to your home address and also reveal your location at the moment, so thieves can see when you aren't home. Data patterns open the door for cyberstalkers, targeted crimes, and surveillance of your every move by complete strangers.

Another potential for abuse comes from the possibility of hackers being able to exploit security weaknesses in the GPS devices and tricking the user into believing they are at another location, called "GPS spoofing." In terms of driving, hackers can give the wrong GPS position and direct the victim to a different, dangerous, location.

Another concern is that while GPS tracker devices are marketed as safety devices, they, in great detail, tell the whereabouts of valuable things people might want to steal or harm and provide an easy target. While the GPS does not explicitly say what it is tracking, analyzing location patterns such as movement from a residence to an elementary school at the same time every morning can indicate that the target is a child, for example. Simple data analysis and surveillance can detect patterns that leave you, your family, or your property vulnerable to malicious intent.

In addition to tracking your person or your valuables, GPS has infiltrated the business world and can now affect you both financially and legally. Car insurance companies are introducing the concept of tracking your every move on the road via a plug-in device which sends data wirelessly to the company. The companies then use

Continues on Page 6...

your data to grade your driving skills and offer a discount if you behave on the road. They analyze data such as your acceleration, deceleration, turns, time of day (it's riskier to drive in rush hour or in the middle of the night), and speed. If they approve of your grade, you get a discount off your premium. However, the cost of this discount is your privacy. For example, divorce lawyers have subpoenaed this information to prove someone's whereabouts. Also, while the company can pull the data if you think it will prove you were not at fault during an accident, it's reasonable to say that the company will begin doing this for all future claims, whether to prove your innocence or guilt.

As a general safety guideline, you must be aware of who else may be seeing your data and how it can be used. If you use mobile apps that ask for geolocation to be enabled, it is recommended you turn off the option unless it is needed. Verify that any app you download is from a legitimate source. Since the public accessibility of GPS technology is relatively new, manufacturers are working on introducing new software that can better detect GPS spoofing; therefore, it is important to keep your devices up-to-date with simple software upgrades provided by the manufacturer of the device. GPS usage comes with both value and risks, but the risks can be at least reduced by using it wisely.

THE RISE OF AUTOMATIC LICENSE PLATE READERS

Privacy, the state of being free from public attention, may feel nearly impossible in today's technologically advanced society. Once you leave the confines of your home, it's no secret that surveillance cameras watch your every move while walking down public streets or shopping in your local supermarket. Over the years, the widespread use of Automatic License Plate Readers (ALPR) has introduced a new form of public surveillance. These high-speed cameras are mounted on police cars and stationary objects throughout the United States, collecting up to 1,800 plates per minute by converting an image of a vehicle's plate into alphanumeric data.

These computer-controlled devices query the captured plate number against "hot lists" and can provide law enforcement with an instantaneous alert when a match is made. Once a plate is queried and yields negative results, one might think this information is discarded. However, often times the plate number and precise date, time, and location where it was encountered is retained in databases, for varying lengths of time. Additionally, this information may even be pooled in regional systems that are accessible not only to law enforcement agencies but to private companies as well.

The privacy concerns among citizens continue to increase as ALPRs continue to gain popularity. If analyzed, the information gathered by these readers could piece together the activities and habits of all vehicles encountered for extended periods of time. That said, law enforcement officials indicate the readers are not used to track citizens, but rather to help solve crimes. The data collected and retained from these readers does not contain any personally identifiable information (beyond the license plate numbers) and all ALPR data is protected by the Driver's Privacy Protection Act. While ALPRs are intended to keep us safe, privacy concerns are valid when this collection is not optional and the data is held for undefined lengths of time.

CAR HACKING: IT COULD HAPPEN TO YOU

People are creatures of habit, and habits can have a calming influence on thoughts and actions. Driving in a car is one of those everyday habitual tasks that people take for granted. Imagine cruising along the highway at a comfortable 70 miles per hour without a care in the world and then suddenly the car engine shuts off. What would you do? This terrifying situation is just one possibility of car hacking, which is defined as the manipulation of the code in a car's electronic control unit (ECU) to exploit a vulnerability and gain control of other ECU units in the vehicle.

Cyber security researchers Charlie Miller and Chris Valasek have performed hacks on vehicles, most notably gaining access to shut off a Jeep Cherokee, over the past couple of years. The results of these experimental hacks have proven to be quite alarming. Miller and Valasek used the Internet to "remotely hijack" the digital systems of a Jeep, leading to a recall of 1.4 million vehicles by Chrysler. Sudden acceleration, slamming on the car's brakes, and even manipulating the steering wheel while driving at any speed are just some of the other things the security researchers could do simply by directing carefully constructed messages on the vehicle's internal network. The work that security researchers are conducting to point out security flaws foreshadows greater concerns that malicious actors could exploit.

Evolving wireless attack methods should not come as a big surprise. ECUs in cars have been in existence since the early 1960's and over the past 50+ years they have become more and more essential to a vehicle's basic functioning. According to Linda Melone of *Computerworld*, more powerful ECUs, including features like GM's OnStar system, were introduced by car manufacturers in the mid-1990s. This OnStar system, which is responsible for detecting and notifying the driver of any issues, presents a problem hidden in its convenience. Car computers have now become susceptible to the same viruses experienced by regular computers because these ECUs connect both to one another and to the Internet. These developments could create vulnerabilities in features such as: braking, steering, air bag deployment, and various other internal systems.

High-tech vehicles with modern car accessories like Bluetooth, cellular radio, and other mobile devices are even more at risk of potential hacks, according to researchers at the University of California. While advances in technology have increased the convenience level for consumers, there is still an inherent risk in continuing to push the envelope. Our technological creativity is adding new ways for hackers to be creative when they hijack our vehicles.

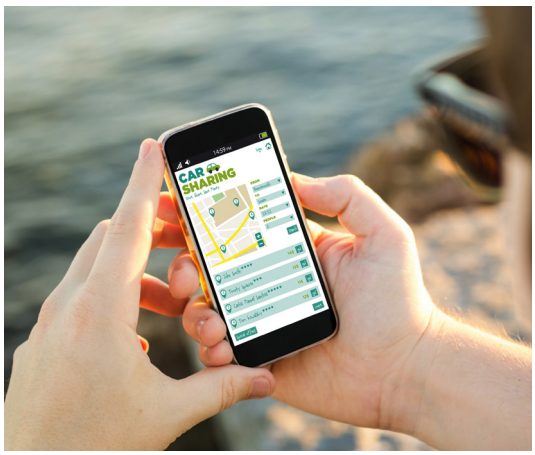
In 2012, a former employee at a car dealership in Austin, Texas, demonstrated this creativity. The employee was able to activate the horn and immobilize the ignition system in more than 100 vehicles. This was done by hacking into company computers and initiating the vehicle-immobilization system. The immobilization system involves an electronic security device fitted to the car that prevents the engine from running unless the correct key is present, which also prevents the car from being hot-wired after the initial entry. New technologies may be providing the hackers with even more tools and attack methods. As the security breach case in Austin undoubtedly proved, where there is a will, there is a way.

Continues on Page 8...

Some vehicles have a slower software development cycle than others, which makes it hard to keep up with new and improving hack methods. Another case in Texas last year saw hackers using a "black box" method to break into and steal more than 30 Jeeps. The vehicle's internal network was connected to a laptop through a port on the dashboard, according to Flavio Garcia, a University of Birmingham computer scientist. This method allowed the hackers to steal considerably more vehicles than an average hack would have. Is further attention to security analysis needed before the vehicle is even in production? Yes, according to Garcia. Urging for change, he stated, "It's a bit worrying to see security techniques from the 1990s used in new vehicles…. If we want to have secure, autonomous, interconnected vehicles, that has to change."

Wireless additions to cars have opened a dangerous gateway full of possible security risks and vulnerabilities. To prevent a carjacking, the best advice is to stay alert and be mindful of your surrounding area. The same can be said to combat against car hacking. People must be prepared and unafraid to educate themselves on different cybersecurity issues as cyber-attacks and threats are more common than ever before. The research conducted by Miller and Valasek underscores the need for all of us to seek out basic cybersecurity literacy. Neglecting vehicle security issues doesn't have to become an everyday habitual task that people take for granted. Some habits are made to be broken.

RIDESHARING: CONVENIENCE AND CONCERNS



Ridesharing apps are incredibly convenient. Nowadays, you can arrange for short-notice transportation just by tapping your cell phone. Uber, Lyft, and Sidecar are some examples of ridesharing companies that have proved to be highly successful. For example, Uber is used worldwide because it offers reliable pickups and clear and affordable pricing after a mere tap of the phone.

Ridesharing services may be convenient, but they also offer their share of security concerns. Uber monitors the location of a user for nearly five minutes after the person is done with the service. While Uber has defended this policy as an aid in detecting driver fraud and improving location accuracy, this policy has been met with some resistance.

Uber has used different strategies to fight back against resistance of its service and its competitors. Beginning in 2014, Uber used a software system called Greyball to identify and target law enforcement seeking to shut down Uber in jurisdictions where it was not allowed. Another more recent strategy utilized by Uber involved spying on fellow competitor, Lyft, using a software named, "Hell." This software involved creating phony Lyft user accounts so that Uber could in turn monitor its competitors' pricing and whether drivers were working for both companies. These strategies represent violations of users' security and privacy.

The onus is on the user to determine the amount of personal data a ridesharing company collects, and to decide which service to use. While there are other services like Uber, we do not know how much data they collect, or with whom they share the data. In the end, being knowledgeable about possible security concerns and analyzing involved risk is vital to maintaining security in an increasingly insecure environment.

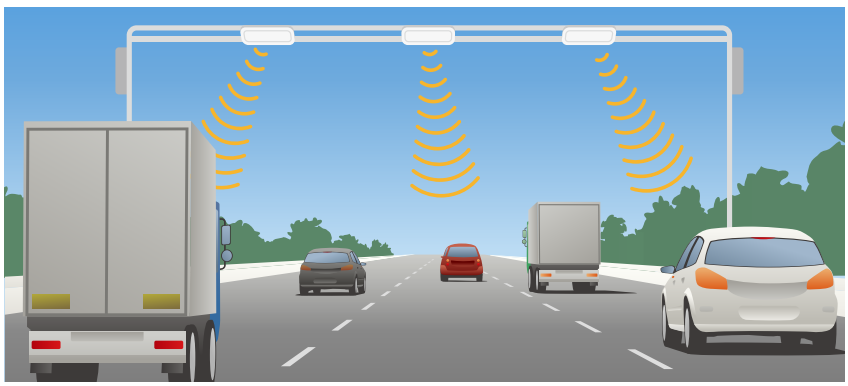
ELECTRONIC TOLL COLLECTION PRIVACY CONCERNS

If you hate waiting in long lines, you are not alone. Americans spend roughly 37 billion hours waiting in line each year. Transportation agencies have taken note of this and have created a radio frequency identification (RFID) device that allows drivers to smoothly pass through a toll plaza without waiting in line to pay. This device, known as an E-ZPass, is a pre-paid electronic toll collection system that uses transponders attached to user's vehicles and overhead antennas that collect the toll. These devices are purchased with the intent of paying a toll and minimizing wait time, but what happens when these mechanisms are used to systematically collect data on E-ZPass users?

The Terms and Conditions of an E-ZPass vary among the 16 participating states. For instance, Virginia's privacy policy states that the Virginia Department of Transportation may provide summarized E-ZPass data for transportation research. The type of information and who it is being reported to is unknown. Meanwhile in New York, the Terms and Conditions for the E-ZPass program make no mention of conducting research using the data from users. However, the results of a New York Civil Liberties Union investigation revealed E-ZPass antennas were placed around New York City away from toll plazas by city and state transportation agencies to gather congestion and traffic volume data.

Whether this data collection is used to track users or is a violation of privacy is unknown. TransCore, the company that makes the New York RFID readers, indicates that the information collected by the readers is not stored and would not be successful in tracking drivers or their speeds. The only way to virtually "opt out" of this data collection is to block the signal by storing your E-ZPass, when not in use, in a Faraday cage type bag made of flexible metallic fabric through which a signal cannot be read.

Although E-ZPass does not appear to sell your personal information or travel data, there are still risks involved. Each E-ZPass is accompanied by an online account that houses the following personal information: full name, home address, telephone number, email address, driver's license number, license plate number, credit card number, and up to two years of toll transactions. This is the type of personal information that hackers are looking for. Be sure to protect yourself and your online account by creating a unique password with at least twelve characters, keep your password in a safe and secure place, and monitor your account for any suspicious activities.



Electronic Toll collection uses networked readers that scan for RFID enabled transponders. Some readers work at highway speeds.

THE FUTURE: AUTONOMOUS DRIVING

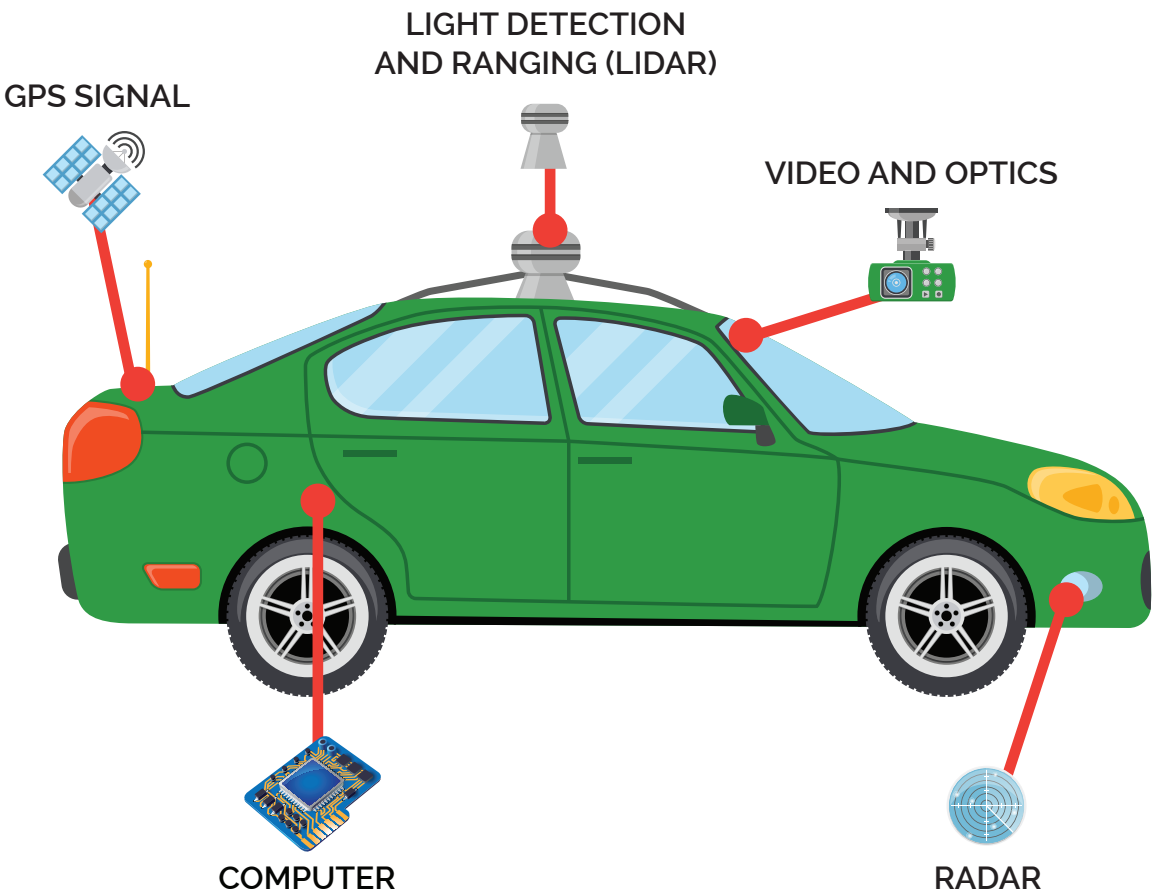
Self-driving cars, or, autonomous driving, have been a long-anticipated indication that the future has arrived. Even just a few years ago, the idea of a self-driving car seemed like something out of a science-fiction movie. However, as computers have gradually become a part of our vehicles, to include automatic parking, lane warning, intelligent cruise control, and emergency braking, it seems only natural that we are progressing to fully computerized, autonomous vehicles. Today, multiple car companies are actively competing with each other to design their own model of autonomous cars: Volkswagen, Mercedes-Benz, Volvo, and even Google. The idea comes with many possibilities and increased freedom at the wheel, but presents several drawbacks and concerns. We will discuss both here.

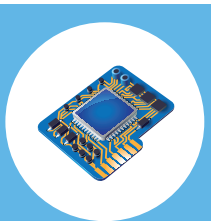
As far as improving our commutes, autonomous driving will make life on the road better in several ways. First, self-driving cars would mean a reduction in vehicular deaths on the road from car accidents, as well as saving healthcare costs related to these accidents. Autonomous driving could change the car and driving industry completely; according to the National Highway Traffic Safety Administration, 94% of most car accidents are due to human error, which are faults attributed to things like decision-errors, performance-errors, and recognition errors. Deaths and injuries from auto accidents will decrease substantially when human errors are eliminated from the act of driving. Drunk driving, speeding, and distractions such as talking to other passengers, adjusting the car audio, eating, drinking, or using the phone, will no longer be problems. These developments could impact the car insurance industry for the better, meaning autonomous cars could end up saving society money in the long run.

However, that saving of money could come at a high safety cost. A big source of security risks for autonomous vehicles comes from the ability of malicious actors to override and control the internal computers. Most, if not all, autonomous vehicles will include a GPS (Global Positioning System) in their design. As with any GPS-enabled device, there is the risk and concern of hacking. Hackers can gain access to the GPS device in the car and use "GPS spoofing," that is, falsifying your coordinates and location for their benefit. Skilled actors with malicious intent could potentially send your car to a different location or off a cliff. They could also conceivably hack into the car's system to access, and control, the car's lock, horn, and flashing lights. An even more disturbing, and arguably the most important, risk is that this could lead to a someone hacking and gaining total access to your car.

Despite the warnings and risks, we are still likely years away from self-driving cars being available on the commercial market. However, these are important concerns to consider beforehand. Automobile companies are already working to mitigate these risks; currently, chip manufacturers are considering introducing new software that can better detect GPS spoofing. It is daunting to consider a future of driverless cars passing you on the highway, and only time will tell if security measures are effective enough to keep you safe, or if they aren't worth the risk.

THE TECHNOLOGY BEHIND SELF DRIVING VEHICLES



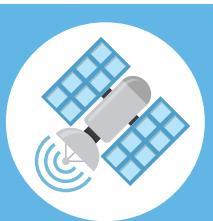


COMPUTER

The onboard computer translates the data collected by all of the instruments in the car. Most vehicles need more processing power than you would find in your average home desktop computer.

RADAR

RADAR sensors in the front and back of the vehicle scan for objects at long ranges.

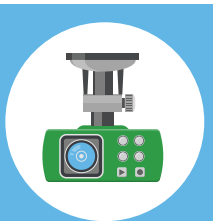


GPS

A built in global positioning system works to keep the car on route with an accuracy of one foot.

LIDAR

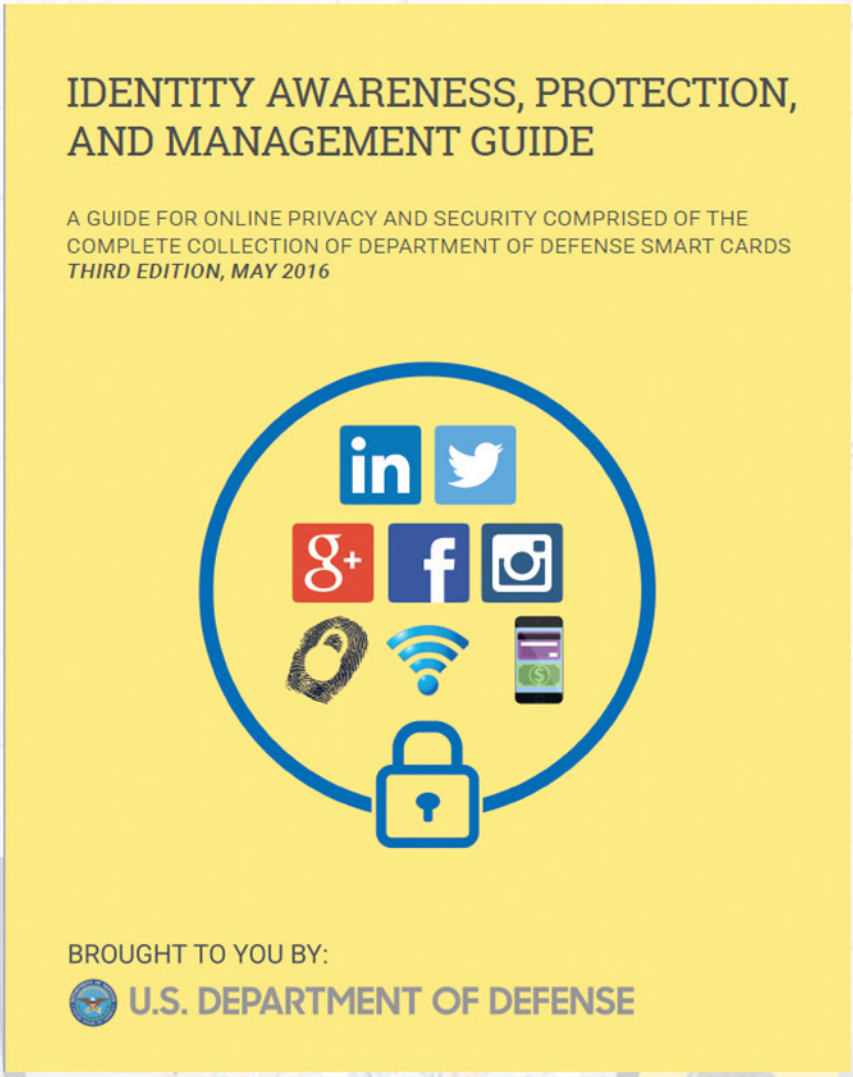
LIDAR emits a laser onto a spinning mirror and outwards 360 degrees around the vehicle to detect obstacles within 100 meters.



VIDEO/OPTICS

Video cameras are used to identify road signs, traffic signals, and lane markers, depending on their location.

For more detailed information on protecting and managing other key elements of your identity footprint online please check out the Identity Awareness, Protection, and Management Guide.



Send an email to this address to get your copy!
OSD.NCR.OSD.MBX.DODSMARTCARDS@MAIL.MIL