A Survey of Wireless Security Concerns and Case Studies in Geolocation Data

Julie Brozovich[1], Aby Tino Thomas[1], Martin Bonugli[1], Luke Thurmond[1]
Vahid Emamian[2], Senior IEEE Member
[1]Computer Science Department
[2]Electrical Engineering Department
St. Mary's University, San Antonio, TX
jbrozovich@mail.stmarytx.edu

Abstract

In the past few decades, there was a revolution in information technology and its real-world implementations, which improved the overall lifestyle of every user and business. One of the key innovations in information technology and telecommunications is wireless devices, their secure communication, and location-specific functionalities. Early implementation was frequently used for commercial and military communications [1], but as the internet became an inseparable part of modern living, the popularity of wireless devices with internet capabilities has grown exponentially. To support this growing use of wireless devices across the world, wireless hotspots and mesh networks have been deployed. This resulted in location-related privacy concerns for normal users. In the modern world, location data is collected from wireless devices every second of every day which causes significant and on-going security concerns. Anyone who has access to this data can interpret information about the user. Collecting and processing this kind of information is not always legal and not always agreed to by the individual. In this paper, we discuss the different aspects of location-related privacy concerns and the real-world capitalization of location data. We also discuss methods to identify the location of a wireless device, how to map an IP to a location and practical countermeasures to secure wireless users.

Categories and Subject Descriptors: Wireless security and protection
General Terms: Security, location privacy
Keywords: Location, privacy, anonymity, wireless networks, ad hoc network routing, security

1. Introduction

When President Barack Obama openly discussed the National Security Administration's (NSA) use of a clandestine electronic data surveillance program that collects personal information from various electronic devices and cellular telephones, many citizens became aware of the powerful surveillance tool they carry in their pocket. The use of cell phone data, particularly geolocation data that can track a user's every move, had people across the country outraged at the government's ability to monitor without consent. This unauthorized tracking of an individual is a clear violation of privacy because geolocation data of an individual is protected by the Fourth Amendment.

Since that day in 2013, the use of location tracking services by the government and corporations alike has increased significantly while the everyday users' concern for privacy has seemingly

decreased. Generally speaking, cell phone users can be broken into two main categories: those who do not understand the extent to which their location privacy is collected, sold or used, and those who have come to accept a certain aspect of privacy loss in order to obtain the convenience that location-based services provide to a daily cell phone user. However, consumer's privacy concerns are not always consistent. Cell phone users are quick to install applications without reading the user agreements or terms and services which can lead to their location data unknowingly being sold to both the government and marketing firms.

Corporations have adapted to this change by using readily available tools to capitalize on the newly available information. Government agencies and local law enforcement have also implemented the use of location data for prevention of drug smuggling, human trafficking, and the creation of cases against child predators. Despite the analysis of geolocation data having a positive impact on the community through law enforcement there is still a growing number of challenges to privacy and security. Users with an understanding of data collection practices are able to implement mitigation strategies to prevent and reduce the probability of encountering these issues.

2. Background

Wireless communications started in 20th century and made its footprint in almost every line of business in a very short period of time. The primary reason for this global acceptance of wireless communications is its convenience and lack of connected physical medium. As information technology has grown exponentially in the last few decades, wireless technology also evolved from single networks into multimode/multistranded networks. The new innovations in information technology empowered wireless device manufactures to invent more creative wireless devices with many real-world functionalities. A modern smart phone is not just a device to facilitate telephonic communication, rather, it combines the functionalities of many devices such as camera, radio, portable music player, e-book reader, calculator, voice recorder, GPS, compass, scanner, alarm clock, timer, video player, internet browser, video chat and many more. Due to this influx of functionalities, a mobile device uses multiple protocols to enable these applications to work and communicate with their backend systems.

For an efficient handheld wireless device to function properly, it needs to be connected to the internet. This connectivity enables the modern applications within these devices to communicate with their online repository and backend infrastructure to deliver unique and real-time functionalities to the end user. This change increased the number of available wireless hotspots and mesh networks to support these devices anywhere and anytime. Together with improved productivity and greater convenience, these technologies bring with them the rising threat of privacy violations: when a user uses a fixed address, that user can be tracked through the network. Many modern applications gain access to the physical location of the wireless device to enable some of their unique functionalities, which in-turn cause a lot of privacy concerns for the end user. The majority of wireless devices are owned by a user with tracking characteristics and the location data of that wireless device can provide detailed whereabouts of that unique individual [2].

2.1. Sources of location data

The location of a wireless device can be collected in multiple ways, such as by using Global Positioning System (GPS), cell towers, Wi-Fi networks, Bluetooth beacons, Internet of Things (IoT) devices, etc [5]. Modern wireless device operating systems detect the location via satellite GPS. The accuracy of GPS signals varies widely depending on the location. Cell towers are used to communicate between the wireless device and service provider. Because the service provider controls this connection, mobile carriers can easily locate the approximate location of a user at any time. A mobile device can also identify its location by scanning the Wi-Fi network or access points. There are public and private databases available to find the physical location of Wi-Fi networks and their respective location information. Modern apps are designed to detect Bluetooth beacons in proximity to infer the device's location or send proximity-based alerts or any other contents. The latest smartphones combine signals detected from the above-mentioned different sources to create a very precise location that is very accurate compared to the data that comes from one source. The latest operating systems does have the capability of the signals coming from different sensors assembles inside a smartphone, such as altimeter, accelerometer, GPS, etc. to provide this consolidated location services to the modern apps for their operations.

2.2. IP address to a geo location

An IP address (an identifier that is freely and openly shared by devices to send and receive Internet traffic) is often sufficient to know a person's city and state. A recent work by Y. Wang [1] introduced a technique to geolocate an IP address with a median error distance of 690 meters. There are two factors that makes this exploration difficult: wireless networks often use encryption for data transfer and Network Address Translation (NAT) feature of the new routers usually prevent unsolicited packets in reaching the wireless devices. To identify the exact location physically of an IP address, first we need to remotely identify the targets geophysical location and then dispatch a mobile observer with the correct tools to traverse the search space and monitor the wireless signals.

2.3. Access to location data

Location data is held by a lot of commercial entities that provide different services to the end user. Mobile phone carrier knows the approximate phone location because they direct the calls to the specific phone through the local towers which will have a Global Positioning System (GPS) location data associated with it. Operating systems like iOS or Android may know the location of their devices to provide an improved functionality to their users. Third party apps installed on the wireless device will gain access to location data shared from the device to provide precise functionalities like local weather or ads. Location Analytics Provides (Internet of Things) can gather user identifying information from a wireless device without having active connection to the device [5]. Some of the protocols will allow some basic communication with wireless device and track the unique characteristics of a user in specific location. A case study below will specifically talk about how these IoT (Internet of Things) devices will try to track a user location data for their benefit.

2.4. Privacy aspects

Precise location data, or "mobility data," involves information about how devices and people move through spaces over time. When individuals are moving in public and private spaces, they are not expected to be tracked wherever they go. But this is not the case when individuals use cell phones or other electronic devices that collect and store location data throughout the day. With this data, anyone can track individual's every moment of the day and infer private information like where they work, where they sleep, where they pray, which doctor office they visit and lot more. Let's understand more about privacy in the next section.

3. Critical Aspects of Wireless Communication Affecting Privacy

The primary issue with wireless device geolocation is the lack of understanding or awareness of what can be done with location history. The fact that phone records are being stored online permanently seems to be forgotten and overlooked by most people. A popular example of this is the iPhone service called "Find my iPhone" [32]. It allows users to access their phone remotely and see the history of where it has been. Consider how many years of location data a feature like this would need. The intrusion of privacy can occur when a user agrees to this service though forgets about it several years later. Another feature of iPhone is the "Find my Friends" service which provides locational data between users [32]. It is commonly assumed that access to these locations is limited to a specific group of friends. The option to turn off an application like this and remove all records from that service are not always available and must be carefully considered prior to using any application that will access locational data.

Another challenge with privacy is the way third party applications and software exchange locational data along with other personal information, which is not always apparent or known to the user. A noteworthy example of this is digital advertisements, which is currently a $151 billion dollar industry that continues to grow [5].

It is not uncommon now to encounter instances where law enforcement officials have been able to link phone records to the timing of events such as burglaries or other crimes, which are then used to determine the identity of multiple suspects. The court decision in many of these cases is that your phone records are essentially public information and, therefore can make the difference between the needed or required evidence for a conviction. Examples will be provided in the following section.

Machine learning is growing considerably and has resulted in situations where people's privacy is violated in ways that had not been anticipated. It is now being offered as a service by Microsoft, Amazon, and IBM and will likely continue to grow significantly within the next several years. The process of machine learning is to conduct automated analysis over large data. A learning algorithm is used in the training phase to analyze parameters and associate them with values that are from the input or sample. The learning phase is designed to identify the characteristics of what can be extracted from the information. These results are checked to ensure that the large data set is indicating relevant conclusions. The algorithm is then used to model and test functional data sets to make determinations and predictions about the input [4]. These algorithms can be supervised or unsupervised meaning, that in some cases, the conclusions that are being generated are not

expected or intended. While machine learning is technical and currently requires significant resources to process large data sets, it is advancing and becoming more accessible with potential to have enormous impacts to both security and privacy.

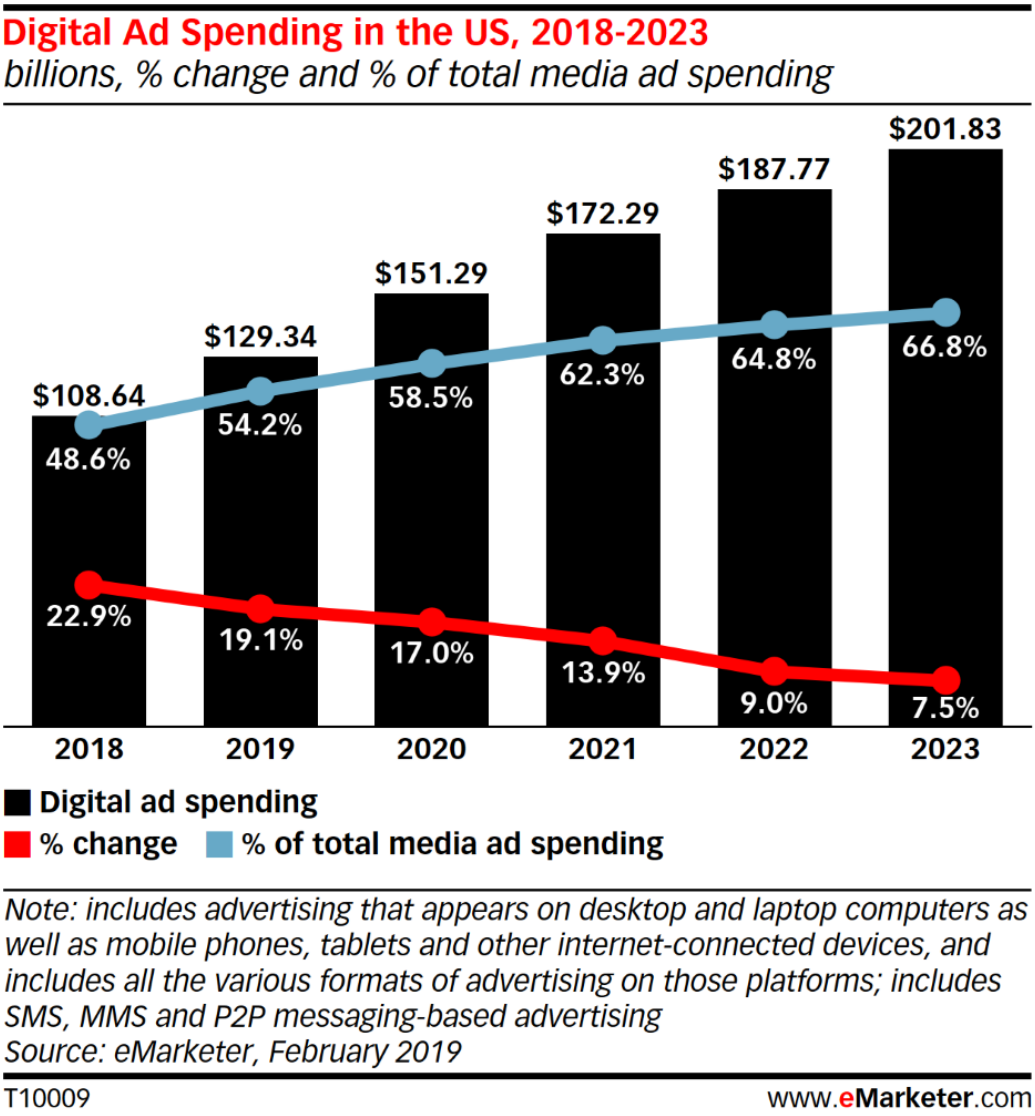

FIGURE 1. US Digital Ad Spending: eMarketer's Forecast for 2019 [5].

The Federal Communications Commission (FCC) is working to put into practice the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act created in 2019. "In 2019, U.S. consumers received 58.5 billion robocalls, an increase of 22% from the 47.8 billion received in 2018, according to the YouMail Robocall Index" [5]. The TRACED Act allows phone service providers the ability to block international phone calls and text messages [5]. Although the effectiveness of this act is currently not fully realized, it is possible that machine learning will eventually become an effective method of preventing these calls.

4. Real world Case Studies

The analysis of wireless geolocation data can provide vital information to corporations, local law enforcement and the U.S. Government. The following section demonstrates the practical implementations of how this data can be used in the prevention of narcotics trafficking, contact tracing of Covid-19 and human movement patterning.

4.1. Case 1: Government Use of Cellular Location Data Purchased from Third-Party Companies

On August 13, 2018, the San Luis, Arizona police department stopped a Yuma county resident for what seemed to be a routine traffic stop. Upon inspection of the vehicle it was discovered that 168 Kg of narcotics were hidden within toolboxes being pulled on a trailer. Further searches of the resident's home and property lead to the discovery of a cross-border tunnel between a former Kentucky Fried Chicken restaurant and a residence in Mexico belonging to the Sinaloa Cartel [10]. According to a February 2020 article in the Wall Street Journal, people with knowledge of the operation admitted it was cellphone tracking data that led to the discovery of the tunnel [11].

Although the Supreme Court ruling of Carpenter v. United States stated that law enforcement must have a warrant to obtain historical cell phone data, the US. Department of Homeland Security (DHS) has managed to find a workaround. Beginning with a purchase for $99,950[12] on September 29, 2017 and as recent as August 05, 2020 with a cost of $475,944 [13], the U.S. Customs and Border Protection Agency (CBP) has been buying cell phone location data from a third-party supplier to track possible undocumented immigrants and others who may be entering the United States unlawfully. Venntel [14], the company that is providing this data markets itself as “Innovative big data analytics for the world’s problems.” Although Venntel does not directly collect the information, it does offer a portal that contains millions of user location data they have purchased from private marketing companies that would typically sell to advertisers. When a user installs an application on their device, such as weather forecasting, social media, or mapping, it is understood that their location may be used to provide specific data, however, users may not know that data is being sold and analyzed as part of a $21 billion dollar industry. According to Alan Butler, General Counsel at the Electronic Privacy Information Center (EPIC), “This is a classic situation where creeping commercial surveillance in the private sector is now bleeding directly over into government. [15]” Although obtaining locational data directly from a cell phone provider would require a warrant, purchasing from a vendor is currently gray area legal. In June 2020, the House Committee on Oversight and Reform opened an investigation [15] into Venntel’s sale of location data to U.S. Immigration and Customs Enforcement (ICE) and CBP, stating that a vast majority of Americans carry cell phones with apps capable of collecting precise location information which raises a serious privacy and security concern. Data collected and provided by each company is stripped of all personal information and provided an anonymous alphanumeric advertising identifier that is unique to each mobile device, however, as shown by the New York Times [16], this can still be used to make personal identifications based on simple correlation of movement. CBP has been noted as using this purchased location data to analyze remote stretches of desert and narrow down border crossing locations such as the previously mentioned underground tunnel, while ICE has used it to identify immigrants who were later arrested.

4.2. Case 2: Beacon Technology in Public Places

Use*:* The implementation of beacon technology has allowed for major retailers to tracker user devices and create profiles based on customer interaction throughout the store. This has allowed for marketing experts to configure product placement and store layouts to increase sales. Additionally, location data collected through third party applications such as a weather tracker can be purchased by marketing firms and sold to retailers. With this information, corporations such as Target [17] can know when, how long, and how often you shopped at Walmart [18].

Beacons also serve a helpful purpose outside of retail tracking and marketing; this technology is currently in airports to transmit real-time gate information to passengers, museums use beacons to guide guests as they approach exhibits, and it allows the for companies such as PayPal to notify you if contactless payment systems are available at your current location. Beacon Technology is continuously growing and according to a report from Proximity Directory, 75% of the top 20 US retailers have implemented beacon technology and it is forecasted that Bluetooth LE (Low Energy) beacons are on track to break 500 million installed units by 2021 [17].

Technology*:* Beacons are small devices, strategically placed throughout stores, that transmit a continuous signal to any mobile device in range. The technology is built on the Bluetooth Low Energy (BLE) stack, which enables short-burst wireless connections and uses a broadcast topology to simultaneously communicate with multiple devices [17].

Unlike GPS, Bluetooth beacons are incredible accurate and can determine your location down to a few centimeters and are particularly efficient indoors. The tracking of specific devices is not done through any personal information or the devices media access control (MAC) address, but rather, through an Advertising Identifier. This identifier is a user resettable ID assigned by a device to help advertising services. It is sent to third parties to advertisers and third parties and can be used to track user's movements.

Major retail store Target [19] has paired with marketing and beacon technology company Estimote [20] to create a network of beacons that can actively track users through Bluetooth chips embedded in their lightbulbs. These beacons do not connect like traditional Bluetooth devices, but rather send a broadcast signal with no specific recipient in mind. Any Bluetooth device in range, such as a smartphone, can then scan for these broadcasts and send a notification that data was received. Beacons generally broadcast data every 200ms, however most phones do not continuously scan for Bluetooth signals which means that tracking, while very near real time, is about 2-5 seconds behind. BLE signals are 2.4GHz radio waves that are broadcast, and location is gathered through the signal strength, with strategic placement of multiple beacons, the X, Y coordinated for a device can be pinpointed with incredible accuracy. Estimote makes the software development tool kit available for free on their website so that developers may implement this code into their applications [19]. This provides the third-party tracking needed for businesses to track your historical location.

Mitigation*:* With this location service being run through Bluetooth and not through GPS it is almost impossible to completely prevent this type of tracking. Mobile marketing is such a profitable technology that it is built into almost every consumer product today.

If you wish to enjoy the convenience of carrying a smartphone or smartwatch you may never truly escape location services, however there are various ways to limit the effectiveness of device tracking [21]:

1. Disable Bluetooth prior to entering a store. Although this is simple, it is generally a hassle as Bluetooth auto enables after 12 hours on most devices.
2. Mobile Marketing firms such as Estimote or Venntel allow you to enter your Advertisement ID into their website to opt out of data selling. This can stop your data that is collected by necessary applications from being sold to additional advertisers.
3. Do not download proprietary applications for every location you visit.
4. Limit advertisement tracking through your device's privacy settings.
5. Reset your Advertisement Identifier

4.3. Case 3: United States v Norris

Use*:* The fourth amendment only allows protections against something that is "unreasonable" however, courts and even scholars, have grappled with what the exact meaning of "reasonable" is in terms of the internet [22].This even brings up such questions as if you leave your wireless network open do you negate any expectation of privacy or if you use a home device such as Alexa do you negate that expectation of privacy? In the case, United States vs Norris, the ninth circuit court ruled that a defendant does not have a reasonable expectation of privacy when they piggyback off their neighbor's router for internet access without authorization [22]. During the investigation, agents traced the IP address of an account which was sharing child pornography on a file-sharing network which traced back to apartment 242. The material in question was not uploaded by residents of apartment 241 and it was noticed two unknown devices were connected to apartment 242's router without authorization [22]. When the MAC address of these two devices were put into an open-source wireless tracking software called Moocherhunter, the location was traced to apartment 243 [22].

Technology: Moochhunter is a wireless tracking software tool which relies on real-time on-the-fly geo-location of wireless moochers, hackers, and/or anyone using 802.11 wireless networks for what is considered objectionable purposes [23]. This software identifies the location of an 802.11 wireless moocher or hacker by traffic sent across the network [30]. Furthermore, this software, allows a network owner to detect unauthorized traffic through use of Moochhunter's passive or active mode through use of a laptop and directional antenna to isolate and track down the traffic source [30]. Additionally, the software allows the operator to move freely and walk towards the geographical location of a moocher/hacker [23].

Mitigation*:* The easiest mitigation to prevent unauthorized use of your network is to make the network hidden as then only those in authorized to use the network would know about the network's existence. As in by hiding your network, those wishing to mooch off your network or hack may be unable to do so. Additionally, having your network encrypted in some manner will prevent any unauthorized activity. As in by configuring your network to use WEP or WPA-2 will encrypt the network and password protect it making it harder for those to eavesdrop on your network.

4.4. Use case 4: COVID-19 Pandemic proximity tracking

Use*:* During COVID-19 pandemic, there has been a heightened interest in harnessing location data by the major tech companies. The goal is to track individuals affected by the virus, better understand effectiveness of social distancing, or to send alerts to individuals who may be affected based on previous proximity to known cases [24]. Furthermore, governments around the word are even considering whether and how to use this mobile location data to help contain the virus [24]. Public health agencies and epidemiologists are even interested in analyzing device data to track diseases [24]. However, this movement of devices effectively mirrors movement of people and thus comes with range of ethical and privacy concerns [24].

Mobile location data can be defined as "geolocation and proximity information from mobile phones and other devices" [25]. This mobile location data is often viewed as a key component in efforts to contain spread of COVID-19 [25]. Tracking is often used to determine if an individual has complied with social distancing and quarantine measures as well if someone has come into contact with someone who is contagious [25]. Three examples of how the government is using technology to respond to the pandemic include: contact tracing, enforcing quarantine and social distancing orders, big data analytics, hot spot maps [25].

Technology*:* Broadcasting refers to any method, through use of technology, through which government are publicly sharing locations of places visited by those within a certain timeframe [28]. This method is by far the easiest and fastest way to get such information out to the public.

Selective broadcasting, only releases information about those diagnosed that have visited a selected place to only a select few instead of everyone [28]. This requires collection of such information as telephone number or even current location from users in order to define these selected groups [28]. This technology has two modes: (i) the approximate location of the which can violate a user's privacy [29] or (ii) a message is sent to all users by the broadcaster but only messages relevant to the user's location are displayed [28].

Unlike broadcasting and selective broadcasting, unicasting only informs those who been in close contact with a person diagnosed with COVID-19 [28]. Unlike the previous technologies, this technology requires government access data of carriers and all those who have crossed their path [28]. This technology is highly effective but presents severe risks such as surveillance state and government abuse [29].

Mitigations*:* One solution to this issue, is limiting the information publicly shared helps to protect the carrier's identity from the public [28]. Given information is shared with third parties, ending this need for third party involvement could also increase privacy of diagnosed carriers [28]. Furthermore, any data collected should be very limited and highly regulated by governments and other entities through allowing users to consent to share their personal data [28]. Finally, having time limited storage of such information would protect diagnosed carriers and having open-source approach any application would help enforce privacy protections [28].

As stated previously, publication of sites where there has been known exposure to someone with COVID-19 is needed so as to inform the public [29]. However, this could cause a local business

to face harassment if their location is a known hot spot [28]. Therefore, having broader location data could better protect a business but affects accuracy [28]. Even with broader location data, a location business might be identified [28]. In short there must be some sort of tradeoff between impacts of utility of contact tracing technology and risks affecting a business and as such before any decision is made a business should be consulted before any location data is released [28].

Finally, the storage of sensitive information creates an opportunity for hackers. One way to prevent this is to have anonymized, redacted, and aggregated information stored instead [28]. Additionally, instead of using a central server to send out information [29], a distributed network makes hacking much harder [28]. However, the safest mitigation is to not only have all data stored in encrypted database that is inaccessible to all including the government but to have time limitations on data stored with in the contact tracing technology [29].

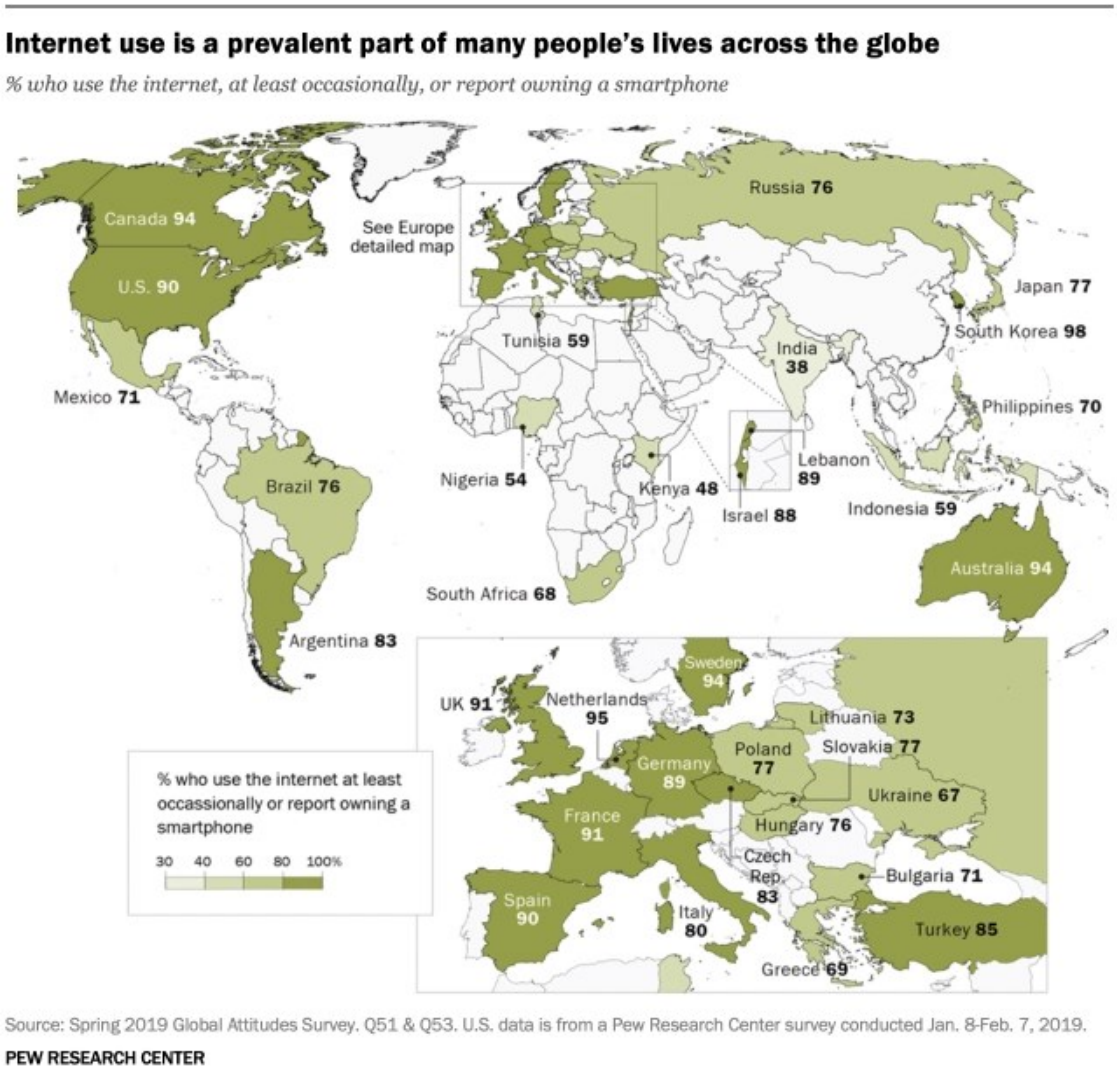

Figure: 2 Internet use is a prevalent part of many people's lives across the globe [3*7*.

4.5. Case 5: Human Mobility Tracking

According to a 2019 Pew Report, a large percentage of people use smart phone for their personal and official use [3]. The world has seen huge transformation in wireless technology. These new smart phones use multiple positioning systems like the cellular antenna, the Global Positioning System—GPS, and the Wi-Fi positioning system (WPS) to generate highly accurate and continuous geolocation of these devices. Below is the pictorial representation of how is internet for many people's lives across the globe.

The availability of these large location data of billions of these wireless device users, creates an increased opportunity for academic, commercial and governmental applications to analyze and interpret human mobility and characteristics. Mobility data can be used to identify patterns like how people travel in weekdays and weekends, how people celebrate different holidays, how human behavior change during catastrophic events like, earthquake or Hurricanes, etc.

These below figures describe a daily distance travelled by user can be tracked, analyzed and interpreted to understand the lifestyle of the user. This explains different activities performed by the user and then how an external factor can influence their daily routine. These data interpretations are done in a multi-step process. First need to segregate user locations, then identify the importance of the location and then map it to the actual user activity. Once we identify these interpretations, we can find similarities and/or variations between users depending of age, sex, race and education.

Figure. 3 Three levels of representing the user's travel distance, representing geo locations visited by the user and representing the semantic meaning of places the user has visited [31].

End user applications are becoming increasingly important for computing and mobile computing and, therefore, pose an ongoing opportunity for big mobility data. Also, these mobility data provide aggregated consumer statistics to businesses to customize the business interaction with user. This kind of analysis does have the ability to produce details about a person's routine, lifestyle and social network, creates both risk and opportunities for privacy. Commercial applications are now using location tracking and location-based services for end users. Contrary to initial expectations, however, location-based services did not emerge as 'killer apps' until recently [4]. These location data collected by these applications are then analyzed by commercial entities to understand the mobility of users within a store and allow the owners to optimize the product location within the store and also promote customized advertisements.

In recent years, a number of studies have been conducted to understand the willingness of customers to take the privacy risk to share the location information in order to gain the advantages

of location-based services. Users in modern world are now less concerned about the geolocation privacy issues to achieve the personalized services provided by these "killer apps". The "whenever & wherever" or "always on" feature of these applications, allows it to gather the geolocation information of the user all the time, which pose a great threat to the end users' location privacy.

5. Practical Countermeasures

Depending on the software and networking used, a variety of considerations will impact security. Routinely changing passwords, closely monitoring user accounts, and implementing encryption are the first and basic steps to be taken for protecting networks and the information on them. The only way to confront the privacy challenges associated with operating various devices is to learn which combinations of software and networking technologies are being used with each. The best privacy settings for computers and smartphones include turning off location services, not letting apps share data, enabling privacy settings in downloaded applications, and being careful with social logins [33].

As mentioned previously, smartphones have numerous features that also create vulnerabilities. Depending on the operating system, the privacy settings will vary. The most common operating systems for smartphones are Google Android, Apple iOS, and Windows Phone. Google Android currently has 85% of the global market, making Apple iOS the only other common option as Windows Phone was discontinued by Microsoft in 2017 [34]. Recommended security settings can be different depending on which version of operating system is installed on a mobile device. For example, the 11^{th} version of android was release on September 8, 2020, meaning that an android device could have another operating system with different features [36]. To determine which version of operating system is on an android device, first open device settings, select about phone or device, and choose android version. Android 11 has options for one-time permissions, scoped storage, background location accesses, secure identity credentials, and biometrics and encryption [37]. Effective application management and control is a continuing struggle between an operating system and applications that can be designed to exploit vulnerabilities. Researching the operating system, settings, and applications that are being used is the way to make educated decisions about the levels of risk involved with smartphones.

The article From an IP Address to a Street Address [7] introduced many of the countermeasures that need to be considered when using a wireless network. There are multiple options that can be implemented to better protect the information being exchanged across these networks. These countermeasures can be difficult to manage and can potentially cause problems by eliminating the use of other networking services and applications. The environment in which these wireless systems are used is typically what determines the available options utilized within that network.

5.1. Network configuration issues [7]

One of the primary issues with all wireless networks is the way they are configured. Most wireless networks are simply installed as quickly as possible and not thought of again. Monitoring, inspecting, and updating most networks is not practical because of the time and energy users would need to commit to this process. Configuring the wireless network versus simply plugging it in and

using the default password can be the difference between security and a significant network vulnerability.

5.2. Limiting signal range [7]

Preventing detection of the network by keeping it out of range or hidden like many wired networks is one of the most effective ways of physically limiting the exposure of the wireless network. Put simply, any wireless network that cannot accessed or reached is safer than one that is within range.

5.3. Firewalls and proxy access [7]

A proxy can be used as a standalone machine for routing or as a browser setting that functions as a network link protecting device IP addresses. Limiting access of the IP address within networks both filters traffic and functions as a firewall preventing malicious network activities that are aimlessly transmitted.

5.4. Regulating network traffic size [7]

Variable-sized packet reshaping is a way to manipulate the size of packets which can make them more difficult to analyze. Traffic shaping can be used to optimize performance, reduce latency, and maximize bandwidth depending on how it is implemented. While using and designing traffic shaping strategies the network can be changed to both reduce or eliminate any network traffic that is not appropriately shaped or configured.

5.5. Controlling bandwidth [7]

Data bursts and micro bursting are ways that networks can be explored. Quickly sending packet switching traffic to overflow packet buffers and discover the line rate at which devices operate is how an attacker can learn about the network. To avoid this issue, networks can saturate the remaining available bandwidth to ensure it is constantly used. This practice can negatively affect performance as it is limiting the rate at which traffic is allowed, therefor it does need to be monitored to allow normal network traffic to increase and decrease periodically.

5.6. Virtual private networks [35]

Many services are now available to route traffic through virtual private networks that are usually for a monthly fee. The fact that the network is virtual makes it a service. As a service it can be configured to change IP address to keep them private and safe. It is important to consider the connection speeds through a VPN as this will have a network performance impact. This has become one of the most popular methods of protecting a network.

This tradeoff between protection, risk, and what is practical for a given network specifically from a cost perspective takes significant planning and preparation as countermeasures offer both advantages and limitations. The settings typically used on personal and home networks is limited compared to institutions where more users need to be protected not only from internet activity, but

also from each other. Large organizations networking needs are frequently categorized into functional and administrative responsibilities for the purposes of planning, implementation, and maintenance. Both the hardware and software will have individual considerations that must be aligned with the plans and goals of the organization. This results in a continually changing set of policies and practices that require constant attention and evaluation. Many organizations employ large teams of people who are responsible for various parts of these processes by ensuring network security is continually being optimized and adjusted for the various networking requirements.

6. Conclusion

The security issues associated with geolocation data continue to become increasingly vulnerable, as demand for these services grow so do the capabilities of exploitation. Being aware of privacy issues associated with compromised geolocation data is imperative to the security of personally identifiable information. Once the location and identity of an end user is correlated, they become vulnerable to a multitude of consequences. Scamming, fraud, and identity theft are prevalent attacks which result from misuse of real-time and historical geolocation data. The main challenge for an end user is understanding and acceptance of risks associated with the collection of their location data. As users seek convince in their daily lives, many freely share their location with developers of mobile applications without being fully aware of how it is analyzed and exploited. The question remains, where is the proper balance between convenience and security? With the implementation of proper risk mitigation strategies and a matured understanding of the 'whenever and wherever' and 'always-on' nature of location-based services, users can make an educated decision of their personalized location preferences.

References

[1] Wang, D. Burgener, M. Flores, A. Kuzmanovic, and C. Huang, "Towards street-level client-independent IP geolocation," in USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2011.

[2] YihChun Hu, & Helen J. Wang. (2005). A Framework for Location Privacy in Wireless Networks. https://doi.org/U.S. Department of Homeland Security (DHS) and the National Science Foundation (NSF) under grant ANI-0335241

[3] Pew Research Center. (2020, April 1). Internet use is a prevalent part of many people's lives across the globe. Pew Research Center. https://www.pewresearch.org/fact-tank/2020/04/02/8-charts-on-internet-use-around-the-world-as-countries-grapple-with-covid-19/ft_2020-04-02_globalinternet_01/.

[4] H. Yun, D. Han, and C. C. Lee, "Understanding Use of LBS Applications with Privacy Concern," UNDERSTANDING THE USE OF LOCATION-BASED SERVICE APPLICATIONS: DO PRIVACY CONCERNS MATTER? 2013.

[5] S. Gray, "Future of Privacy Forum," A Closer Look at Location Data: Privacy and Pandemics, 25-Mar-2020. [Online]. Available: https://fpf.org/2020/03/25/a-closer-look-at-location-data-privacy-and-pandemics/. [Accessed: 19-Nov-2020].

[6] J. Enberg, "US Digital Ad Spending 2019," 2019. [Online]. Available: https://www.emarketer.com/content/us-digital-ad-spending-2019. [Accessed: 19-Nov-2020].

[7] E. De Cristofaro, "An Overview of Privacy in Machine Learning," arXiv.org, 18-May-2020. [Online]. Available: https://arxiv.org/abs/2005.08679. [Accessed: 19-Nov-2020].

[8] P. Figliola, "Federal Communications Commission: Progress Protecting Consumers from Illegal Robocalls," EveryCRSReport.com, 10-Apr-2020. [Online]. Available: https://www.everycrsreport.com/reports/R46311.html. [Accessed: 19-Nov-2020].

[9] C. A. Shue, N. Paul, and C. R. Taylor, "From an {IP} Address to a Street Address: Using Wireless Signals to Locate a Target," USENIX, 01-Jan-1970. [Online]. Available: https://www.usenix.org/conference/woot13/workshop-program/presentation/shue. [Accessed: 19-Nov-2020].

[10] Tau, B., & Hackman, M. (2020, February 7). WSJ News Exclusive | Federal Agencies Use Cellphone Location Data for Immigration Enforcement. https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600.

[11] Barron, L. (2018, August 24). Arizona: Police Find Cross Border Drug Tunnel in Former KFC. https://time.com/5377009/arizona-drug-tunnel-kfc-mexico-bedroom/.

[12] Contract- Department of Homeland Security (DHS) & PANAMERICA COMPUTERS, INC. (2017, September 29). https://www.usaspending.gov/award/CONT_AWD_HSHQDC17J00525_7001_HSHQDC12D00013_7001.

[13] Bradstreet, Inc. (D&B), D. & (Ed.). (2020). Homeland Security Department & U.S. CUSTOMS AND BORDER PROTECTION Order. https://www.fpds.gov/ezsearch/fpdsportal?s=FPDS.GOV&templateName=1.5.1&indexName=awardfull&q=Venntel+PIID%3A%2270B04C20F00000914%22.

[14] Venntel, Provider real-world location intelligence. (2020). https://www.venntel.com/.

[15] Carolyn B. Maloney, Elizabeth Warren, Ron Wyden, & Mark DeSaulnier. (2020, June 24). CBM Warren Wyden DeSaulnie to Venntel re Mobile Phone Location Data.

https://oversight.house.gov/sites/democrats.oversight.house.gov/files/2020-06-24.CBM%20Warren%20Wyden%20DeSaulnie%20to%20Venntel%20re%20Mobile%20Phone%20Location%20Data.pdf.
[16] Valentino-devries, J., Singer, N., Keller, M. H., & Krolik, A. (2018, December 10). Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.
[17] Marcel, J. (2020, February 12). Bluetooth Beacons are onTarget with a Major Retailer. Bluetooth® Technology Website. https://www.bluetooth.com/blog/bluetooth-beacons-are-on-target-with-a-major-retailer/.
[18] Saiidi, U. (2019, March 8). Retailers can track your movements inside their stores. Here's how. CNBC. https://www.cnbc.com/2019/03/08/how-retailers-can-track-your-movements-inside-their-stores.html.
[19] McFadden, C. (2019, June 20). Some Businesses Are Tracking Your Every Move Using Bluetooth Beacons. Interesting Engineering. https://interestingengineering.com/are-you-being-tracked-by-bluetooth-beacons-while-shopping.
[20] Estimote a complete Software Development Kits (SDKs). Prototype, test and deploy with Estimote products. https://estimote.com/products/.
[21] Jess Bolluyt More Articles November 27, 2014. (2014, November 27). What's So Bad About In-Store Tracking? Showbiz Cheat Sheet. https://www.cheatsheet.com/technology/whats-so-bad-about-in-store-tracking.html/.
[22] Recent Case: _United States v. Norris_ (Harvard Law Review): The Fourth Amendment has long been understood to be an important source of constitutional protection of an individual's right to privacy. The rise of digital technologies has, however, eroded the clarity of these protections, which turn on physical words such as "persons, houses, papers, and effects." Legally, a police investigation only implicates the Fourth Amendment... Harvard Law Review. https://blog.harvardlawreview.org/recent-case-_united-states-v-norris_/.
[23] Securitystartshere.org. MoocherHunter™ wireless tracking software tool. MoocherHunter(tm) - Geo-locate and hunt down wireless moochers and hackers on-the-fly! https://securitystartshere.org/page-software-moocherhunter.htm.
[24] GRAY, S. T. A. C. E. Y. (2020, March 25). Future of Privacy Forum. Future of Privacy Forum iCal. https://fpf.org/2020/03/25/a-closer-look-at-location-data-privacy-and-pandemics/.
[25] Mobile Location Data and Covid-19: Q&A. Human Rights Watch. (2020, October 28). https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa.
[26] GELINAS, J. A. M. E. S. (2020, July 10). What are the security and privacy risks behind digital contact tracing? Komando.com. https://www.komando.com/coronavirus/coronavirus-tracing-apps-privacy-risks/745788/.
[27] Toch, E., Lerner, B., Ben-Zion, E. et al. Analyzing large-scale human mobility data: a survey of machine learning methods and applications. Knowl Inf Syst 58, 501–523 (2019). https://doi.org/10.1007/s10115-018-1186-x
[28] R. Raskar, R. Barbar, and I. Schunemann, Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic, Mar. 2020.
[29] Md. Tanvir Rahman, Risala T. Khan, Muhammad R. A. Khandaker, and Md. Sifat Ar, *An Automated Contact Tracing Approach for Controlling Covid-19 Spread Based on Geolocation Data from Mobile Cellular Networks*, 2017.

[30] Darknet, “MoocherHunter – Detect & Track Rogue Wifi Users,” *Darknet*, 11-Sep-2017. [Online]. Available: https://www.darknet.org.uk/2008/07/moocherhunter-detect-track-rogue-wifi-users/. [Accessed: 20-Nov-2020].
[31] E. Toch, B. Lerner, and E. Ben-Zion, “Analyzing large-scale human mobility data,” A survey of machine learning methods and applications, 2018.
[32] “Locate a device in Find My iPhone on iCloud.com,” Apple Support, 2020. [Online]. Available: https://support.apple.com/guide/icloud/locate-a-device-mmfc0f2442/icloud. [Accessed: 20-Nov-2020].
[33] “What are the best privacy settings for my computer and smartphone?,” Common Sense Media: Ratings, reviews, and advice. [Online]. Available: https://www.commonsensemedia.org/privacy-and-internet-safety/what-are-the-best-privacy-settings-for-my-computer-and-smartphone. [Accessed: 20-Nov-2020].
[34] N. Galov, “Mobile and Desktop Operating Systems Market Share,” HostingTribunal, 12-Nov-2020. [Online]. Available: https://hostingtribunal.com/blog/operating-systems-market-share/. [Accessed: 20-Nov-2020].
[35] “Finally, A VPN explanation for the non-technical world,” WhatIsMyIPAddress.com, 2020. [Online]. Available: https://whatismyipaddress.com/vpn. [Accessed: 20-Nov-2020].
[36] “Android version history,” Wikipedia, 19-Nov-2020. [Online]. Available: https://en.wikipedia.org/wiki/Android_version_history. [Accessed: 23-Nov-2020].
[37] D. Nield, “The Android 11 Privacy and Security Features You Should Know,” Wired, 27-Sep-2020. [Online]. Available: https://www.wired.com/story/android-11-privacy-and-security-features/. [Accessed: 23-Nov-2020].