SMU Data Science Review

Volume 1 | Number 3 Article 13

2018

Unintended Consequences of Location Information: Privacy Implications of Location Information Used in Advertising and Social Media

Alice Karanja
southern methodist university, akaranja@smu.edu

Daniel W. Engels
Southern Methodist University, dwe@smu.edu

Ghizlane Zerouali
Southern Methodist University, gzerouali@mail.smu.edu

Ariel Francisco
Southern Methodist University, afrancisco@mail.smu.edu

Follow this and additional works at: https://scholar.smu.edu/datasciencereview

Recommended Citation

Karanja, Alice; Engels, Daniel W.; Zerouali, Ghizlane; and Francisco, Ariel (2018) "Unintended Consequences of Location Information: Privacy Implications of Location Information Used in Advertising and Social Media," *SMU Data Science Review*: Vol. 1 : No. 3 , Article 13.
Available at: https://scholar.smu.edu/datasciencereview/vol1/iss3/13

This Article is brought to you for free and open access by SMU Scholar. It has been accepted for inclusion in SMU Data Science Review by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.

Unintended Consequences of Location Information: Privacy Implications of Location Information Used in Advertising and Social Media

Ariel Francisco, Alice Karanja, Ghizlane Zerouali, Daniel W Engels
Southern Methodist University (SMU), 6425 Boaz Lane, Dallas,
TX 75205, USA
{afrancisco, akaranja, gzerouali, dwe}@smu.edu

Abstract. In this paper, we identify and evaluate the privacy implications caused by ourselves sharing information on social media platforms. Each day, millions of people use Facebook, Snapchat, Instagram, Twitter, and many other social media services and applications to stay connected with friends and family. We broadcast personal information such as our names, location, occupation, spouse's and children's names, personal photographs and videos, and other intimate details of our everyday lives. Social media sites monetize this free exchange of personal information by capturing and mining this data and significant metadata for advertising and other revenue generation activities. As we have divulged more of our private lives on social websites and applications, the opportunities for criminals to victimize users by capturing and mining this same information has increased exponentially. Yet, most social media users are unaware of the dangers that exist with even their casual use of social media. We found that our privacy is not well protected by neither the social media companies nor the law as it relates to our social media activities, and, therefore, consumers must take the initiative to understand the privacy implications of their social media activities.

1 Introduction

Social Media Platforms (SMP) allow users to communicate both within and beyond their local and social boundaries. According to *The Statistics Portal*, as of 2018, 77% of the population in the United States have a social networking profile[1]. Worldwide, there are 2.34 billion social media users, and that number is expected to grow to 2.95 billion by 2020[3].

The use of social media has been made even easier by the widespread adoption and use of smartphones. Smartphones have evolved from merely portable telephones to powerful computing devices that integrate a broad range of technologies including high resolution digital cameras, Global Positioning System (GPS) capabilities, touch screens, and multiple networking technologies like cellular communications, Wi-Fi, and Bluetooth. The newest cell phones even rival laptops in price and capabilities and allow users to do even more with a palm held device than with a laptop computer. Ubiquitous, fast communications accessible from our palm means that we can search

[1] *The Statistics Portal* aggregates statistics and studies from a broad range of sources and may be found at https://www.statista.com/.

[3] The chart of worldwide social media users is available at: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/Statist_Number_of_social_media_users_worldwide_from_2010_to_2021_(in_billions) (accessed August 18, 2018).

for commodities, businesses, or stores wherever we or they may be in the world. GPS and other location technologies integrated into smartphones and other mobile devices helps us navigate simply to the even the furthest stores, and now we can even utilize the apps and communication capabilities to shop online and have our purchases delivered directly to us, whether home or on the road. With these new technologies, the world is at our fingertips, and it can come to us with the push of a button.

The integration of real-time location information through the GPS module, cellular tower triangulation, and the mapped location of Wi-Fi networks enable location-based applications and benefits; however, these same technologies have turned smartphones into real-time tracking beacons that are constantly with their owners. This new method of tracking people, in real-time via their smartphones, raises a concern about personal privacy. The availability of this tracking technology in all smartphones and the hidden nature of its operation results in many consumers being unaware that they are being tracked and unaware of who is tracking them, usually with their explicit permission.

The use of real-time location information for consumers with cell phones has allowed Social Media Platforms to take advantage of their users' locations to provide targeted, location-based services. Additionally, location information is commonly used to provide contextually aware advertisements and unsolicited location-based recommendations. However, these recommendations have the potential to violate privacy, for example, by recommending users to connect with people who frequent the same locations. This method of marketing is legal, although potentially unethical.

Businesses, including Social Media Platforms, often slip the disclosure that they are tracking their users into lengthy terms of service contracts or privacy policy statements that are unlikely to be read by users. These policies and what businesses do with a user's collected data are non-negotiable. The user either agrees to use the application or service or cannot use the application. When consumers agree to terms of services, they have no ability to opt-out or prevent the collection of at least some of their location information while they use the service. The collection of all this information has enabled location-based advertising to become a great source of revenue for social networks and other third parties.

The use of Social Media Platforms poses various types of threats to users that can be grouped into three broad categories: Privacy related threats, Identity related threats, and Social threats. The profiles that we create on SMPs are a treasure trove of information that could easily be accessed by criminals. Data mining techniques can be used to collect profile related attributes from Facebook, Twitter, or Instagram which can be used to blackmail or expose private information about the user. It has also been said that even employers are combing through social media to screen prospective job applicants. According to CareerBuilder, as of 217, "70% of employers use social media to screen candidates, 50% of employers check current employees' social media profiles, and over a third have reprimanded or fired an employee for inappropriate content"[4]

In this paper we explore the privacy, social and identity related threats to social media users. Then we talk about the Laws and Regulations in place to

[4] http://press.careerbuilder.com/2017-06-15-Number-of-Employers-Using-Social-Media-to-Screen-Candidates-at-All-Time-High-Finds-Latest-CareerBuilder-Study

protect us on line. We also discuss the techniques used to gather location information and how users can protect themselves. Finally, we review previous surveys that have been conducted on SMP users to learn just how much the public knows about all the data collected by SMPs.

Privacy Related Threats

Any information and uploads that are shared publicly on social media, size to be private and can be viewed and used in countless ways by the collector. It is therefore, important to be careful about what we post because it could have implications to us and others. For instance, image tagging links a photograph to the names and profiles of the persons present in the photo (even if they did not initiate it). This can be used to eventually link names, images, profiles from other SMPs and even email addresses. All this information can be used by criminals and cause immeasurable losses to the user. To make it worse, it is nearly impossible to completely delete one's profiles and comments from social media. Even if a user deletes their account, they cannot erase any comments they made on someone else's page [1].

Social Network spam can result in traffic overload, phishing attempts and even diversion to pornographic websites. In SMPs, spam comes in the form of wall post, news feed, and message spam and is more effective than the traditional email spam. The social network spam usually contains advertisement, or hyperlinks that victims can click on. Once spammers have access to our information, they can log into other accounts or websites and cause other problems such as Denial of service attacks, viruses and worms[5].

Other Threats

An individual's context in the social network can be used to extract sensitive information through social phishing. Social phishing threats include an email phishing attack which can achieve a 72% hit rate by using information available in the social network [2]. Phishing attacks can also incorporate greater elements of context to become more effective. An attacker could gain the trust of victims by obtaining information about their bidding history or shopping preferences [4]. These phishing attacks can reveal important information like login usernames and passwords or bank account information.

Profile squatting, when someone impersonates another, can end up causing embarrassment and or financial ruin. Criminals can gain access to financial accounts using log-in information garnered from email phishing attacks. Once they have control of your money, they could make purchases in your name, transfer funds out of your accounts or even open new accounts in you name. Cyber stalking is another danger of sharing personal information online such as address and other contact information.

[5] http://www.net-security.org/secworld.php?id=10208- Facebook users think social networking spam is a problem,

When strangers know where you are always, they can easily track you to your home or place of work both of which can lead to physical or psychological harm.

The social network providers need our private data for advertisement to generate revenues. Hence, it is a trade-off between providing security to users and releasing the same data to advertising companies. While the data are meant for the advertisers, attackers can take advantage of it as well. Providing this balance is challenging as the size and complexity of the data increases [3].

2 Laws and Regulations

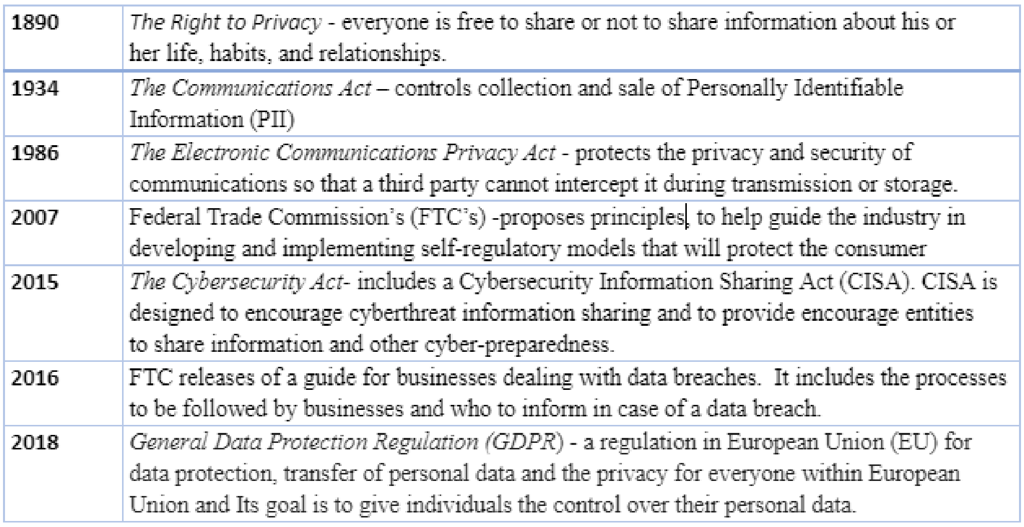
Location-based information is required by law for emergency purposes. In 1999, The United States Congress passed the Wireless Communications and Public Safety Act [18]. This law was enacted with the intent to modernize the 911 emergency telephone number which assists emergency responders to locate those in need. The law stipulates that wireless network operators be able to provide both the telephone number and the geolocation of the phone that made the 911 call. The location of the phone must provide latitude and longitude with an accuracy of between 50 and 300 meters.

In the US, the two laws that govern location data are the Electronic Privacy Act of 1986 and the Communications Act of 1934. Both laws were enacted before most of the current technology was developed and may be irrelevant in today's world. In addition, the Federal Trade Commission's "Behavioral Advertising Principles" calls for "companies to obtain affirmative express consent from consumers before they use data in a manner that is materially different than promised at the time of collection and before they collect and use "sensitive" consumer data for behavioral advertising" [5].

A policy is a document explaining how and why websites collect, use and manage user information. Most privacy policies are full of terminology that is not familiar to the public. They are long, imprecise and almost impossible to understand for the layperson. Even though a website provides a privacy policy, it does not mean that they protect any information they collect. This practice is contrary to the common perception of safety among Americans where the Pew Research Center[7] found that more than 50% of Americans believe a privacy policy ensures information to be kept confidential.

Table 1: Summary of data protection Laws and regulations in the USA [19[[20]

[7] http://www.pewresearch.org/fact-tank/2014/12/04/ half-of-Americans-don't-know-what-a-privacy-policy-is/.

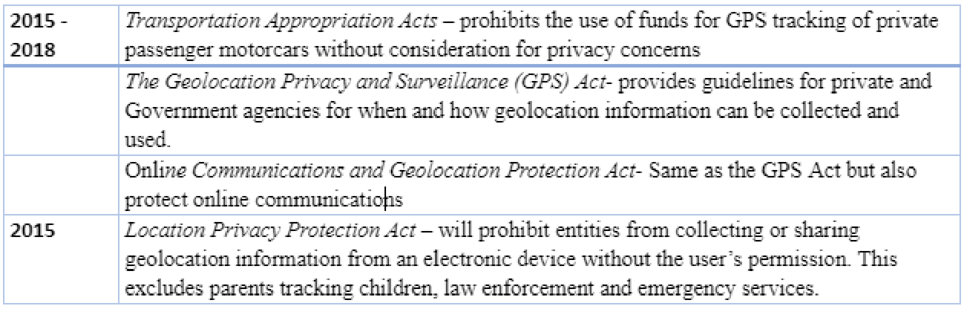


1890	*The Right to Privacy* - everyone is free to share or not to share information about his or her life, habits, and relationships.
1934	*The Communications Act* – controls collection and sale of Personally Identifiable Information (PII)
1986	*The Electronic Communications Privacy Act* - protects the privacy and security of communications so that a third party cannot intercept it during transmission or storage.
2007	Federal Trade Commission's (FTC's) -proposes principles to help guide the industry in developing and implementing self-regulatory models that will protect the consumer
2015	*The Cybersecurity Act*- includes a Cybersecurity Information Sharing Act (CISA). CISA is designed to encourage cyberthreat information sharing and to provide encourage entities to share information and other cyber-preparedness.
2016	FTC releases of a guide for businesses dealing with data breaches. It includes the processes to be followed by businesses and who to inform in case of a data breach.
2018	*General Data Protection Regulation (GDPR)* - a regulation in European Union (EU) for data protection, transfer of personal data and the privacy for everyone within European Union and Its goal is to give individuals the control over their personal data.

The GDPR is only applicable to US companies or entities that collect personal data from someone in a European Union (EU) country e.g. via the internet.

Several U.S. states have enacted laws that protect personal location information. However, the federal U.S. statute does not have such laws in place. Table 2 lists a few such laws and regulations that are currently awaiting approval by congress.

Table 2: Location Information Laws[9]

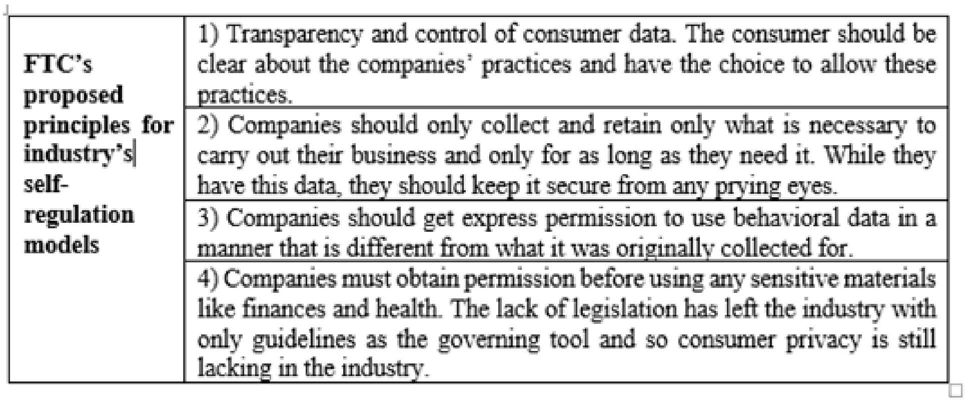


2015 - 2018	*Transportation Appropriation Acts* – prohibits the use of funds for GPS tracking of private passenger motorcars without consideration for privacy concerns
	The Geolocation Privacy and Surveillance (GPS) Act- provides guidelines for private and Government agencies for when and how geolocation information can be collected and used.
	Online *Communications and Geolocation Protection Act*- Same as the GPS Act but also protect online communications
2015	*Location Privacy Protection Act* – will prohibit entities from collecting or sharing geolocation information from an electronic device without the user's permission. This excludes parents tracking children, law enforcement and emergency services.

Table 2 outlines the Federal Trade Commission's (FTC's) proposed principles, from December 2007, to help guide the industry in developing and implementing self-regulatory models that will protect the consumer [15]

Table 3: FTC proposed principles

[9] https://www.gps.gov/policy/legislation/gps-act/



FTC's proposed principles for industry's self-regulation models	1) Transparency and control of consumer data. The consumer should be clear about the companies' practices and have the choice to allow these practices.
	2) Companies should only collect and retain only what is necessary to carry out their business and only for as long as they need it. While they have this data, they should keep it secure from any prying eyes.
	3) Companies should get express permission to use behavioral data in a manner that is different from what it was originally collected for.
	4) Companies must obtain permission before using any sensitive materials like finances and health. The lack of legislation has left the industry with only guidelines as the governing tool and so consumer privacy is still lacking in the industry.

3 How Information is Gathered

All social media is not created equal. Some of the Social Media Platforms require more information to be disclosed for users to sign up for services than others. Research suggests that ordinary users don't fully understand the scope of the data that is being collected on them — or how small amounts of data can be used to create a much more detailed portrait when matched with information from third-party sites that collect and share various types of customer information with each other[6]. People understand that their data is being used, but, according to a study performed by the Pew Research Center[10], don't truly understand how data mining works where one or two data points can be linked with other sources to uncover information they would have never given out in the first place.

While one SMP may only require your name to open a profile account, the next one may require phone numbers or email address with the name. Social engineering can allow for all these data points to be connected and come up with a pretty accurate history, likes and behavior of the user. Figure 1 shows a summary of mandatory information for Facebook, Google, LinkedIn and Twitter accounts.

[10] http://www.pewresearch.org/fact-tank/2014/12/04/ half-of-Americans-don't-know-what-a-privacy-policy-is/.

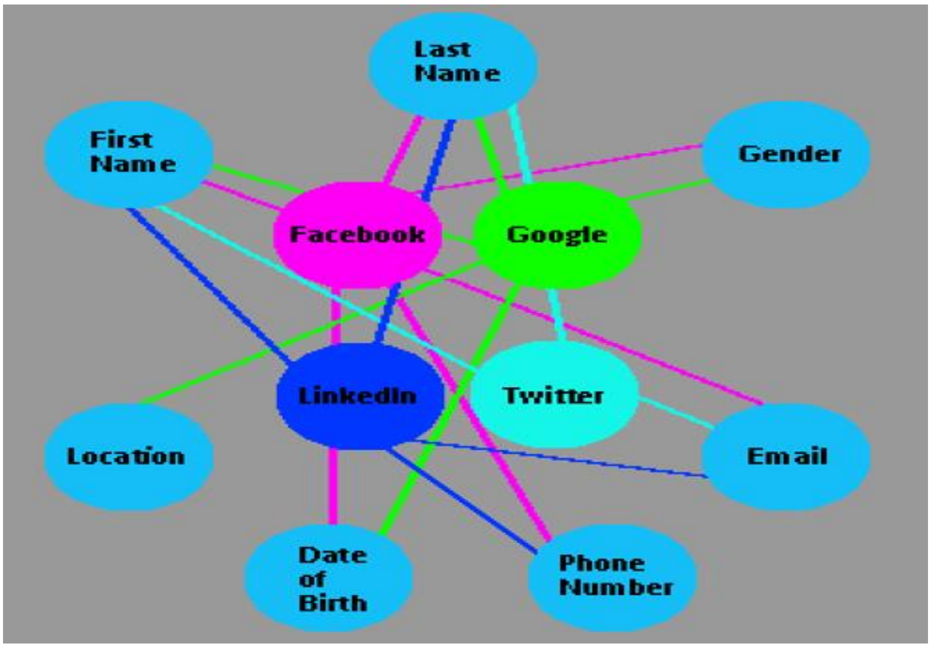


Figure 1. Mandatory Information Comparison

3.1 Location Information

Social media platforms such as Facebook, Instagram, and Snapchat use location information. Some platforms require the user to allow permission for the app to track the location of the phone at least during the use of the app with some requiring location tracking at all times. Other platforms record the location of the user at the time of usage, i.e. the location a picture was taken. As with computers, using cell phones to access the Internet may also divulge their location via the IP address. Constantly providing the location of the user allows the apps to provide improved services, but it does raise issues regarding privacy, societal interactions, and ethics related to the use and dissemination of the information.

The use of location information for advertising, in addition to social media, has posed privacy, societal, and ethical questions that must be addressed in order to safeguard privacy concerns. Location information is used to send advertisements to the smartphone users. Social media applications will usually display advertisements based on the general location of the smartphone. This can be intrusive and quite eerie at times as search history is also considered when deciding what to advertise.

Another privacy concern regarding location information is what amount of this information is accessible to the government. If social media applications are required to provide their services to law enforcement, it can be assumed that location information will be highly desirable information along with any collected data on the user. This can be a powerful tool for the police and other law enforcement agencies. Although one may dismiss this concern in a country with a strong sense of civil liberties, citizens in more authoritarian states may be at risk. An example of this can be seen when analyzing the Arab Spring and the subsequent Syrian Civil War and rise of ISIS. Even without a live feed of location information, the whereabouts, or recent whereabouts of an individual can unwillingly be made publicly available. For instance, John McAfee (of McAfee antivirus) had been in hiding from Central American authorities for years. He was an avid social media user with a lot of followers. McAfee agreed to an interview and a selfie with one of his fans, a blogger. The blogger posted that selfie on social media and it was downloaded by the local authorities in Central America. Using the photo's metadata, they were able to locate and arrest McAfee shortly thereafter. The blogger had GPS and location services turned on while he took the photograph, and the GPS coordinates were embedded within the photograph.

Location-based information can also be a societal issue, and the person posting the picture should consider how making that picture and its location public may affect the individuals in the picture. When you take a photograph, the device used adds metadata to the image. Metadata may include time and date, location coordinates, information about the camera and even copyright information. For instance, an individual may wish to keep their attendance at a certain event or location private; however, social media applications also advertise to those in one's network that they are attending an event or visiting a nearby location.

Considering all the privacy concerns and ethical issues involved with location-based information, many users aren't aware of or are not concerned by the amount of information they are providing to social media platforms [5]. There are both benefits and perils to supplying location-based information to social media platforms. Users need to be well informed on exactly what they are providing and to whom. They should also be knowledgeable on how to prohibit or limit the access to information given to social media platforms.

3.2 Mobile Device Tracking Technologies

To provide security to users, and to help businesses control the trajectory of their employees, multiple software and hardware systems have been developed for tracking mobile devices. Android's Network Location Provider application determines user location using cell tower and Wi-Fi signals. The purpose of location-based services is to find the Physical location of the device in case the device is lost. Internet of Things (IoT) is the network that consists of physical objects, or "things", embedded in electronics, software, sensors, and network connectivity to enable objects to exchange data with the producer, operator, and/or other connected devices based on the infrastructure. All applications for mobile devices have a combination of the most popular techniques to track the location.

Social Media Platforms provide users a service that is payed for with our information. Companies track their users for reasons such as personalization and targeting which leads to timely, targeted advertising; session management (the websites remember the items that are in a shopping cart whenever the user logs into their account); and tracking a user's browsing habits which again leads to more advertising and recommendations.

Online tracking of users is accomplished by use of Hypertext Transfer Protocol (HTTP) Cookies, digital fingerprinting, social widgets among others. Cookies track users online by storing information in the user's web browser, so that the web browser, or device, is recognizable. Its stored activities are retrieved whenever the user returns to the site and hence keeps a history of your internet activity as shown in figure 2. There are two types of cookies used by Social Networking Sites, namely persistent and session cookies. Session cookies, also known as temporary cookies, are only active for one session, and are deleted when the user closes the web browser. This is unlike persistent cookies that are stored on the user's browser and expire after a length of time. Persistence (or tracking) cookies are preferred by advertisers because they collect information about a user's browsing habits. These are of great concern because of privacy issues, especially involving third-party tracking cookies. Third-party cookies are set out by advertising companies or data brokers, not the host website.

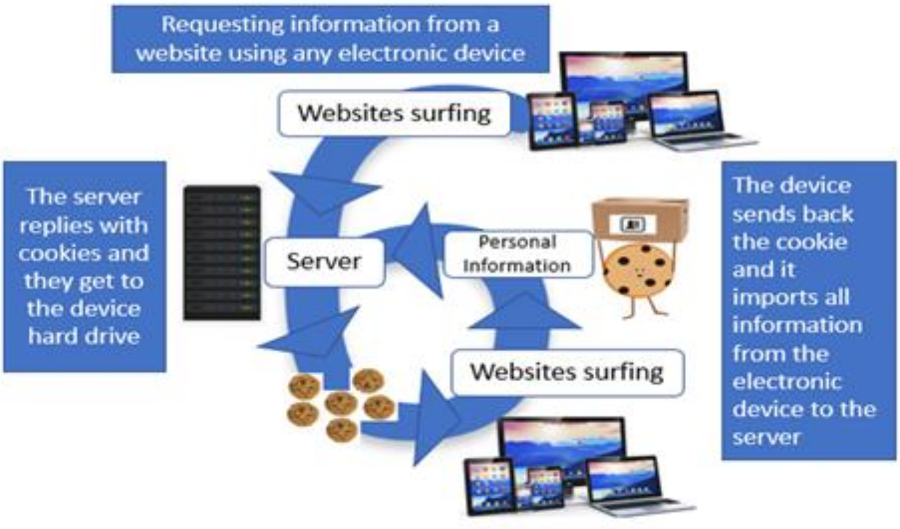

Requesting information from a website using any electronic device
Websites surfing
The server replies with cookies and they get to the device hard drive
Server
Personal Information
The device sends back the cookie and it imports all information from the electronic device to the server
Websites surfing

Figure. 2: How HTTP Cookies Work

Social widgets are small pieces of code that are found on websites to redirect users to other websites. These include pop-up windows, dialogue boxes or buttons that collect information from Social media platforms about the users. Digital fingerprints like IP Address, device information and other settings are left behind whenever a device is connected to the Internet. This is how multiple devices, smartphone, tablet and laptop can be linked to the same user via the IP address. Web beacons are graphic images placed on websites and used together with cookies to gather user information.

The use of cookies, widgets, digital fingerprinting and web beacons has made it very easy for the internet browsers and Apps to trace us wherever and whenever.

3.3 GPS Tracking

GPS (Global Positioning System) tracking system is the most widely used technique for accurately tracking location. GPS is a radio navigation system that allows land, sea and airborne users to determine their exact location, velocity, 24 hours a day, in all weather conditions, anywhere in the world[11]. GPS is distinguishable from other techniques because of its outstanding accuracy. GPS tracking systems not only tell the exact location of the service, but also provides historic navigation data.

The GPS system is a collection of 24 satellites and their ground stations which was initially funded and controlled by the US Department of Defense[13]. The GPS system uses a network of Global Navigation Satellite Systems (GNSS) that use microwave signals that are transmitted and received by GPS devices. The devices use the received signals to calculate information such as location, time, and direction.

GPS receivers in mobile phones receive signals from the satellite. The time difference between the transmission of a signal from a satellite to its reception by the receivers, is used to calculate the receiver's coordinates. Trilateration is a concept of measuring distances that is used to pinpoint the exact location of a GPS receiver. Trilateration is done with the help of at least three satellites. Each of several satellites emits a signal to a GPS receiver and the distance to the receiver is measured. Where all the distances to the receiver intersect, is the true location of the GPS receiver [16] [17].

GPS technology is now available in nearly all new smartphones, and it enables the tracking of anyone carrying these GPS enabled smartphones. Locating a device is accomplished by measuring power levels and antenna patterns as the mobile phone communicates wirelessly with one of the satellites in the network. The use of advanced systems gives a rough estimate of the distance from the base station while more precise approximation is done by interpolating signals between antenna towers. The precision of location can achieve a precision of about 50 meters in urban areas where there are more antenna towers.

Once the GPS locates the mobile phone, the GPS tracking applications communicate this location information to a software program or application. This is done through transmission by text, data connection or Wi-Fi.

3.4 Wi-Fi Tracking

Wi-Fi tracking uses Wi-Fi hotspots or access points to track the location of a device. Wi-Fi is the wireless version of a wired Ethernet network. Wi-Fi radios can identify the RSSI of each signal and report this upstream. Wi-Fi supports monitoring mode, which is implemented by most vendor solutions. Monitoring mode allows the upstream drivers to obtain every received packet, while still supporting the ability to send Probe Requests. Access points are typically available at public and private places both, making it easier for us to track the location of the desired device.

Devices can use both GPS and Wi-Fi send signals back to the GPS company about any networks around. The device sends the access points along with the location determined by the GPS. The GPS scans the nearby networks for any publicly accessible information that can be used to identify the network [6]. After the network has been identified its location is recorded and stored. This location information is later used to track other users that are in the nearby networks but may not have good GPS signals.

[11] http://www.gis2gps.com/GPS/GPSDEF/gpsdef.html/GPS_definition._Gis2gps

[13] http://www.gis2gps.com/GPS/GPSDEF/gpsdef.html/GPS_definition._Gis2gps

Wi-Fi tracking is less accurate than GPS tracking as the results vary from 20 to 30 meters, but the positive thing about this tracking technique is that it works perfectly indoors. Also, Wi-Fi signals are not affected by weather conditions.

3.5 GSM Tracking

A GSM device must be connected to a network for it to receive or make calls. A GSM phone emits a signal when turned on. The emitted signal is received by nearby towers which connects the phone to another when a call is made. A GSM signal from a phone is picked up by the towers at any time even when the user is not making or receiving calls. Each transmission tower has a known location and perimeter of operation. The location of a cell phone user is determined based on its presence from a specific tower. The tower uses a combination of hardware and software to detect a signal from a phone and compute its location based on the gathered data by the nearest tower.

For a more precise location determination, more sophisticated tracking technologies can be used to combine data from several transmission towers simultaneously. All these signals are received at different strengths by the respective towers leading to higher precision and tighter perimeter in which the user is located [8].

The two main methods of GSM mobile phone tracking are Network based and Handset-based. The network-based only uses the signal emitted and/ or received by the towers. These towers are part of the telecommunication company’s network which owns and runs them using their specific hardware and software. The handset-based method utilizes a GSM tracking device which must be connected to the phone that is being tracked. Sometimes, a microchip or special software can be installed in the phone to replace the GSM device. This method is not commonly used because not all phones are compatible with the hardware and software that is required.

GSM or cell tower-based tracking is the cost-effective way of tracking the location of smartphones, it has an accuracy of few miles to 50 meters. GSM tracking also has a few drawbacks. Firstly, the accuracy of its results depends on the number of cell towers present in the surroundings of the device to be tracked. GSM assigns unique numbers to each mobile device (IMEI) and each mobile subscriber (IMSI). For example, each mobile phone has a hardwired IMEI, and each SIM card stores an IMSI. Therefore, the Base Station can identify not only each unique phone, but the unique subscriber using the phone.

3.6 Tracking a Cell Phone using Third Party Apps

Apart from the Android Device Manager for android phones and iPhone function for iPhones, there are some third-party Apps used for tracking mobile phones. Once installed, these Apps use the built-in GPS technology of the mobile phone to track the exact location, calls, text messages, social media activity, medial gallery, emails, and browser history. Examples of these apps are Highster Mobile and Safeguarde.

Internet Protocol (IP) addresses are the unique numbers assigned to every computer or device that is connected to the Internet. Among other important functions, they identify every device connected to the Internet, whether it is a web server, smartphone, mail server, or laptop[14]. IP addresses enable our computers, servers, telephones, cameras, printers and sensors to communicate with each other even without human intervention.

As you surf the web, your device sends out this IP address to every website you visit. IP addresses are not fixed to a specific geographic location. Therefore, knowing that a particular Internet Service Provider is based in a particular city does not pinpoint a precise location[8] [10]. That is why we need Geolocation service providers that link each IP address to a specific location via their databases. Some geolocation databases are available for sale, while some can also be searched for free online [9].

4 Location-Based Advertising

Online shopping for products and services has become very popular because it has several advantages for both the consumer and businesses.

Table 4: Benefits of location information.

Advantages for the consumer	Advantages for the businesses
1) convenience of getting what you want in the comfort of your home or office	1) to reach more customers at once
2) Much easier and faster to compare prices and consumers' reviews.	2) to make new customers
3) You can buy from stores that are far away (even from other continents).	3) to increase their revenue

However, business have gone a step further in the search for higher revenues [2]. Online advertising has been enhanced from its more rudimentary beginnings through the advent of new technology. A great example is when you walk into a mall, your smartphone gets bombarded with promotional ads from stores nearby. This is known as location-based advertising.

Advertisers can personalize their ads based on the location of the consumer. This type of marketing is very effective because it happens in real time, while you are in the store. If you walk into a shoe store, you get ads about their specials for the week or day. The Ads are relevant because they target your interest. That is why if you are in a shoe store and you get an ad for furniture, you are more likely to ignore it because furniture is not relevant at that instant. The Ads are also personalized and targeted i.e. customized to suit the consumers.

For instance, if you are in a college town, or near a major university, advertisers will send you Ads that are more appealing to students. There have also been cases where business will offer certain discounted prices if there were competitors within a certain distance of the consumer.

Advertisers can also keep track of all our online activity and target us with relevant ad. When we install apps on our mobile devices, the companies claim that the

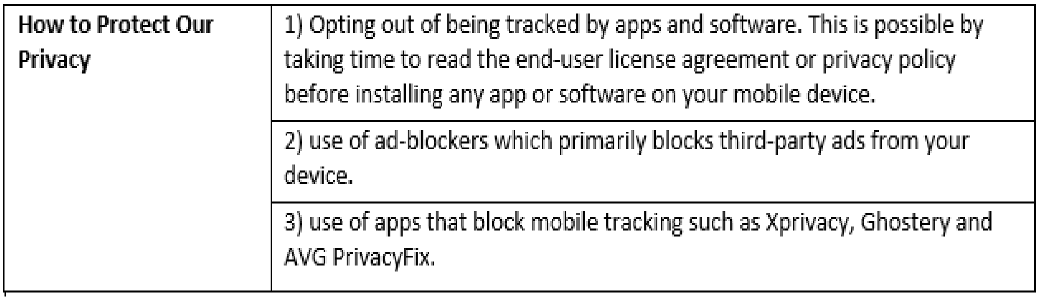
[14] https://www.icann.org/en/system/files/files/ip-addresses-beginners-guide-04mar11-en.pdf/

information they collect is anonymous which is not entirely true. For instance, advertisers can track several mobile devices like a smartphone, table, and a laptop to the same user. This is made possible by the data-specific identifiers like serial numbers on the devices or installation of software onto these devices. These coupled with any unique data that can be used to identify a specific connection like IP address leave the consumer prone to several privacy issues. It is noteworthy to point out that there are options to opt out of some of these device-identifying technologies but most of the public is not aware of them. Data is collected from a user's device as he/ she moves from one device to another and between websites. Once the advertisers figure out your interests, then they can target you more precisely and timely. Furthermore, companies can make a link between an internet user's social media accounts and their web browsing activity and sell it to any interested third-party [3]. Location-based advertising (LBA) can take a push or pull approach. Pull advertisement are those that show up after the mobile user has initiated a search for a certain item or service. Push advertisement are just messages to the customers based purely on their location. Of the two, push advertisement seems more intrusive and disruptive because they appear without the consumer's request or approval. LBA is a dream come true for the business but can be a privacy nightmare to the consumers

4.1 What can the Users do?

In order to regain our privacy, it is paramount to formulate ways to outsmart these location and privacy invasive technologies. Table 5 lists ways that consumers can accomplish this.

Table 5: Ways to Protect Our Privacy



How to Protect Our Privacy	1) Opting out of being tracked by apps and software. This is possible by taking time to read the end-user license agreement or privacy policy before installing any app or software on your mobile device.
	2) use of ad-blockers which primarily blocks third-party ads from your device.
	3) use of apps that block mobile tracking such as Xprivacy, Ghostery and AVG PrivacyFix.

Users can opt out of being tracked by taking time to read the end-user license agreement or privacy policy before installing any app or software on their mobile device. Do-Not-Track is only a proposed header, meaning that there is no standard telling companies how to interpret the signals. Therefore, it is currently up to each company to decide what to do when they receive a Do- Not- Track signal. Reportedly, most websites have not changed their practices yet and will probably not consider it until a standard is in place [16].

[16] https://allaboutdnt.com/Future_of_Privacy_Forum._ All_about_ do_not_track

4.2 Previous Work

The Social Media Platform experience involves several players including the SMP platform providers, users and advertisers. In a perfect world, each of the players would have clear privacy and safety protocols to keep information secure. Unfortunately, this is not the case due to lack of laws and regulations. It is particularly important to find out what the SMP users know and how they feel about privacy and protection of their information that they so freely share online. Several surveys have been conducted to determine just how well informed the public is about social media and privacy.

a) Social Media Use

Approximately 50% of Facebook users have accounts on each of the other (Google+, LinkedIn and Twitter) SMPs although the activity rate on these others is much lower. Facebook remains the most prominent with the highest activity rate and 57%, share information on special occasions. Less than 10% of the remaining social networks admit to sharing information more often than "rarely." here was about a 50/50 split between; "I only provide what is necessary" and "I provide what I want to" [6]. Fourteen percent of the respondents claim that they do not share personal information on the internet without realizing that their name (a requirement for some SMP) is considered personal information [5].

b) Privacy Policies

Every SMP that we use or App that we download has a lengthy privacy policy that we must accept to gain access to the service. Unfortunately, these privacy policies are poorly understood in part due to their length and language used. Figure 3 illustrates how well consumers read privacy policies before signing up for a profile page on social media.

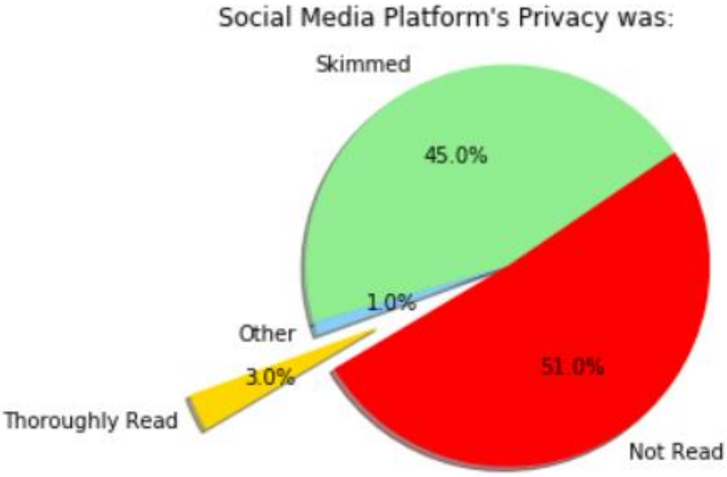


Figure 3: How many consumers read the privacy laws.

Interestingly, all 3% of respondents who have thoroughly read a privacy policy have an education of a bachelor's degree or higher and answered the question on privacy policies protect them as “false". They proved to have a good understanding of SMPs use of tracking mechanisms to provide tailored advertising and to offer better services. In contrast, among the respondents who believe that privacy policies protect them, 65%, have never read a privacy policy.

22% of respondents do not understand that privacy policies are neither obligated to protect user information nor act in the best interest of the user.

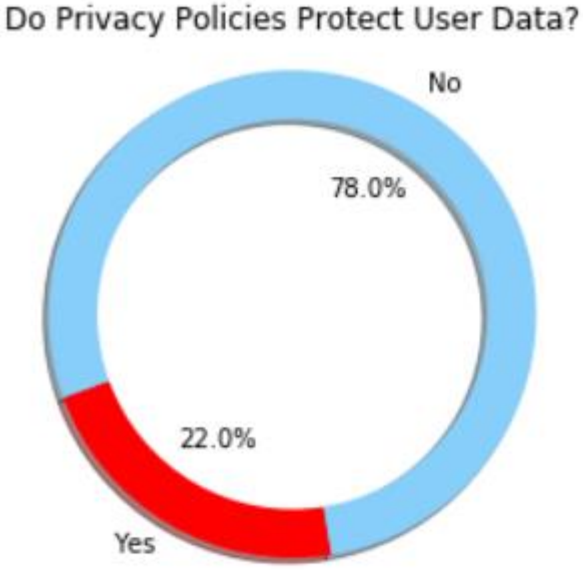


Figure 4: Do privacy policies protect data?

c) **Tracking Mechanisms**

Cookie profiling is one tracking mechanism that is still not well understood by many internet users. Some users think that cookies are used for encryption, storing of usernames and passwords, map their online activity or improve their browsing experience.

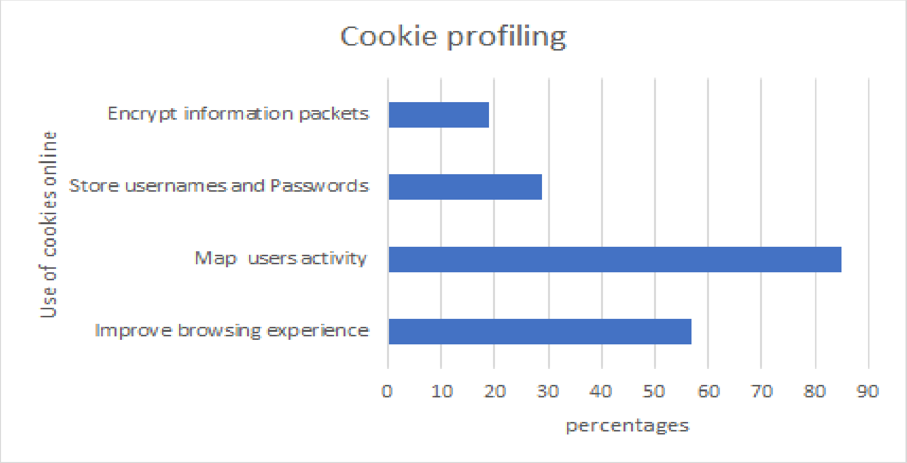


Figure 5: How cookies are used.

If the public does not view the use of cookies as a threat, then they don't feel the need to opt out of their usage. Even in the UK, 85% of respondents to a survey were not aware of internet cookie 'opt-out solutions. Additionally, 29% of those respondents who are aware of the 'opt-out" possibilities had not used them [13].

d)Trusting Social Media

Of the 2,000 respondents, in the Consumer Intelligence Study, only 10% feel they have control over their information and 25% believe their information is handled responsibly. However, 69% believe that companies are vulnerable to attacks and hacking. While 72% believe that businesses should play a bigger role than the government in protecting the consumer, 82% want the government to regulate how companies use data [17].

Emergence of Technology like machine learning, IoT and wearable devices has facilitated the exchange of information online. Internet experiences such as shopping have been improved by technologies such as IoT, data mining and machine learning. However, consumers believe that these technologies present more risk to privacy [11]. Wearable devices like Fitbit and Apple watch are convenient to use, they pay attention to us and our bodies and then communicate information to larger computing machines. These small devices have limited capacity and bandwidth and therefore less security. 42% of consumers consider these devices untrustworthy [12].

[17] https://allaboutdnt.com/Future_of_Privacy_Forum._ All_about_ do_not_track

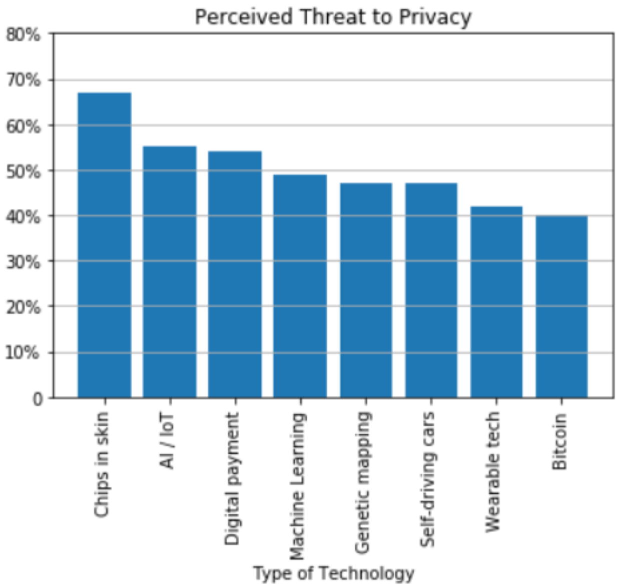


Figure 6: Main threats to our privacy

55% of consumers view Artificial Intelligence (AI) and Internet-of-Things (IoT) as a threat to privacy while 49% mistrust Machine learning (one of the applications of AI). Machine learning (ML) is the technique of developing algorithms to allow machines to learn from available data and then apply that knowledge to predict or forecast the future [18]. ML is used for better Ad targeting and on social media to connect users with people they may know, or facial recognition of any pictures uploaded on Facebook. Other uses of ML are refining of search engine searches and product recommendations like on Amazon[18].

[18] https://medium.com/app-affairs/9-applications-of-machine-learning-from-day-to-day-life-112a47a429d0

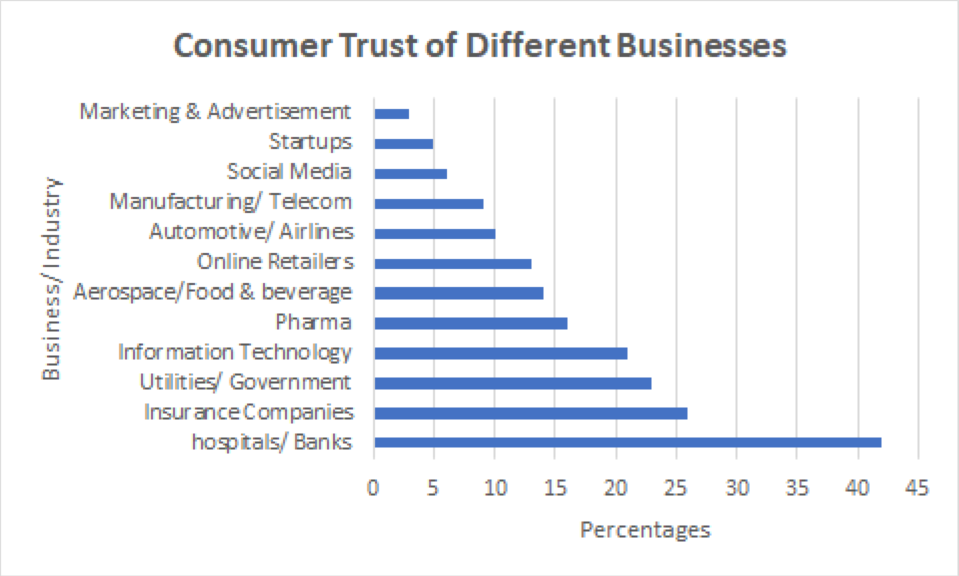


Figure 7: Which industries are trusted by consumers?

Consumer trust varies by industry, only 6% of the consumers trust social media while 3% trust Marketing and Advertisement industries. These are the two industries that we interact with during our online sessions.

5. Ethics

Privacy preservation is a vital factor for the widespread usage of LBS since location data can leak massive sensitive personal information such as whereabouts, daily habits, and real identities [21]. The fact that SMPs can now link an individual's browsing habits, interests and behavior to location information heightens the threat. Some internet users are aware that cookies are used to track their online sessions and browsing history. They are also aware that the information shared on SMP is collected by the companies. However, when this information is sold to a third party without the user's express knowledge or consent, then the question of ethics comes into play. For instance, If I take a photo while at a concert with friends and post it on social media, I expect that the SMP will store that data and metadata in their database. However, should another party get hold of that information, then I shouldn't I have a chance to permit or deny the sharing of that information. It is even worse in the case of my friends who I may have tagged on the photo. They may be violated by me, sharing the photo on Social media, the SMP that sells or gives access to this information and the third party that gets this information for their own purposes. In conclusion of this study, privacy must be understood primarily in terms of the general morality, not in terms of professional standards [22].

6. Conclusions

Social media use has grown exponentially in the recent past because of its low costs and wide reach to users worldwide. We set out to investigate the risks of using social media and the privacy, societal, and ethical implications. Although social Media users know that they are being tracked and their personal information is being gathered, they are not concerned enough to cease the use of SMP's. They do not appreciate the quantity of information they are revealing while online and how technology works to piece together every bit of information from our online activity. The users need to be more proactive about how to protect themselves and their information instead of leaving it all in the hands of the software companies and the SMPs. Consumers have very little trust in marketing companies and SMP's and it is important for the Government to enact laws and regulations to protect them.

Future work should investigate how the Government, marketing and Social media industries can work together to protect consumers without crippling the marketing and social media industries.

References:

(1) Threats of Online Social Networks Abdullah Al Hasib Helsinki University of Technology aalhasib@cc.hut.fi

(2) J. N. J. M. M. F. Jagatic, T. Social phishing. In Communications of the ACM Forthcoming (2006), 2006. www.indiana.edu/\~phishing/ social-network-experiment/ phishing-preprint.pdf.

(3) Prateek Joshi and C. –C. Jay Kuo. Security and privacy in online social networks: a survey

(4) T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer, “Social Phishing”, Communications of the ACM, October 2007

(5) Hannah Ersdal and Sølvi Svendby Skjærstad. Privacy and Social Media: Do Users Really Care?

(6) Hayes, Darren & Snow, Christopher & Altuwayjiri, Saleh. (2017). Geolocation Tracking and Privacy Issues Associated with the Uber Mobile Application.

(7) Khan, Salman & Ahmad, Waheed & Ali, Riaz & Saleem, Slman. (2015). A research on mobile applications for location tracking through web server and short messages services (SMS). 7. 2309-3978.

(8) Radhika Kinage1, Jyotshna Kumari2, Purva Zalke3, Meenal Kulkarni4. Mobile Tracking Application. Student, Department of Computer Technology, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra, India

(9) Jamie Taylor, Joseph Devlin, Kevin Curran. Bringing location to IP Addresses with IP Geolocation. School of Computing and Intelligent Systems University of Ulster, Magee Campus, Northland Road, Northern Ireland, UK Email: kj.curran@ulster.ac.uk

(10) Furey, E., Curran, K., Lunney, T., Woods, D. and Santos, J. (2008) Location Awareness Trials at the University of Ulster, Networkshop 2008 - The JANET UK International Workshop on Networking 2008, The University of Strathclyde, 8th-10th April 2008

(11) Rui Pedro Paiva, PhD Researcher @ Proyecto Prometeo, Ecuador Professor @ University of Coimbra, Portugal; May 2013. Machine Learning: Applications, Process and Techniques

(12) Ke Wan Ching and Manmeet Mahinderjit Singh. School of Computer Sciences,University Sains MalaysiaPenang, Malaysia. Wearable technology devices security and privacy vulnerability analysis

(13) Department for Culture. Media & Sport Research into consumer understanding and management of internet cookies and the potential impact of the EU Electronic Communications Framework/PwC_Internet_Cookies_final.pdf

(14) Hatoon S. AlSagri, Saad S. AlAboodi, "Privacy awareness of online social networking in Saudi Arabia", Cyber Situational Awareness Data Analytics and Assessment (CyberSA) 2015 International Conference on, pp. 1-6, 2015.

(15) FTC Staff Report: February_2009_Self_Regulatory_ Principles_For_ Online_Behavioral_Advertising/
https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-

commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf

(16) Electronic Engineering Times. How does a gps tracking system work. https://www.eetimes.com/document.asp?doc_id=1278363

(17) The GIS 2 GPS Portal. GPS definition, Gis2gps, updated 02/22/2018. [online]. Available: http://www.gis2gps.com/GPS/GPSDEF/gpsdef.html

(18) The Wireless Privacy Enhancement Act of 1999 and the Wireless Communication and Public Safety Enhancement of 1999. https://www.911.gov/pdf/Wireless_Communications_and_Public_Safety_Act_1999.pdf

(19) Dorothy J. Glancy. The invention of the Right to Privacy- Arizona Law Review/ http://law.scu.edu/wp-content/uploads/Privacy.pdf

(20) Alan Charles RaulPrivacy_Law_Review_2017/ https://iapp.org/media/pdf/resource_center/Privacy-Law-Review-2017.pdf

(21) Zhengang Wu, Liangwen Yu, Jiawei Zhu, Huiping Sun, Zhi Guan and Zhong Chen, “Privacy Protection against Query Prediction in Location-Based Services”, Institute of Software, EECS, Peking University, Beijing, China, IEEE, 2014.

(22) A. Y. Xue, R. Zhang, Y. Zheng, X. Xie, J. Huang, and Z. Xu, “Destination prediction by sub-trajectory synthesis and privacy protection against such prediction,” in ICDE (C. S. Jensen, C. M. Jermaine, and X. Zhou, eds.), pp. 254–265, IEEE Computer Society, 2013.

Footnotes:

1. The Statistics Portal aggregates statistics and studies from a broad range of sources and may be found at https://www.statista.com/.
2. The chart of worldwide social media users is available at: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/Statist_Number_of_social_media_users_worldwide_from_2010_to_2021_(in_billions) (accessed August 18, 2018)
3. http://press.careerbuilder.com/2017-06-15-Number-of-Employers-Using-Social-Media-to-Screen-Candidates-at-All-Time-High-Finds-Latest-CareerBuilder-Study
4. http://www.net-security.org/secworld.php?id=10208- Facebook users think social networking spam is a problem,
5. http://www.pewresearch.org/fact-tank/2014/12/04/ half-of-Americans-don't-know-what-a-privacy-policy-is/.
6. https://www.gps.gov/policy/legislation/gps-act/

7. http://www.pewresearch.org/fact-tank/2014/12/04/ half-of-Americans-don't-know-what-a-privacy-policy-is/.
8. http://www.gis2gps.com/GPS/GPSDEF/gpsdef.html/GPS_definition._Gis2gps
9. http://www.gis2gps.com/GPS/GPSDEF/gpsdef.html/GPS_definition._Gis2gps
10. https://www.icann.org/en/system/files/files/ip-addresses-beginners-guide-04mar11-en.pdf/
11. ttps://allaboutdnt.com/Future_of_Privacy_Forum._ All_about_do_not_track
12. https://allaboutdnt.com/Future_of_Privacy_Forum._ All_about_do_not_track
13. https://medium.com/app-affairs/9-applications-of-machine-learning-from-day-to-day-life-112a47a429d0
14. https://www.icann.org/en/system/files/files/ip-addresses-beginners-guide-04mar11-en.pdf/
15. https://allaboutdnt.com/Future_of_Privacy_Forum._All_about_ do_not_track