California State University, San Bernardino
CSUSB ScholarWorks

Electronic Theses, Projects, and Dissertations

Office of Graduate Studies

6-2020

GEOFENCING AS APPLIED WITHIN THE FIELD OF CYBERSECURITY: AN OVERVIEW OF POTENTIAL RISKS AND ADVANTAGES

Kasandra Adams

GEOFENCING AS APPLIED WITHIN THE FIELD OF CYBERSECURITY: AN OVERVIEW OF POTENTIAL RISKS AND ADVANTAGES

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

in

Information Systems and Technology

by

Kasandra D. Adams

June 2020

GEO-FENCING AS APPLIED WITHIN THE FIELD OF CYBERSECURITY AN OVERVIEW OF POTENTIAL RISKS AND ADVANTAGES

A Project

Presented to the

Faculty of

California State University,

San Bernardino

by

Kasandra D. Adams

June 2020

Approved by:

Tony Coulson PhD, Committee Co-Chair

Vincent Nestler PhD, Committee Co-Chair

Conrad Shayo PhD, Committee Member

Javad Varzandeh PhD, Department Chair

ABSTRACT

This culminating experience project explores geofencing as a potential risk and advantageous tool within the field of cybersecurity. Geofencing is defined here as a software program feature that allows its users to collect and deliver data within a specific targeted geographical area. Currently used applications are addressed from a cybersecurity mindset by applying the hacker methodology to demonstrate the potential threat. Additionally, geofencing is applied to the NIST Cybersecurity Framework to demonstrate potential benefits for cyber defence. Finally, vulnerabilities associated with applying geofencing to cyber defense, and its potential implications on privacy and cybersecurity laws is discussed and recommendations for further research are suggested.

Key findings include:

- Demonstrating geofencing as an unknown threat in the field of cybersecurity, suggesting attention be dedicated to the type of data that is collected and the safety measures protecting that data.
- Geofencing can be used as a tool to defend as well as support risk management. By using it as a source of data collection, decisions can be implemented to better manage the risk of devices entering and leaving a specified geographical area.
- Geofencing can provide data that falls into Personally Identifiable Information (PII) which should make it regulated under most privacy laws.

- Current privacy policies and laws are insufficient when the scope of geofencing is applied to current methodologies. Geofencing must be regulated in a fashion that ensures data collected is necessary and relevant, and that the data is kept safe from potential threats.

ACKNOWLEDGEMENTS

I want to take this opportunity to thank all those who have always believed in me. Those who saw the fire that lived in me and who helped me set it free. I wouldn't be the person I am today without your unwavering support. Thank you to my faculty mentors, my family and my most dedicated friends

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

With the ever-evolving threat of hacker innovation, cybersecurity administrators must be vigilant in staying abreast of new and emerging technologies that can be used as a tool for malicious threats. Often, due to the rapid evolution in technology, policies, laws, and regulations are established after a zero-day threat has been announced and well after substantive damage has been done. Geographical Information Systems, specifically geofencing, is one of those impending threats. This project is a demonstration that geofencing can be used as a tool for hackers. Specific attention will be given to the lack of policies and barriers necessary to avert this threat.

Geofencing, written interchangeably as geo-fencing, is a tool, that is mostly used in marketing campaigns to collect and distribute information within a specified geographical location. Other uses of geofencing include, airspace regulation of drones, tracking at risk populations and location-based push notifications by cell phone carriers. The value of geofencing technology is the ability to collect or provide information within a set geographical area. Information and data analytics feed administrative decisions, therefore, geofencing affords its user the ability to capture and distribute data in real time, with location based precision, thus enhancing the accuracy of the information derived. This tool allows its user to collect an exponential amount of data within a given virtually fenced area. This is done with minimal limitations and often without the knowledge or consent of the patron, whose data is being harvested. This begs many questions:

1. Is geofencing an unknown threat in the field of cybersecurity?
2. Can it be used as a tool in a risk management plan?
3. Is the data collected using geofencing considered PII and if so, how is it being protected?
4. Are there laws and regulations already developed to guide application developers and users of geofencing? If not, is there a need for new laws and regulations be developed?

This project will explain geofencing, where it is commonly found, new and emerging practices. It will discuss laws and regulations currently in place that pertain to those uses to see if they are sufficient in aiding the protection of data. The hacker methodology and NIST framework will be reference as widely accepted methods of attack and defense. These will be used to prove geofencing as a tool that should be regulated. Finally, suggestions for future research and action will be suggested.

CHAPTER TWO

GEOFENCING

Geofencing Defined

Depending on its application, geofencing can be described in many ways. In 2015, geofencing is described in a paper on performance assessment of geo-triggering in small geo-fences as “a virtual perimeter for a real-world geographic area that allows users to receive notifications whenever they enter or exit a specified area.” (Alsaquer, M., Hilton, B., Horan, T., & Aboulola, O. 2015) Finally, ESRI, a geographical information systems software supplier, defines geofencing as "a designated boundary around a geometry that, if crossed, initiates a notification. Geofences are often used in real-time route Web applications." (ESRI) Therefore, geofencing is a virtual perimeter set around a specified location which can be used to monitor, control, and collect information. It can be used, within applications, to send messages to users and administrators, allowing fluidity in data collection and sharing. This includes the ability for administrators to set a call to action, including but not limited to mobile phone devices, drones, laptops and tablets. In this research project, I will be exploring the potential of geofencing as it relates to cybersecurity, including both the benefits of using geofencing to collect and/or secure information in a location, known vulnerabilities and the potential for using it as an exploitation technique. The goal of this project is to identify the various way geo-fencing, a marketing tool, can be used as a tool in the field of cybersecurity. Specific attention will be given to the inquiry of whether it poses a threat in the field of cybersecurity with the gaining popularity of geographical information systems (GIS) and, if so, whether there is a need for legal regulation.

In their paper, Alsaquer and his associates collected a variety of ways geo-fencing is currently being used, based on a review of their literature. Among those ways are listed location based advertisements, child location services, road safety, gaming, geo-targeted alerts and warnings."(Alsaquer, M., Hilton, B., Horan, T., & Aboulola, O. 2015) Geofencing is also seen in drone airspace regulation, as in using "keep-in, keep-out barriers", (Cho, J., & Yoon, Y., 2018) Alzheimer's and dementia patient location (Yüce, Gülkesen, Barcın, 2012) and large wild animal preservation, specifically, elephants in Africa as seen in the article "Creating Conservation Stewards For A Modern Kenya". Finally, geofencing is seen in logistics management (Oliveiera, Cardoso, Barbosa, J. L. V., da Costa, C. A., & Prado, 2015) and data visualization (Tectonix). "Geo-fencing has been predicted to be a multi-billion dollar market in areas such as retail, ambient intelligence, entertainment, healthcare, etc. Businesses have been adopting geo-fencing technology, and now there are several platform providers such as Google, Qualcomm, ESRI, Urban Airship, and others. These tools are continuing to attract application developers." (Alsaquer, M., Hilton, B., Horan, T., & Aboulola, O. 2015)

Geofencing is being used to collect data all over the world. With minimal consideration to what locations can be targeted, type of data collected, protecting the data collected, this leads to an excessive amount of stored personal data. Data can be sold or stolen with no limitation on the malicious ways it could be utilized.

How It Works

In order to understand geo-fencing and its potential vulnerabilities, one must understand the basic mechanics of how geo-fencing works. There are two parts to geofencing, first, setting the targeted area, known as a geo-definition. Second is the collection or distribution of data and/or information within the virtual perimeter. The perimeter can be defined around a specific point as either a radius or as a polygon. (Alsaquer, M., Hilton, B., Horan, T., & Aboulola, O. 2015) This point is selected based on GPS but can be made more accurate with cellphone towers and Wi-Fi routers, or beacons. The more densely an area is packed with these points, the smaller and more accurate your geofence can become. A geofence can be as small as 10 meters in areas with heavy cell and Wi-Fi access, such as metropolitan areas. (Pulsate, 2016)

Although any device that has Global Positioning System (GPS) or Wi-Fi capabilities can be tracked, the most used device is cell phones. GPS requires a large energy expenditure, while Wi-Fi usage results in almost no noticeable energy cost on the device. “Receiving continuous, accurate, locations using cellular phones results in a tremendous energy cost that reduces the value of locations-based applications; Kim et al. [5].”(Alsaquer, M., Hilton, B., Horan, T., & Aboulola, O. 2015) When considering threats in cybersecurity, we must take this obvious indicator into account as malicious intent will be delivered via Wi-Fi as opposed to directly through GPS. The ideal situation for attackers in cybersecurity is to not only gain access but to maintain access for as long as possible. This requires their presence to remain undetected, in this situation to ensure energy expenditure does not give away their position. This is something that can be highly regulated by the client "ESRI provides a geo-trigger service that allows developers to send targeted messages to users when they enter, exit, or dwell in a geo-fenced area. This service also provides the ability to choose higher levels of accuracy or battery saving by offering different location tracking profiles." (Alsaquer, M., Hilton, B., Horan, T., & Aboulola, O. 2015) How energy expenditure comes into play, will be discussed in more detail in chapter three “Geofencing Applied in Cybersecurity”

Often, location-based services are not a necessity for applications to function but can assist in the customers experience.

> Example: A customer crosses a geofence into a designated location, that customer may receive a notification for a promotional offer or news related item via text message or push notification from an app.

Digital privacy is something many are becoming aware and cautious of. A customer may resent the idea of a company knowing their location, especially if asked to consent immediately when downloading the application. Since geotargeting and data collection are extremely valuable to companies, they are aware of this hesitation and advise clients of ways around it. This ensures they are compliant with data privacy laws to the extent that they receive consent to, but no further.

In some areas, strict regulations require geolocation consent when downloading an application. However, in places with looser regulations, applications are not required to ask for location-based services permission when the customer initially installs an app. Instead, the permission can be set up to be requested at a later time, so long as it is requested before accessing the customers geolocation. The suggested method is to ask once the customer has been using the app, realizes the benefit and then would like to use a function on the app that requires location. The customer is then, more inclined to grant permission.

CHAPTER THREE

GEOFENCING APPLIED IN CYBERSECURITY

In this chapter, geofencing will be presented as a tool to be used by malicious threats via the hacker methodology and as a tool for defense with the NIST Framework. Once this has been successfully demonstrated as a tool, legal barriers, policies and regulations that are applicable to, will be applied to demonstrate the gap in legal boundaries and the need for more severe regulations.

Risk Profiling Based on Current Cybersecurity Practices

To ensure complete understanding of the risk and benefits associates with geofencing within the field of cybersecurity, a general overview of the subject needs to be presented. The National Institute for Science and Technology defines cybersecurity as “"Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."(NIST) In this project, cybersecurity is defined as the protection and security of data held electronically.

Within the field of cybersecurity are many malicious threats, one of which is called hackers. NIST defines the hacker as an “unauthorized user who attempts to or gains access to an information system.” (NIST) The hacker’s goal is to breach an organizations security and gain access for a variety of reasons, but for this project we will focus on stealing data. Hackers use an abundance of tools to achieve this, from social engineering, to brute force cyberattacks. The hacker's path is often referred to as the "Hacker Methodology". Organizations have teams designed to keep these adversaries out and kick them out if/when they get in. One of the major tactics used to help protect data assets is the NIST Framework. Both the hacker methodology and the NIST framework can benefit from using geofencing as a tool. As there is little to no regulation on its usage, this is to be considered with some caution.

In the following sections, both the Hacker methodology and NIST Frameworks will be explained. To support the project hypothesis, that geofencing is a tool that can be used for malicious threats, for preventing attacks and that it is unregulated by current laws, each "process step" will offer the following:

- Process Step: An overview of the process
- Tool Example: How geofencing could be used as a tool applied to the process step
- Current Application Example: A current application of geofencing similar or related to the process step or tool example
- Potential Risk: A suggestion on the potential risk or liability associated with the geofencing capabilities
- Potential Benefit; A suggestion on the potential benefit to be gained by using geofencing capabilities

The Hacker Methodology

Hacker Methodology is taught in cybersecurity courses to assist specialist in fighting against attackers puts defenders in a a frame of mind that allows them to think like the adversary. Similar methods such as the “kill chain” or “penetration testing” process could be used as well. (NIST) This methodology will be used as a framework to display the potential security risks posed by geofencing. The framework seen in Figure 3.1 is a rendition of the NIST methodology and includes:

- Reconnaissance: Background information hunting
- Scanning: Listing all potential entry points
- Gain Access: Exploit the information found previously to gain entry
- Maintain Access: Create a foothold
- Cover Tracks: Attempt to make it impossible to find you

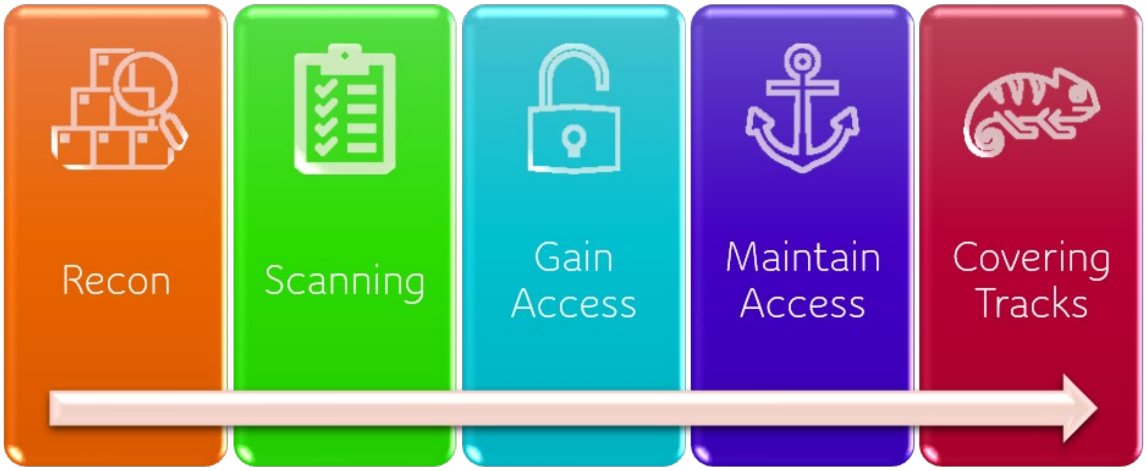


Figure 3.1: Rendition of the Hacker Methodology

Hacker Method Step 1: Reconnaissance “recon”. This step encompasses everything required to find out intelligence on the target. This includes corporation information, server names, names of coworkers, and social media accounts. Gathering this information will aid an attacker in password cracking, social engineering and many other possible scenarios for gathering personal data. (Nestler, 2019)

Tool Example 1:

Geofencing has the potential of aiding attackers in gathering this data. In an interview with a private investigative firm, Diedre R. Lane, Investigative Case Manager at National Business Investigations, Inc. was quoted to state that being able to geofence a specific location to gather open source intelligence and potentially capture incriminating evidence on targets would be lucrative. (Adams, Lane, 2019)

Current Application Example 1:

Many applications are being built specifically to target shoppers, others are built to gather and share information. You can ask Siri, Alexa, Bixby or Google, the personal assistant applications on various smartphones, to remind you to do a task when you get home. This requires the devise to know where your home is, track your geographical location and set up an alert when you cross into a specified area around your home.

Google Maps, Apple Maps, Waze and MAPS.ME are a few popular navigation service apps that rely on customer sourced data to function. By collecting the data of those using the application, the map services can tell customers how long their commute may be, if there are traffic disruptions or potential hazards. The reliability of the application's information is dependent on the customer actively enabling GPS and/or having the application running in the background. Information is being gathered even when the customer is unaware.

Potential Risk Example 1:

Consider how knowing a target's location patterns and being able to set a geo targeted fence alerting you to that's targets comings and goings could be valuable to hacker or be used to protect a company.

Potential Benefit Example 1:

Physical corporate espionage could be prevented or exposed, where digital means cannot.

Hacker Method Step 2: Scanning. This requires the attacker find all devices on the specific network their target is using, including both personally and professionally. The attacker is seeking ports that are open on each device, cellphones, laptops, tablets, desktops etc. They take note of what applications are running on each port, and what version. Once established, they use that information to research for known vulnerabilities that can be exploited. (Nestler, 2019)

Tool Example 2:

Geofencing can tell an attacker a devices IP address, what applications to target as well as what the people surrounding their target are using. If an attacker were to geofence a house, or an office building and gain access to devices surrounding a target, no amount of protection on that targets devices will protect them. Those around them, family members, neighbors, coworkers and customers could provide the vulnerabilities that attacker needed to compromise the target, simply by their nearness.

Current Application Example 2:

China is currently using geofencing to monitor and track its citizens during the COVID-19 pandemic. By monitoring where they have gone geographically, they can set up alerts and use predictive analytics to define a risk factor for their citizens. This risk factor is displayed on their mobile device as a coded color/number and monitored by law enforcement. This allows those at high risk of being exposed to be quarantined and slow the spread of the disease. This brings human rights and privacy into question, as mentioned in an interview in the NYTimes "such surveillance creep would have historical precedent, said Maya Wang, a China researcher for Human Rights Watch. China has a record of using major events, including the 2008 Beijing Olympics and the 2010 World Expo in Shanghai, to introduce new monitoring tools that outlast their original purpose, Ms. Wang said. “The coronavirus outbreak is proving to be one of those landmarks in the history of the spread of mass surveillance in China,” she said." (Mozur, Zhong, &amp; Krolik, 2020)

Potential Risk Example 2:

By collecting IP addresses, a hacker has begun “scanning”. IP addresses and the ability to send text messages or push notifications to devices give attackers the power to send malicious links, monitor devices and potentially control devices. Many children have cellphones now. By geofencing a target’s children, at school, in transit at a bus station, or at a friend’s house, an attacker could use the less secure situation to gain access.

Potential Benefit Example 2:

By understanding how geofencing can be used, higher security can be placed by platforms and companies on where a geofence can be placed and what data can be collected. If a phone could be placed in “child mode” essentially quarantining it from all data collection, including geofencing, this risk could be mitigated.

Hacker Method Step 3: Gain Access. Also known as the exploitation phase, in this step, an attacker would crack passwords, look for back doors, use social engineering, etc. (Nestler, 2019)

Tool Example 3:

A geofence could allow the attacker to gather information such as where a target frequents, gather pertinent information and provide a foothold for social engineering that would gain much information. As mentioned in chapter one's section on applications, many apps are using location-based services to send push notifications to their customers. When attempting social engineering, a hacker could infiltrate and send false push notifications to gather information or send compromised links. Attackers can even infiltrate through physical means, sneaking in, and gaining access to the device.

Current Application Example 3:

The safety and location awareness of at-risk populations is another way we see geofencing in today's society. Many are using this for their children, to receive alerts when they arrive and leave school or home. Recently, this concept has been applied to Alzheimer's patients, to help keep them safe as well. Yüce and his associate discuss the use of geofencing for Alzheimer's patients in their article "Geotracking Patients with Alzheimer's Using a Personalized Geotracking System with Social Support Network". The system was being constructed using Java at the time of the article’s release but they speak about how it should function as "a personalized geotracking system that aims to balance patient security and need for privacy and autonomy is proposed. In addition, the system tries to form and organize a social support network among family caregivers to help each other locating patients during wandering episodes. The system introduces a personalized, four-level temporal geofence based tracking, warning and notification protocol that incorporates a safety check mechanism operating over Global System for Mobile Communications network."(Yüce, Gülkesen, Barcın, 2012)

Potential Risk Example 3:

Privacy, human rights and potential risks are the major source of concern for this functionality. Taking advantage of knowing these at risk populations’ locations in real time puts the safety of children and elderly under scrutiny.

Potential Benefit Example 3:

The information being collected and shared through geofencing is helping to protect at risk populations, and wildlife. Through geotracking, children, Alzheimer’s and dementia patients and larger potentially destructive wild animals, alert their care takers when they travel out of range or into danger. This allows an authority figure to take action and ensure the safety of the target being monitored. This is an immense benefit, especially to those that are caring for or monitoring many targets at once.

Hacker Method Step 4: Maintenance. Once they have gained access, they want to stay in, to monitor their targets actions or gather data. They use tactics to plant back doors, add other user accounts, and access other machines, essentially becoming a weed in the system. The reconnaissance work done previously, combined geofencing can assist the attacker in becoming very difficult to locate and remove. (Nestler, 2019)

Tool Example 4:

Geofencing can also alert the attacker to the movements of their target. Notifications and continual monitoring can keep the hacker ahead of the game as seen in the next and final step.

Current Application Example 4:

ESRI, a national leader in the software and platform development for GIS used geofencing with many of its customer offering. "The ArcGIS GeoEvent Server is ESRI's geofencing platform. You can connect to GPS devices and social media and construct your own real-time awareness apps. Also, you can connect to streaming data feeds and automatically send alerts by emails or text messages. In addition, you can update a database or perform other types of events."(Bob, Nik, Randy, & Daniel, 2019) Social Media is not directly mentioned here, however, by geofencing a specific location, you can target open source information (OSI) and gather data.

Potential Risk Example 4:

Although its main purpose is to be used as a tool for clients to send information, this platform, if hacked could send false information, and collect data on every devise connected to the source. Further, platforms can be combined, “Valarm is one of the leading monitoring platforms that uses geofencing. They’ve monitored flooding, air quality and even noise with a real-time dashboard. One of the best things is how it integrates with ArcGIS Online, ESRI’s cloud-based platform. As part of this whole platform, users can intuitively create apps and maps in the cloud. In turn, your organization can use these online apps for mobile, tablet and even field collection."(Bob, Nik, Randy, & Daniel, 2019)

Hacker Method Step 5: Covering Tracks. The goal of step 5 is to make tracing the attack back to the malicious source, to difficult or costly to achieve. Some infiltrations remain unnoticed indefinitely. (Nestler, 2019)

Tool Example 5: If a hacker was attempting to cover their tracks and knew geofencing was a tool being utilized, they could potentially “hack” their location data. This would essentially send the team tracking them on a wild goose chase.

Current Application Example 5: Applications have been developed to track at risk populations, namely children but more recently Alzheimer’s patient. These populations need to be monitored for teir protection. By setting up alerts when they enter or leave a location, those monitoring can be alerted to potential danger.

Potential Risk Example 5:

When considering using geofencing as a method in cybersecurity, the known vulnerabilities must be considered. A major source of vulnerabilities is provided from a 2014 analysis by NCCGroup. They discovered flaws in false information presentation, third party intervention and code manipulation. The NCCGroup discovered a flaw in being able to monitor targets. They state "we have found that it is possible to bypass their geofencing capability and to send false location information to users. This effectively means that if users are utilizing such applications to keep track of resources or people, attackers could make it look like these people or resources are not where they should be."(NCCGroup, 2014)

This research applies to the targets themselves being able to manipulate their own data, or vulnerable populations being targeted due to their known location. "One of the popular uses of geofencing apps is to track children, but users, and this even includes clever kids, could hack the app to make it look as though they are always in a safe place.

> Kidnappers could hack the app to make out the child is where they are supposed to be, when in actual fact they are in a different location and could send false signals in order to confuse both police and parents to their actual whereabouts."(NCCGroup, 2014) If geofencing is being used to track or implicate threats, this inability to be able to offer sound proof of location ruins the reliability of the tool. The code would need to be fortified to assist in ensuring location reliability. This type of vulnerability was discovered by NCCGroup across all platforms, "we found that all of the applications that we tested were vulnerable to similar attacks involving HTTP modification via active traffic interceptions, and to third-party GPS spoofing applications. Some were vulnerable to straightforward code decompilation and modification." (NCCGroup, 2014)
>
> Potential Benefit Example 5:
>
> This function, is rendered safe from tampering, gives administrators the ability to safely monitor the comings and goings of people and devices entering a physical location. By being alerted to abnormal situations as opposed to constant monitoring, the administrator has the benefit of geotracking while the personnel maintain privacy in their comings and goings within and outside of the fence.

Depending on the goal of the infiltration the plan may be to get in and get information or plant a virus, bug, worm etc. meant to cause damage. However, with the sales of information and data being so lucrative in today's market, often the hacker is in the system to monitor continuously for data. Geofencing is a tool, if left unchecked, that can make hacker's that much better in achieving their goal and compromising or stealing data.

NIST Cybersecurity Framework Version 1.1

The National Institute of Standards and Technology (NIST) has developed a cybersecurity framework to be used as a guideline for organizations to protect data through careful risk assessment and planning. It has five steps that can be utilized in a cyclecar fashion to prevent and recover from data intrusion as shown in Figure 3.2. (NIST, 2019) The Framework includes the following steps:

- Identify: Discern an organization risk profile
- Protect: Develop a plan to protect assets
- Detect: Create a plan to detect intruders
- Respond: Plan for responding to intrusion
- Recover: An action plan to minimize losses after intrusion

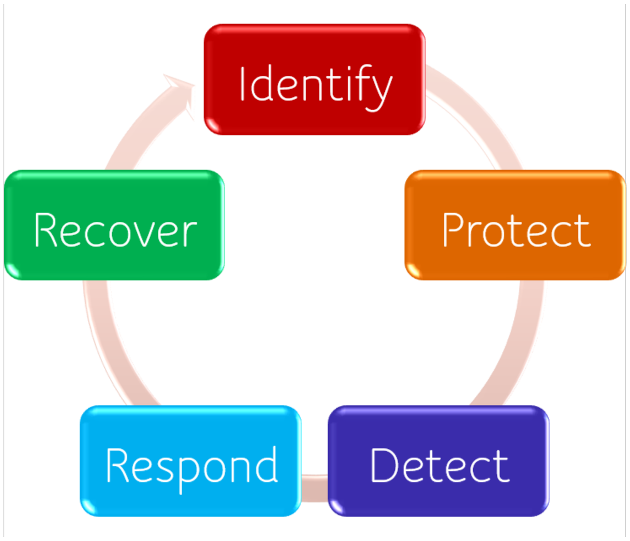


Figure 3.2: NIST Cybersecurity Framework Version 1.1 (NIST, 2019)

As demonstrated with the hacker methodology the NIST framework will be used here to display the potential security benefits posed by geofence encapsulation. The same format is applied: Step> Tool Application> Current Application> Potential Risk> Potential Benefit.

NIST Step 1: Identify. The Organization must develop a risk profile to understand and manage the threat to systems, people, assets, data and capabilities. At this point the organization will be weighing the level of protection that is deemed reasonable.

Tool Application 6:

Geofencing and location tracking can be utilized to help identify risk to an organization. By tracking and understanding the physical patterns of devices coming and going from an organization, a risk profile can be established. Questioning why and when it is appropriate for a work device to leave company property or personal devices to be brought in, is one concept. It could prevent lost/stolen work devices and discourage unsecured personal devices from being introduced to the network. A new, data backed, policy could be implemented based on the findings of a geofencing campaign.

NIST Current Application 6:

Logistics, or supply chain management, is using geofencing to manage the route of supplies. Olivera and associates discuss their technique in the article “An intelligent model for logistics management based on geofencing algorithms and RFID technology”. They discuss two solutions implemented and the technology used to accomplish it. "Furthermore, the model monitors detours in planned routes and deals with alarms notifications using mobile devices. To provide that features, we employed geofence concept with two solutions that enable to detect, in real-time, the occurrence of detours in planned routes. " (Oliveiera, Cardoso, Barbosa, da Costa, & Prado, 2015) The major goal of this solution is to manage one of the largest costs in supply chain, which is the transportation of goods. Provided in their article is a detailed illustration of how this system works, as seen in figure 3.3.

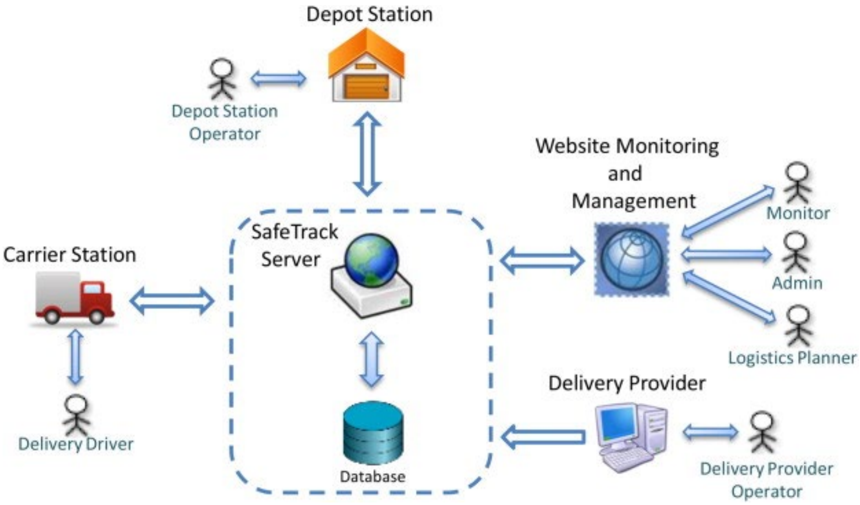


Figure 3.3: Supply Chain Solution

Geofencing is used to assist the algorithm in preforming decisions to reroute cargo when detours or slowdowns arise.

Potential Risk Example 6:

Tracking a device which can relate to a specific person can be compromised, letting an attacker who has gained access have location data on their target. Location data, which is considered a way to collect personally identifiable information(PII), discussed later with legal issues, must be protected. An attacker can use this information combined with other information to gather true PII.

Potential Benefit Example 6:

The information collected can help administrators request and allocate budget to better protect the organization. With data on how often personal devices are brought on network, regardless of policy, it may be determined that providing antivirus to employees can be less expensive than a potential compromise or lawsuit.

NIST Step 2: Protect. Once a level of risk is established, appropriate action and plans are created to protect data and infrastructure.

Tool Application 7: Many organizations have physical barriers to keep intruders out. Activities like war scanning may not keep malicious threats off your network, especially in densely populated areas. A geofence could be set to alert administrators to strange devices that have crossed into a virtual barrier. It can also alert administrators when devices that should never leave the premises have cross the barrier. Although this has not prevented the intrusion, it may alert the organization of an imminent threat, giving them a head start in the race.

NIST Current Application 7:

Drones are rapidly becoming more popular, so much so there are laws in place to regulate airspace. You can purchase a basic drone online ranging in price from 29.99 USD to +20,000.00 USD. (Amazon) Amazon is a global online shopping platform that claims it can deliver packages up to 5 pounds using drones. From the abstract of Cho and Yoons' article on assessing the capacity on urban airspace "The anticipated proliferation of small Unmanned Aerial Vehicles (sUAVs) in urban areas has garnered greater interest in capacity estimation of the low-altitude airspace. As a first step to assess such capacity, we propose a topological analysis framework to identify free versus usable airspace in a 3D environment filled with abundant geometric elements. To incorporate the underlying geospatial complexity as well as vehicle operational requirements, two types of geofence keep-out and keep-in are utilized."(Cho, J., & Yoon, Y., 2018) Geofencing is being used to manage and regulate airspace used by drones. Drones are used recreationally by sightseers and travelers, as well as professional photographers

Potential Risk Example 7:

If compromised, devices attached to drones, taking photos can be compromised for unethical reasons but can also be commandeered to protect areas. Hackers can steal visual information from these devices

Potential Benefit Example 7:

Chief Information Security Officers (CISO) can see what potential threats are looking at and even potentially shut the devices off completely.

NIST Step 3: Detect. Part of the protection plan is to be looking for and able to identify potential intrusion. As mentioned in the hacker methodology, part of the attacker's plan in to get in, unnoticed, and stay in as long as possible or disappear without a trace. Organizations must be able to identify when a breach has occurred.

Tool Application 8:

Threats can come from external, virtual means, and can often be a physical device. A raspberry Pi, a small credit card sized computer, can be placed within an organization’s walls and run on the network, invisible to those around it. In an Cyber Defense course at California State University, San Bernardino, students are taught basic steps to program a Raspberry Pi to reverse SSH into a Google Cloud instance. This device automatically connects to Wi-Fi and allows the student to connect to any device or network this Pi has accessed. (Nestler, 2019) Although geofencing is usually limited to a minimum of 10 meters, and should not be overlapped, placing specific geofences around high risk areas can monitor devices coming and going. If a threat was detected, this may give the cyber response team a data point to be able to locate and retrieve the malicious device, granted the device was powered on and connected to Wi-Fi when it crossed the barrier.

Current Application 8:

Geographical Information Systems (GIS) are being used at an ever-expanding rate, in marketing, in the classroom, for data gathering and predictive analytics. Due to the rise in GIS popularity, geofencing and its functionalities are becoming standard knowledge and practice. There are a few companies offering geofencing within their applications services to include control, information gathering and actions. In a overview of an application, CodeProof lists the following policies “1. Disable or block camera in the certain geographical area. The administrator can block the phone’s camera automatically inside company campus, as an example. With this feature un-authorized users or devices will be unable use the camera to take pictures or video, which helps prevents data leakage and theft. 2. Notify administrator via email or SMS when the device enters or exits a specified region." (CodeProof, 2014)

Potential Risk Example 8:

Any collection of data is at risk. As an administrator, the risk of this data getting into the wrong hands must we weighed with the benefits of trend analysis and the intelligence that can come from it.

Potential Benefit Example 8:

Geofencing can allow the administrator to identify patterns, comparing incongruencies and potentially detecting a threat.

NIST Step 4: Respond. Once an intrusion has been detected, whether it is active, benign, or past, the organization must have a plan to respond.

Tool Application 9:

Communication is one of the major functions included in response. Geofencing is designed to allow communication within a targeted area. If a security breach has been identified, administrators could communicate or even take action over devices within a geofence. If a system crashing phishing email has been sent out, administrators could react with a push notification too employees, literally turn off devices, or functionality. This would be especially useful if a physical attack was happening. Administrators could communicate with specifically located member of the company, without having to send out mass communication.

Current Application 9:

Geofencing is emerging as a tool offered to perform tasks, instead of just notifying administrators. As mentioned previously, geofencing has already been seen in the use of appointing barriers for drones, providing a keep-in, keep-out function in airspace. At this time, most functionalities require this to be on an application with preauthorized approval on the device, however, this can change. If a “master key” could be created to fit any application and allow administrators to take over control of devices in secured locations. Administrators could see what trespassers are seeing, shut down cameras and audio to prevent information leaks and even “push” drones out of restricted airspace. A research paper on Geofencing in a Security Strategy Model demonstrated the beginning of experiments to try and use geofencing in cybersecurity. In the experiment, the laptops were tracked to see if they stayed within a predetermined area of a building “it provides a strategy whereby field-based operatives are tracked to ensure they remain within their authorized geographical limits during their working day [12]. This research aims to use the idea of geographical limitation inherent in geofencing to develop a security solution to the risk caused by the leakage of the radio waves through a security strategy model (SSM) to control access to the wireless network within an organization's predefined geographical space." (Ijeh, A. C., Brimicombe, A. J., Preston, D. S., & Imafidon, C. O., 2009)

Potential Risk Example 9:

In a situation such as corporate espionage, a communication plan such as this, may give administration a sense of false security. This communication style could alert the adversary to their every counter move.

Potential Benefit Example 9:

When utilized correctly, this can function exactly as it was intended and as it is currently best used, as a tool to deliver information at the right time to people in an exact location.

NIST Step 5: Recover. The attack may be ongoing, or the issue discovered after the assailant has left the system. Regardless, a plan of to recover any lost capabilities that have been impaired must be in place to allow the organization to recover from the attack.

Tool Application 10:

If data is being tracked through geofencing, trend analysis can be applied to continue to improve a cybersecurity plan. By understanding what went wrong, administrators can make better decisions to ensure it does not happen again and even potential predict future attacks.

Current Application Example 10:

Of recent importance, the COVID-19 Pandemic has brought about a new race to track encounters. China began using geofencing to alert travelers if the locations they had visited became a hot zone. “The Alipay Health Code’s creators say it uses big data to draw automated conclusions about whether someone is a contagion risk.” (Mozur, Zhong, &amp; Krolik, 2020) The Chinese citizens receive codes that clear them to enter subways and other public places. According to NYTimes “the Times’s analysis found that as soon as a user grants the software access to personal data, a piece of the program labeled “reportInfoAndLocationToPolice” sends the person’s location, city name and an identifying code number to a server. The software does not make clear to users its connection to the police. But according to China’s state-run Xinhua news agency and an official police social media account, law enforcement authorities were a crucial partner in the system’s development.” (Mozur, Zhong, & Krolik, 2020) Tectonix, a computer software company, is using data visualization to share awareness. The used cellphones that were present on a public beach in Florida during spring break 2020, to track potential spread of the disease. They drew a geofence around that beach and use the location data, anonymously, to show how far one beach party can distribute infection. (Tectonix GEO, 2020)

Figure 3.4 shows Tectonix drawing a geo fence around the beach and devices to be tracked.

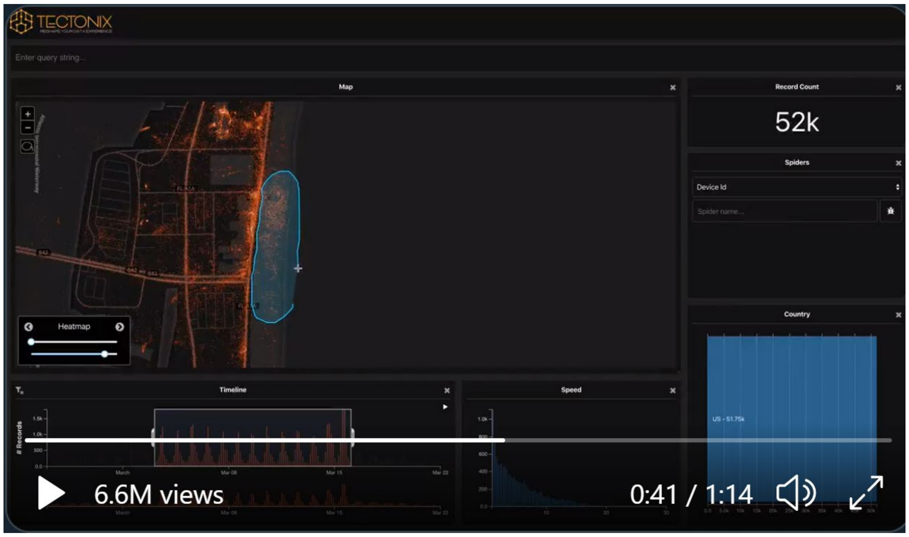


Figure 3.4 Twitter Post by Tectonix

Figure 3.5 demonstrates the use of a “spider query” where the devices that were targeted inside the geofence traveled to.

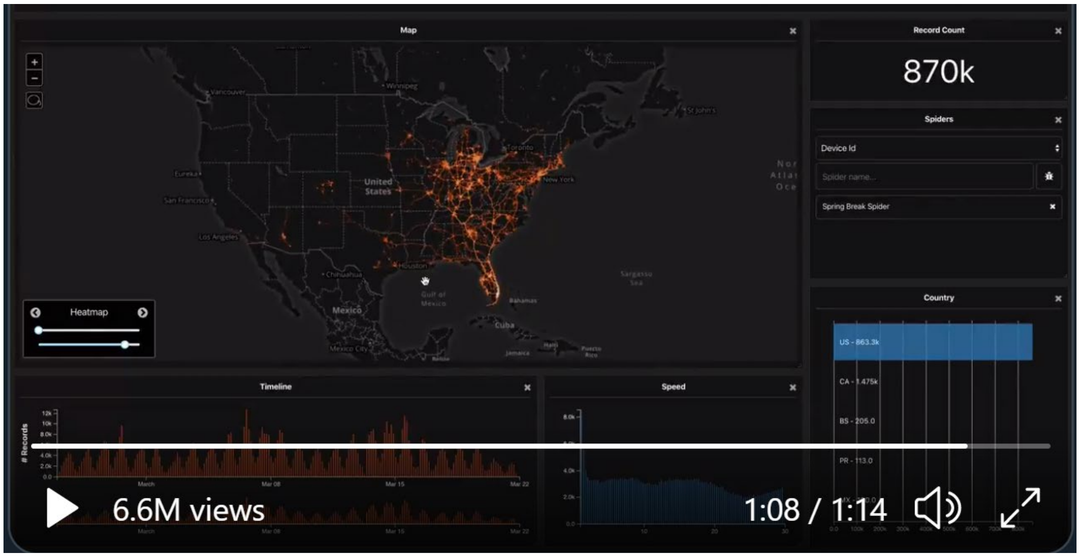


Figure 3.5: Tectonix Spider Query

Potential Risk Example 10:

The ability to fool the system or present false information would greatly impair the reliability of the system. If this approach was taken by a malicious threat in China with the COVID-19 application, an attacker could shuffle information, or even swap the data to clear infected people. This would cause a rapid spread of the disease, potentially killing thousands and inciting chaos and government distrust.

Potential Benefit Example 10:

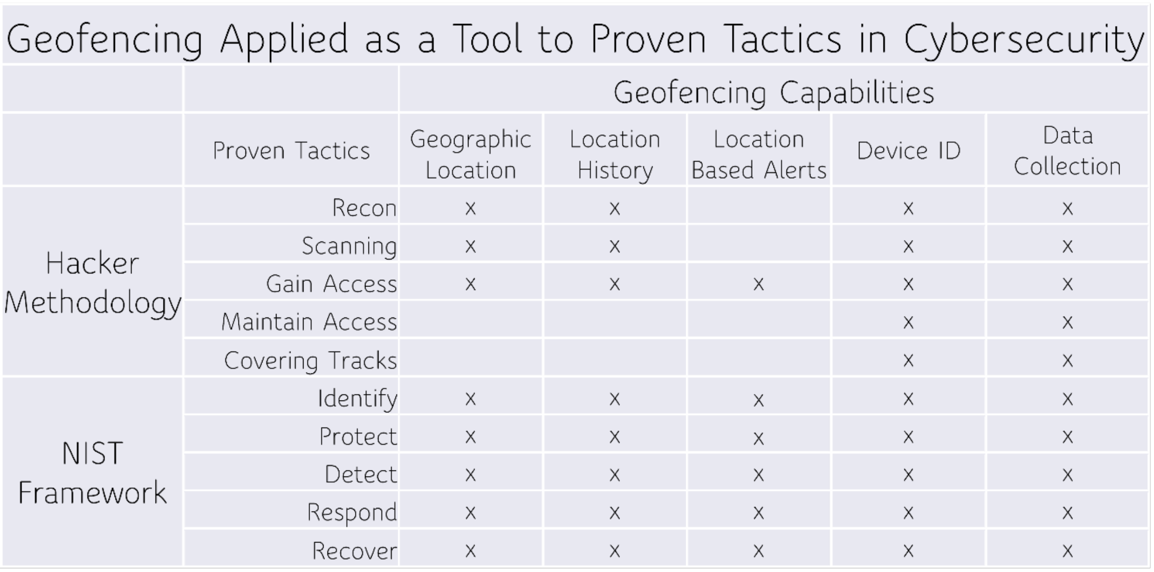
When done correctly, this data can emphasize a point and spread information to assist in compliance. In business, Change Management reduces and battles resistance from employees. By showing them statistics and data trends, administration can help foster the company's human capital collaboration.

After an attack, the organization should return and modify the plans set in the identify phase. They must continue to fortify security and ensuring all reasonable steps have been taken to ensure cybersecurity.

Geofencing Applied to Hacker Methodology and the NIST Framework

When you look at the sequence starting with the hacker's methodology, flowing into the NIST framework, they appear to be a series of events. The hacker exposes an organizations vulnerability and breaks in, then the organization responds against the attack. It makes sense that geofencing can be used as a tool for both sides as displayed in the Tool Examples 1-10. Based on these examples, a table of geofencing capabilities has been created.

Table 1: Geofencing Applied as a Tool to Proven Tactics in Cybersecurity



Geofencing Applied as a Tool to Proven Tactics in Cybersecurity

		Geofencing Capabilities				
	Proven Tactics	Geographic Location	Location History	Location Based Alerts	Device ID	Data Collection
Hacker Methodology	Recon	x	x		x	x
	Scanning	x	x		x	x
	Gain Access	x	x	x	x	x
	Maintain Access				x	x
	Covering Tracks				x	x
NIST Framework	Identify	x	x	x	x	x
	Protect	x	x	x	x	x
	Detect	x	x	x	x	x
	Respond	x	x	x	x	x
	Recover	x	x	x	x	x

CHAPTER FOUR

LAWS AND REGULATIONS ASSOCIATED WITH GEOFENCING

The is no standardized global law for cybersecurity and privacy. The European Union (EU) has stricter encompassing privacy policies than those in the United States (US). According to IT Governance, "unlike the European Union, the US has no single federal law that regulates information security, cybersecurity, and privacy throughout the country. Several states have their own cybersecurity laws in addition to data breach notification laws. These areas are currently regulated by a patchwork of industry-specific federal laws and state legislation, with varying scope and jurisdiction.

The challenge for organizations that conduct business across all 50 states and potentially across the world is considerable."(ITGovernance) Laws and regulations must be considered when deciding how to incorporate a tool such as geofencing into a cybersecurity plan. Although there are many more laws that are applicable to privacy that may be threatened by geofencing, the following can be used as a sample of the legal precautions that must be considered. Penalties for breaching any of these laws range from a percentage of annual income to millions of dollars. A legal implication such as this can bankrupt a corporation and must be considered in the risk framework. As hackers do not abide by the law, the only legal prevention that can be applied is more severe policies on the platforms that facilitate geofencing. Since the laws do not reference geofencing specifically, examples will be provided that reference privacy and personally identifiable information (PII), which are regulated and are the major vulnerability with geofencing.

Privacy and Personally Identifiable Information

The potential control geofencing offers is unprecedented and threatens privacy rights. However, knowing unethical and malicious threats will not consider privacy as a barrier in their efforts to obtain a target, administrators must take steps to utilize this tool to fight back. In this next chapter, known vulnerabilities and threats will be explored, including privacy and the threat associated with legal implications.

Privacy, or the impression of privacy is important to most everyone. This is a major legal consideration from high risk top-secret facilities to at risk populations who require monitoring for their protection, like those with Alzheimer's. The benefits of geofencing as a tool must be balanced with ensuring only relevant data is being collected and stored, that data is being protected and that those whom the data is being collect on are aware and have accepted to the terms of your tracking.

Services that are trying to use geofencing as a tool to help protect people in at risk populations have already faced this hurdle with Alzheimer's patients. As legal adults, unlike children who are managed legally by their parents, these patients have privacy rights, like anyone else, which has made applying this technique difficult. "Systems for geotracking Alzheimer's Disease patients with dementia are reported to raise ethical issues and concerns. Studies stated possible loss of freedom and autonomy for patients, along with violations of their privacy, which may lead to loss of prestige/dignity."(Yüce, Gülkesen, Barcın, 2012) Tracking children, another function geofencing has been seen in, must also satisfy privacy and data protection laws like COPPA.

Although laws and regulations are currently in place to protect privacy and data collection, storage and protection, there are gaps in regulations that geofencing does not seem to fall under. Although geographic indicators falls under a sub category of personal identifiable information (PII) according to NIST, geofencing seems to be overlooked as a geographical indicator “information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).” (Macallister, Grance, & Scarfone) Since client opt into this service, they waive their privacy rights for the convenience of targeted marketing. So, although you may not be able to store someone’s address, tracking them in their daily routine would easily allow for this information to be assumed. Geofencing fall into this category and therefore, should be regulated as such. Figure 4.1 illustrates the type of information that is considered PII.

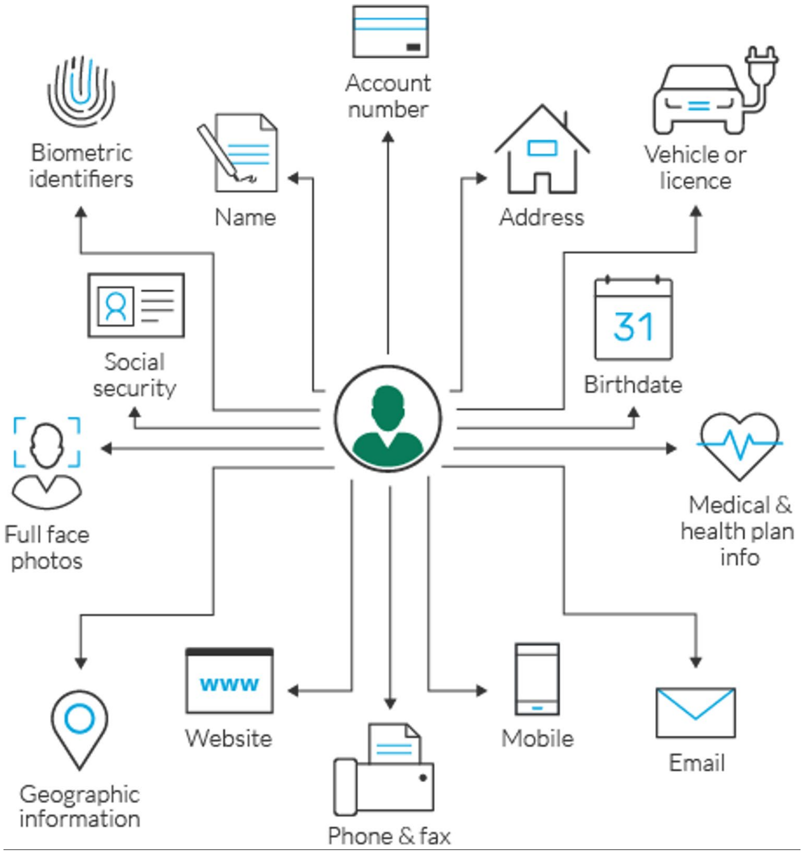


Figure 4.1: Personally Identifiable Information

Laws and Regulations

The following is a sampling of laws that apply to geofencing as it is considered for privacy, data collection, and geographic location. They will be evaluated for sufficient coverage to protect against malicious threats. Consideration will also be given to legal hurdles administrators must consider with the laws and regulations that are in place. A table of coverage as compared with geofencing capabilities can be seen in Table 2. Geofencing Capabilities vs. Current Laws.

Legal Example 1: SEC Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information, 17 CFR Part 248, Subpart A.

- Organizations must adopt written policies to safeguard customer records and protect against unauthorized access.
- SEC Regulations should already be in place; however, special consideration will need to be made if people's daily whereabouts or habits are being collected.
- If you implement this on employees or customers, you must ensure their data is safeguarded. In the field of data mining, a competitor's company may pay a large sum to have the information on the customer of their competitor. This information could help them become more appealing to that customer and change their campaigns to target that clientele directly.
- Anonymous use of geofencing, can be useful, but does not provide specific target data. If an administrator's goal is security, there must be an ability to trace a specific device back to a specific person. Gaining the users permission, by mandate, or by corporate policy, can alleviate the potential of legal implications. Much like RFID badges, retina scanners, and other styles of access control, adding a geofencing policy to devices can be made mandatory within a corporation's boundaries.

Legal Example 2: FTC: Federal Trade Commission Act §5, 15 U.S. Code § 45.

- A regulation on information security as well as a privacy law. It encompasses the need for organizations to have reasonable and necessary security practices.
- The FTC could be a barrier if geofencing is seen as an unreasonable security threat. The organization must take into consideration how they will not only ensure the data that is being collected is secure, but that collecting the data is making the organization safer.

Legal Example 3: DFAR: Defense Federal Acquisition Regulation.

- This regulation applied to contractors and subcontractors of the Department of Defense (DoD) and mandates they "provide adequate security to safeguard the covered defense information on unclassified information systems."
- This law mandates the contractors and subcontractors maintain compliance with the National Institute of Standards and Technology (NIST), something not common among other cybersecurity laws.
- Although "adequate" and "reasonable" are used often in these privacy laws, administrators must take into consideration the potential repercussions of the possibility of the data they are collecting, getting leaked or stolen.
- If the DoD or its contractors began geofencing everything and collecting the data of people and products coming and going, an

attacker could steal that information and use it to infiltrate. However, as mentioned previously, malicious threats will most likely already be using these tactics to their advantage. A geofence can be applied by anyone over any geographical location without the knowledge of those inside that digital barrier.

Legal Example 4: COPPA: Children’s Online Privacy Protection Act, 15 U.S. Code Chapter 91, 16 CFR Part 312.

- This law regulates how online platforms that provide services, holds information, or is used by children under 13, can “collect, use, and/or disclose personal information from and about children.”
- This law can be directly applied to tracking children. With the known vulnerability stated previously, this law can be considerably difficult to comply with. Ensuring an application cannot be altered or hacked is difficult to do but must be done with a reasonable amount of surety to protect the organization using or controlling the platform.
- If a school were to implement this tactic to try and create a safer environment for their students, they would need to first consider the cyberthreat.

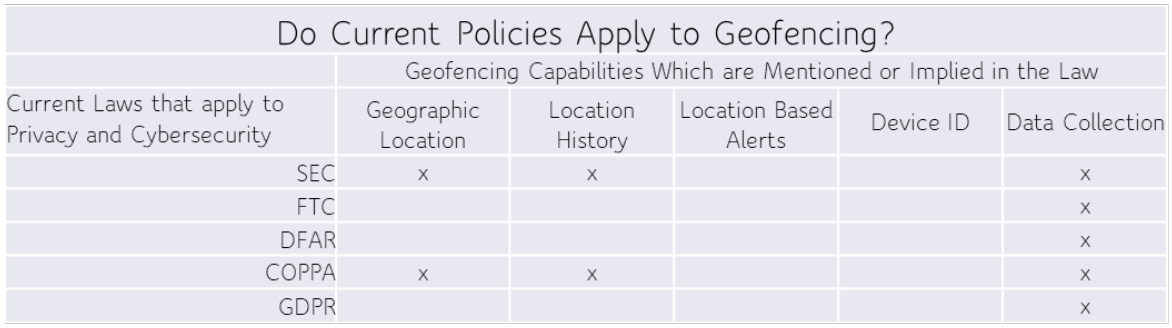
Legal Example 5: General Data Protection Regulation (GDPR).

- This is a law passed in the European Union (EU) but it applies to all organizations who collect data on citizens of the EU. It controls personal data, data processing, data subjects, data controllers and data processers. (What is GDPR, 2019)

- This law may be the strictest data privacy law implemented to date, competing with California, and has penalties up to 20 million euros or 4% of global revenue.
- This is the first regulation that holds all aspects of the data lifeline in check. This, or something like it, will be the first step towards regulating geofencing.
- This regulation would require the legitimate data collectors to be more vigilant in their efforts to protect the data collected.

When comparing what these legal examples regulate and what geofencing has been proven to do, there is an obvious lack of regulation and a need for attention.

Table 2: Geofencing Capabilities vs. Current Laws



Do Current Policies Apply to Geofencing?					
	Geofencing Capabilities Which are Mentioned or Implied in the Law				
Current Laws that apply to Privacy and Cybersecurity	Geographic Location	Location History	Location Based Alerts	Device ID	Data Collection
SEC	x	x			x
FTC					x
DFAR					x
COPPA	x	x			x
GDPR					x

CHAPTER FIVE

FINDINGS AND FUTURE APPLICATIONS

Geofencing as a tool has been explored as a potential threat and a potential tool in the field of cybersecurity. With a world full of data, where almost everything is tracked and stored in a database and “big data” is everywhere, more methods are needed to secure and understand the information being collected. Current methods using AI and collecting massive data is no longer producing the desired effects in the desired amount of time. Applying geographically specific barriers for data is one way to solve this problem and add another line of defense to securing digital information.

This project posed the following questions:

1. Is geofencing an unknown threat in the field of cybersecurity?
2. Can it be used as a tool in a risk management plan?
3. Is the data collected using geofencing considered PII and if so, how is it being protected?
4. Are there laws and regulations already developed to guide application developers and users of geofencing? If not, is there a need for new laws and regulations be developed?

Result 1: Geofencing is an Unknown Threat in the Field of Cybersecurity. Special attention must be provided to what information is being collected, how it is intended to be used and how that information can remain safe. Administrators should immediately begin considering potential threats posed by geofencing. Training and ensuring cybersecurity teams understand the threat and have tools to defend against it. Research should begin on how best to secure code to prevent manipulation within the platforms. Finally, policies should be considered on how to prevent against malicious threats gathering data by geofencing another's physical location.

Result 2: Geofencing is a Tool that can be used in Risk Management. Just as geofencing has been demonstrated as a tool to be used for malicious intent, it has been shown as a tool for defense. Utilizing it as a tool for data and asset tracking can assist in decision making. In addition, using is as a tool for early intrusion detection, forensics and emergency communication can help an organization respond to threats more efficiently.

Result 3: Geofencing is Personally Identifiable Information. Geofencing provides data and trends that can show a person's geographical location throughout the day. This should easily fall into the category of PII and is therefore protected under many privacy laws. Any platform that is using geofencing should take additional measures to ensure the data is kept safe and that only relevant data is being collected.

Result 4: Laws and Policies Must Adapt. There are laws and policies in place that address some aspects of geofencing. However, the high demand for targeted marketing circumvents these policies through consumer consent. Geofencing platforms must become more selective with what data their customers can collect, where geofences can be placed and the security that should be placed on that data.

There is much that is unknown regarding vulnerabilities associated with geofencing, and there has not been a significant amount of research surrounding the subject. Unknown vulnerabilities must be considered, and research pursued. Suggestions for future research in geofencing capabilities can be found in Appendix A.

APPENDIX A

SUGGESTED FURTHER RESEARCH TOPICS

Based on the information shared in this paper, administration and customers should place GIS and geotargeting at the forefront of research and development. GIS Platforms should regulate who can use this technology, how much data can be obtained, and appropriate protection of data collected. In addition, there should be regulations on where a geofence can be placed, and attention given to regulating high risk areas like schools and government buildings. Below are suggestions for further research directions.

Intelligence Gathering using Geo-fencing

Currently, tactics are being used to capture data on a wide scale. This data can be scrubbed and consistently monitored for key words and insights. However, due to the large amount of data available, also known as "big data", artificial intelligence (AI) can only determine so much. “Getting high quality insights from data analysis is a task that hasn’t yet been mastered by automated tools and machine learning. Partly because algorithms lack human understanding and cannot detect subtleties like sarcasm (which social media is chock full of), but also because what may be a valuable insight for a sports team, will likely be useless to a financial institution. Each set of insights needs to be catered very specifically to each use case. For true insight to be delivered, there has to be a human element."(Echosec) As mentioned, in the article by Echosec, we have to determine a better way to allow machine learning and AI to gather insights. I propose geofencing can be used to gather intelligence in a more targeted fashion, thus allowing algorithms to work more efficiently.

A specific example of this theory is with the use of social media monitoring at high risk events. Echosec talks about this phenomenon within marketing, as we have referenced in this paper most geofencing and geo targeting is being used for. They state "there are limits to what social media monitoring tools can do. The people using these tools still need to add their own human interpretation to truly understand a situation. It is the job of social media monitoring platforms to help them find what they’re looking for faster, to make this job as easy as possible.”(Echosec) It is in my experience that I see people will post on social media, essentially a trusted group of people, about things that concern them. Where they will not come outright and tell an authority figure or report it to law enforcement. Using geofencing and in turn geotargeting, administrators can monitor and interact with customers for safety protocols. Many social media users use slang or shortened text to express themselves. An extensive dictionary of potential "buzz words" and their common grouping could assist with machine learning. If the monitored situation, i.e.. concert, festival, party, college campus algorithm, can be trained to target key words within a geofenced area, an alert can be sent to the administrator that there may be an issue. This would allow the suspicious activity to be flagged and appropriate personnel alerted to a potential threat. Pairing the algorithm with attendee’s general population statistics and event genre, paired with tightening the location the data is being pulled from, should assist the AI.

Gathering intelligence in this manner can open threats to the security of information. In an interview with a Private Investigator, that requested they not be named, the question was posed, “how can we gather information on a target in a specific location?” They asked with the intention of gathering posts from open social media accounts, namely incriminating photos, to prove insurance fraud. This tactic can be applied to any corporation that does not have a policy on device or application usage within the physical perimeter. If an application was compromised, or had geo location pre built in to the permissions, a malicious threat could strike. They could gather photos from social media posts, activate cameras to view internal structures, and much more. What makes this so dangerous, is this can be running with little to no signs to the cell phone device/application users. The repercussions of not building policies and measures to prevent this type of intrusion are unmeasurable, spanning from liability and insurance claims to compromising corporate intellectual property.

Geo-fencing as an Enforcement Tool

The ability for an administrator to have ultimate power over certain capabilities in a device within a targeted geographical area is a control that should be developed further. CodeProof explains what can be done with the use of an application with geofencing. "We’ve introduced the anticipated location based mobile policies also known as Geofencing. With this feature an administrator can define multiple geographical regions within the CodeProof console and apply the mobile policies to devices in those regions. When the device is identified within the defined region boundary the regional restricted policies defined by the administrator get enforced automatically. Similarly, when the device goes out of the region the policy reverts back automatically." (CodeProof, 2014) This is one example of companies that are already beginning to implement geofencing for administrative controls.

Weapons than can be controlled or better secured using technology is an advancement that we are likely to see in the near future. As technology advances and gun safety protocols continue to come into question, I believe it is logical that technology including GIS and geofencing become immersed in the topic. One topic to be research further is using geofencing to lock down areas or equipment. With built in applications, weapons may be able to be deactivated or rendered useless if taken outside of an area, or brought into a designated area such as airports, schools, hospitals, etc. If a mechanism could be engineered to lock and unlock in a specified geographical area, or within proximity to a specified person, it could be used in this fashion. Locking doors, cases, etc could follow this same concept. If information is being transported, for example physical information bearing devices, they could be secured inside a locked case that is programed to only be able to unlock inside of a specified geographical area. This concept can be manipulated to keep information and any number of items out of the hands of malicious threats.

For the purposes of securing sensitive or copywritten content, geofencing can be utilized as a tool. Many issues with content leaks come from people using their personal devices to capture content when they have been explicitly told not to. In extreme cases, applications can be made mandatory on all devices that allows administrators to disable cameras and audio upon entering a geofenced area. This can ease the burden of asking people to turn in devices and holding them in a secured location. This lowers the personnel burden of checking in and checking out devices as well as the risk to losing or damaging property. This can also give users the freedom of access to their devices without compromising intelligence security.

Currently, employees working inside many maximum security/clearance locations must turn in devices upon entering, sometimes being provided with a location issued device. This poses the same issue as mentioned before regarding personnel burden and risk of damaging property. If guests or employees could opt into an application that gives full administrative governance inside the specified area, this could elevate data safety. This could be a passive application that simply renders all devices usable to the extent of placing and receiving emergency phone calls, to active monitoring of what is happening on those devices including captured content, ingoing and outgoing messages as well as device location within the premises. Schools can use this as a tool to control student cellphone usage while in class, to prevent cheating as well as to track malicious activity.

REFERENCES

Adams, K. (2019, October 17) Personal Interview with Diedre Lane.

Alsaquer, M., Hilton, B., Horan, T., & Aboulola, O. (2015). Performance Assessment of Geo-triggering in Small Geo-fences: Accuracy, Reliability, and Battery Drain in Different Tracking Profiles and Trigger Directions. Retrieved January 15, 2020, from https://www-sciencedirect-com.libproxy.lib.csusb.edu/science/article/pii/S1877705815010437

Bob, Nik, Randy, & Daniel. (2019, June 20). What is Geofencing? A Guide to Virtual Barriers. Retrieved October 13, 2019, from https://gisgeography.com/geofence-geofencing/.

Cho, J., & Yoon, Y. (2018, May 8). How to assess the capacity of urban airspace: A topological approach using keep-in and keep-out geofence. Retrieved January 15, 2020, from https://www.sciencedirect.com/science/article/pii/S0968090X18305850

CodeProof. (2014, January 27). Location based mobile policies – Geofencing. Retrieved January 5, 2020, from https://www.codeproof.com/blog/location-based-mobile-policies-geofencing/

Echosec. (n.d.). Social Media Monitoring. Retrieved January 5, 2020, from https://www.echosec.net/social-media-monitoring

ESRI. (n.d.). GIS Dictionary. Retrieved April 17, 2020, from https://support.esri.com/en/other-resources/gis-dictionary/term/8abe5222-da9f-4298-9f29-61b9bc6381d2

Ijeh, A. C., Brimicombe, A. J., Preston, D. S., & Imafidon, C. O. (2009, September 1). Geofencing in a Security Strategy Model. Retrieved September 25, 2019, from https://link.springer.com/chapter/10.1007/978-3-642-04062-7_11

Imperva. (n.d.). What is Personally Identifiable Information: PII Data Security: Imperva. Retrieved from https://www.imperva.com/learn/data-security/personally-identifiable-information-pii/

INTUZ. (2018, May 29). Geofencing Apps: A newfangled competitive business strategy - Intuz Blog. Retrieved September 25, 2019, from https://blog.intuz.com/geofencing-apps-a-newfangled-competitive-business-strategy/

ITGovernance. (n.d.). Federal Cybersecurity and Data Privacy Laws Directory. Retrieved April 26, 2020, from https://www.itgovernanceusa.com/federal-cybersecurity-and-privacy-laws

Lexico. (n.d.). Cybersecurity: Definition of Cybersecurity by Lexico. Retrieved April 21, 2020, from https://www.lexico.com/en/definition/cybersecurity

Mozur, P., Zhong, R., & Krolik, A. (2020, March 02). In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags. NYTimes. Retrieved April 26, 2020, from https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

NCCGroup. (2014, March 7). Vulnerabilities found in geofencing apps. Retrieved

October 13, 2019, from https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2014/march/vulnerabilities-found-in-geofencing-apps/

Nestler, V. (2019, September 25).. *IST 511 Ethical Hacking*. Lecture. CSU, San Bernardino

NIST. (2019, November 18). Framework Documents. NIST. Retrieved from https://www.nist.gov/cyberframework/framework

NIST. (n.d.). COMPUTER SECURITY RESOURCE CENTER. NIST. Retrieved May 12, 2020, from https://csrc.nist.gov/glossary/term/cybersecurity

Oliveiera, R. R., Cardoso, I. M. G., Barbosa, J. L. V., da Costa, C. A., & Prado, M. P. (2015). An intelligent model for logistics management based on geofencing algorithms and RFID technology. Retrieved January 13, 2020, from https://www-sciencedirect-com.libproxy.lib.csusb.edu/science/article/pii/S0957417415002316

Pulsate. (2016, May 23). 7 Things About Geofencing You'll Kick Yourself For Not Knowing. Retrieved April 17, 2020, from https://www.slideshare.net/pulsatehq/7-things-about-geofencing-youll-kick-yourself-for-not-knowing-f-62310847

SaveTheElephants. (n.d.). Creating Conservation Stewards For A Modern Kenya. Retrieved April 17, 2020, from https://www.savetheelephants.org/project/geo-fencing/

Tectonix. A Better Way to Bring Big Data to Life. Retrieved April 17, 2020, from https://www.tectonix.com/how-it-works.html

Tectonix GEO. (2020, March 24). Tectonix GEO (@TectonixGEO). Retrieved April 21, 2020, from https://twitter.com/tectonixgeo?lang=en

What is GDPR, the EU's new data protection law? (2019, February 13). Retrieved from https://gdpr.eu/what-is-gdpr/

Yüce, Y. K., Gülkesen, H., & Barcın, E. N. (2012). Geotracking Patients with Alzheimer's Using a Personalized Geotracking System with Social Support Network. Retrieved January 15, 2020, from https://www-sciencedirect-com.libproxy.lib.csusb.edu/science/article/pii/S1877050912005078