Privacy Issues with Unwarranted Data Collection from Web and Mobile Applications

A Research Paper Submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia – Charlottesville, Virginia

In the Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

By

Akanksha Alok

Spring, 2020

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed:_____ Akanksha Alok _____ Date_____04/12/2020_____
Akanksha Alok

Approved: _____ Richard Jacques _____ Date 4/30/2020
Richard Jacques, Associate Professor of STS, Department of Engineering and Society

Introduction

As our society has the potential to progress towards "smart cities" with built-in sensors and technological components integrated in all aspects of our daily lives, there are high risks of these systems being hacked and the collected data to be compromised. Researchers have already developed algorithms and detailed networks that will be able to keep track of all vehicles based on traffic cameras and sensors on the roads (Khan, Sargento, & Luis, 2017), and the hacking of this system can potentially put every vehicle-owner at risk. Despite this fact, there is no mention of how their vehicle data will be secured or safeguarded, and this is a clear indication that as a society, we are moving towards extensive data collection without the proper safety measures in place. As Brad Smith mentions in his book, "Tools and Weapons: The Promise and Peril of the Digital Age" (2020), "when your technology changes the world, you bear a responsibility to help address the world you have helped create", but as a society, we haven't been doing a good job with protecting consumer data or our basic privacy rights even though we have significantly increased the amount of data we generate and collect with the technology we have created.

In this paper, I will be exploring the ways in which a user's social media accounts, and web and mobile applications wrongfully elicit their personal information without their knowledge, and possible steps that we can take as a society to prevent this from happening. I have researched how certain data-collecting applications operate, and how the companies design them in a way to be hidden or disguised from the users. I have explored how different groups of people are impacted by the misuse of their personal data. This breach of privacy can affect almost every person on this planet, regardless of race, age, locality, or economic status, and can range from a person's name and email being stored in an external database to their entire identity being stolen (Irshad & Soomro, 2018). After thoroughly understanding the problem, I have

suggested ways in which we can solve this problem from a technical, legal, and social standpoint. I have looked into the existing rules and regulations provided by governing bodies of the United States on how data from these applications can be used and distributed, and have listed improvements to the laws in place for privacy in the technological realm. Most of all, I want to raise awareness among users of the potential dangers of sharing too much information online or on other online applications. As I have found solutions to a problem that will become more prevalent in our society as time passes and technology becomes more integrated in our lives, I have employed technological futurism to analyze whether these techniques will be able to persist in the future, before stating and supporting my suggested solutions to this problem.

Part I: How Applications Steal and Distribute User Information Wrongfully

Mobile applications, web applications and social media platforms are all responsible for stealing user information, and can either be solely created for the purpose of infringing on users' privacy or can be misused as an intermediate tool by third parties for stealing user data. In the sections below, I will describe some of the ways in which these applications and platforms have stolen or misused user information, but by no means does it extensively cover all of the ways that these technologies can infringe on our privacy, especially as hackers and malicious companies are constantly coming up with new techniques to secretly steal user information, and are finding new ways to circumvent the security measures put into place. Instead, I have covered the most prevalent ways in which consumer information is stolen and wrongfully disseminated, and hope that other malicious techniques which are similar in nature to the ones described can be mitigated by the readers' awareness.

Mobile Applications

Most of the research for mobile applications in this area are based upon Android applications, especially in terms of gaining unauthorized access into special user permissions on the mobile device. In one such research paper by Zhang et. al (2013), they created the platform, VetDroid, which simulated how mobile applications obtain access to special permissions to access sensitive system resources, such as the camera and other phone sensors, and how these acquired permission-sensitive resources are further utilized maliciously by the application. Several other mobile applications, such as SnapChat or other navigation apps like Google Maps, also rely on location permissions that are enabled by the user. However, third parties have hacked into these mobile applications and have taken advantage of the granted location permission, making the hacked users vulnerable to personalized attacks at any given time (Fisher, Dorner, & Wagner, 2012).

Another common technique used by mobile applications is runtime-information-gathering (RIG). In all of these attacks, a malicious app needs to run side-by-side with the target app to collect its runtime information. This type of attack is used on Android-based home security systems, where malicious apps can figure out when the house is empty and when the user is not monitoring surveillance cameras, and then proceed to disable the alarm delivered to the users' mobile devices (Zhang et. al., 2015). Another such example of this RIG attack is when these apps try to gain access to and misuse the virtual assistant applications, such as Siri or in the case of the research paper by Diao et. al (2014), Google Voice Search - an Android system built-in voice assistant module. The researchers simulated one of the attacks, called a GVS-Attack, in which the mobile app gained unwarranted access to utilize the Google Voice Search, and with Android Intent mechanism and the VoicEmployer module, they brought Google Voice Search to

the foreground, and played prepared audio files, with commands such as "call number 1234 5678", in the background. Google Voice Search then was tricked to recognize this as a voice command and performed corresponding operations. In a similar manner, these GVS-Attacks also have the potential to store texts and emails, access privacy information, and transmit sensitive user data and without user permission.

Web Applications

In terms of malicious web applications, the two most prevalent techniques of stealing user information are through malware or phishing attempts.

Malware is malicious software that is written with the intent of compromising a system and stealing the data available on the system. These programs perform a variety of functions, but mainly steal or delete sensitive data and secretly track the user's activities. Many web applications distribute fake or pirated software or operating systems, which often come with malware, once downloaded by the user. There are three main types of malware that are involved with infringing on the user's private information: trojans, spyware, and keyloggers. Trojans disguise themselves as legitimate software, while creating backdoors within the security of the system to let attackers remotely monitor the activities being performed by the user of the system. Similarly, spyware also hides itself within the background of a system and tracks everything the user does online - storing passwords, credit card numbers, and user web-surfing habits. It has the ability to do anything from recording the screens and websites the user visits, video-graphing the user from the webcam, to even recording user conversations through the microphone. Finally, keyloggers are a subcategory within spyware, in which it simply records the keys the user types and the places online where the user has typed them. From this information, attackers can

analyze the keystrokes to find a user's passwords, private emails and chats, and other private information (Johar, 2017).

Phishing involves the distribution of fake emails which often redirect to malicious web applications that wrongfully steal user information by manipulation. These emails appear to come from a legitimate source, and try to create a sense of urgency to trick users into giving out their personal and private information to another source. Often times, the phishing emails contain links that guide users to a fake web page. For example, the link may redirect a user to a fake bank website, and if the user falls for the scheme, they will end up sharing their bank account details which will actually be stored on the hacker's server (Johar, 2017).

Social Media Platforms

Social media platforms often operate as mobile and web applications, and can be misused by hackers by some of the aforementioned techniques. For example, a keylogger malware, known as the Pony botnet, affected the Facebook, Google, Yahoo social media platforms by breaching 2 million users' accounts by stealing their authentication credentials upon login, and then used this information to discreetly pull personal data from users' online friends and colleagues (Lake, 2018). Certain phishing sites have also popped up on social media platforms, where these fake websites will urge users to change their passwords but will instead steal login information ("How Cybercriminals Target Social Media Accounts").

The information from these social media platforms are also heavily leveraged by third party companies, and hackers often have an easier time attacking the poor security measures put in place by these smaller companies using the data. For example, on May 20, 2019, more than 49 million Instagram influencers, celebrities, and brands had their private contact information

exposed after an India-based social media marketing company, Chtrbox, left data scraped from Instagram unprotected on an Amazon Web Services database (Whittaker, 2019).

While Instagram was not directly responsible for the data breach above, they were still held accountable for not informing the users of Instagram that their data was being shared with this Chtrbox application. These social media platforms are often involved with mishandling or disseminating user information to these third parties without proper consent or permission from the users themselves. Perhaps the biggest and latest scandal to date was the Facebook – Cambridge Analytica data scandal, where Cambridge Analytica was working for United States Senator Ted Cruz and using data harvested from millions of people's Facebook accounts without their consent ("Facebook's data-sharing deals exposed", 2018). This was a major eye-opening moment for the American public, where they realized that their information was not being kept secure and safeguarded by these social media companies. In fact, other articles and journals indicate that Facebook has been selling user information to other companies for financial gains, such as Microsoft's Bing search engine being able to see the names of virtually all Facebook users' friends without those friends' consent, in order to personalize the results for the user. Netflix, Spotify and the Royal Bank of Canada were also able to read, write and delete users' private messages and see all participants on a chat thread in Facebook ("Facebook's data-sharing deals exposed", 2018). These are only a few ways in which these social media companies have been haphazardly disseminating our information, affecting thousands of unaware people who are on these platforms.

Part II: The People Affected

In this day and age, people are extensively reliant on different web and mobile applications and social media platforms as a form of entertainment, news, communication, or ease in their lives. Since there is such a wide variety of applications available to us, especially in the past decade with the rise of the Internet and creation of smartphones, there is a global audience of all ages, backgrounds, ethnicities, and socioeconomic statuses that can be negatively affected by a data breach on these applications. As our society shifts towards an increasingly technological one, more user data for this audience will be collected and these security and privacy problems can impact more people to a larger degree.

Data breaches during the past year on popular web and mobile applications, as well as social media platforms give insight into the wide range of people whose information has been wrongfully stolen or disseminated. On January 16, 2019, a flaw within the popular video game, Fortnite, exposed players to being hacked. The game has 200 million users worldwide, including minors and teenagers (Sobers, 2020). Similarly, personal information of current and former faculty, students, staff and student applicants of Georgia Tech University were accessed by a hacker through a central database on April 2, 2019 (Sobers, 2020). The database affected by the breach contained names, addresses, Social Security Numbers and birth dates of 1.3 million individuals and was the university's second breach in less than a year. On September 27th, 2019, the food delivery service, DoorDash, confirmed a data breach through a third-party vendor exposing the information of 4.9 million customers, delivery workers, and merchants (Sobers, 2020). These cases indicated the widespread reach of these data breaches, regardless of the type of application.

However, the users of these applications aren't the only people affected by these data breaches. As mentioned before, several social media platforms and other web and mobile applications are wrongfully used as intermediaries for stealing user information by malicious third-parties. Not only do these companies suffer financially due to lawsuits, but the consumers also lose trust in these applications and companies. Based on a recent survey, sixty-five percent of people have lost trust in Facebook, and demand the company to disclose how it uses the information that they collect (Edwards-Levy, 2018). Employees at these companies are also being tasked with extra responsibilities for security even when they don't have expertise in the area. In fact, the study done by Acar et. al (2016) shows that companies are increasingly assigning each developer involved in the mobile application development cycle a specific role in implementing the security measure for ensuring user data safety, despite having no security knowledge. While the emphasis on security is beneficial, having inexperienced people working on these matters creates additional problems and can have more negative outcomes than positive.

Finally, the US Government's systems have also been infiltrated by external sources several times in the past few years. In the Office of Personal Management data breach in June 2015, the United States Office of Personnel Management (OPM) announced that it had been the target of a data breach targeting the records of as many as 4 million people, with the final estimate of stolen records to be approximately 21.5 million. This included records of people who had undergone background checks, including current or former government employees, and this breach has been described by federal officials as one of the largest breaches of government data in the history of the United States. Chinese hackers had been able to succeed in this attack by employing malware in the OPM network, and collected personally identifiable information, such as Social Security numbers, names, dates and places of birth, and addresses (Chandler, 2015).

Not only did this breach impact government officials and employees, but it also put our nation's security at risk, and can pose a risk going forward, as our confidential information is increasingly being stored online. Based on these scenarios, we need the technical, legal and societal sectors to cooperate and work together to find a solution to this problem, as all three sectors are facing heavy losses in the face of data breaches.

Part III: Technical Solutions to the Privacy Issue

With the increase in data breaches, it is imperative that there be some countermeasures integrated with these web and mobile applications to prevent them from stealing user information or from being used as tools by third parties to do the same. While there are countless anti-malware, anti-phishing, and anti-virus software available for web applications that seem to work against these attacks, research shows that the software fails to prevent them up to forty percent of the time, especially on social media platforms. Most research in this area focuses on creating better protective software, and software than can work across several new platforms, such as the Cloud network, like the CloudAV anti-virus software does (Malwarebytes, 2018). However, they are still in development and require a great amount of testing, since most intrusions are novel and can come from any source.

On the other hand, there seems to be no proper preventative measures for mobile apps, yet. While there are a few solutions in the works, they have yet to be tested and adapted by the public. One such solution is the TISSA system, which creates another privacy mode on an Android phone that can empower users to flexibly control what kinds of personal information will be accessible to an application. This granted access can be dynamically adjusted at runtime

in a fine-grained manner to better suit a user's needs in various scenarios, and allows for an additional layer of privacy (Zhou et. al., 2011). Another innovation was App Guardian, which thwarts malicious app's runtime monitoring attempt by pausing all suspicious background processes when the target app is running in the foreground, and resuming them after the app stops and its runtime environment is cleaned up (Zhang et. al., 2015). This is a direct solution to the RIG technique used by malicious apps described in the section before.

The researchers working on these solutions should be granted full support, in order for these innovations to be foolproof and ready to use against any attack.

Part IV: Legal Measures that Need to be Taken to Resolve this Issue

Current Privacy Regulations in the United States

In the United States, the Federal Trade Commission (FTC) has handled privacy and electronic commerce since 1914, with the enactment of the Federal Trade Commission Act. The current guidelines from the FTC only pertain to web applications, and expects that commercial websites that collect personal identifying information from or about consumers should be required to comply with the four fair information practices: Notice, Choice, Access, and Security ("Privacy and Security").

Practice	Details
Notice	Web applications should provide clear notice of their information practices, what information they collect, how they collect it, how they use it and whether they disclose it to others.
Choice	Websites should offer the users choices as to whether their personal information can be used beyond the purpose for which it was provided.
Access	Web applications should offer users access to their information that a website has collected about them so the consumers could correct or even delete information.
Security	Websites should take reasonable steps to protect the security of the information they collect.

Figure 1: FTC Four Fair Information Practices. The table goes into further detail as to what each practice entails ("Privacy and Security").

These rules and regulations seem to work in favor of protecting user privacy, at least on the web application front. In fact, a few other federal laws have been passed in order to protect user privacy since 1914, such as the Electronic Communications Privacy Act (ECPA), which protects certain wire, oral, and electronic communications from unauthorized interception, access, use, and disclosure as well as the Computer Fraud & Abuse Act (CFAA), which makes computer-related activities involving the unauthorized access of a computer to obtain certain information unlawful (Steinke, 2002).

However, in 2000, the FTC conducted a survey of commercial web applications and their privacy practices. They found that most websites (up to 97%) collect personal information about consumers, 88% of the randomly selected web applications posted at least one privacy disclosure statement, yet only 20% of the web applications followed some part of all four fair information practices. Only 41% of the sites of their random sample met the basic notice and choice standards in 2000, and as the Internet has grown over the past decade, this percentage is

bound to be only lower in this day and age (Steinke, 2002). Not only do these companies not abide by these laws, but there are currently no rules put into place specifically for mobile applications or social media platforms.

Companies in the United States fight against and find loopholes around these regulations, proclaiming that self-regulation will work. The lack of unified governmental control and regulation on these companies is emphasized in this article by O'Connor (2018) relating to our health information and how it is disseminated without our authority. The author claims that the Health Insurance Portability and Accountability Act (HIPAA), the United States' primary health privacy and security law, only applies to "covered entities" holding "protected health information." Separate privacy laws govern specific areas of the U.S. health-care system. For example, student immunizations and other school health records are generally covered by the Family Educational Rights and Privacy Act (FERPA), which was enacted in 1974, but sometimes overlaps with and contradicts the Children's Online Privacy Protection Act (COPPA), which does protect data, but only of children under the age of thirteen. Starting with California, which enacted the first data breach notification law in 2003, forty-eight states have also passed laws that require individuals to be notified if their information is compromised (O'Connor, 2018). This issue specifically highlights the lack of an overall national regulation, as these laws have different and sometimes incompatible provisions regarding what categories and types of personal information warrant protection, which entities are covered, and even what constitutes a breach per state. For example, notification requirements also vary, where New Jersey requires that the state police cybercrime unit be notified, while Maryland requires that the state attorney general be notified before any affected individual is (O'Connor, 2018).

Privacy Regulations in Europe

While the big technological companies, such as Facebook, Microsoft and Google, do not follow the laws and regulations in place in the United States due to lack of enforcement and unified national guidelines, they do follow the stricter rules put in place by the European Council (EU). The safe harbor agreement forces US companies doing business in the EU to adhere to a code of business practices that allows them to conform to the EU Privacy Directive while continuing to follow industry self-regulation with the FTC rules as a backup. Companies must certify to the Commerce Department that they will follow the regulations of the EU directive. If a company does not live up to the agreement, they would be subject to prosecution by the FTC for deceptive business practices (Steinke, 2002).

In order to standardize the protection of data privacy, the European Union in 1995 enacted the EU Data Protection Directive that took effect in 1998. The following are some of the requirements of the directive: an organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization and the types of third parties to which it discloses the information, an organization must offer individuals the opportunity to opt out whether their information can be used for a purpose besides the one for which it was originally gathered, each organization handling personal data must take reasonable steps to ensure its security and integrity, individuals must have access to their personal information and be able to correct it, corporations and governments are forbidden from using virtually any personal records for any purpose other than the original one, without explicit permission, and the personal data on EU citizens may only be transferred to countries outside the 15-nation blockade that adopt these rules or are deemed to provide “adequate protection” for the data (Steinke, 2002).

This act forbids the transmission of some consumer data to companies in countries that do not live up to the same stringent data protection laws. In particular, this directive would prevent data about EU citizens being sent to the US, because the US legal system does not have the necessary data protection laws (Steinke, 2002). However, the companies have complied to follow their rules in order to stay in business in Europe, especially with the passing of the General Data Protection Regulation (GDPR) in which the directive was turned into a regulation, which enforced these measures on a greater level.

Reform in the United States laws on Privacy

Most of the laws enacted by the EU seem to be in line with the guidelines from the FTC in the Untied States, in terms of content. The companies that do not abide by these guidelines in the US seem to be doing that in the European countries, and therefore, we know that they can follow them if these rules were enforced. Like the EU did in 2016 with the passing of the GDPR, our national government needs to make stricter laws with better enforcement and higher severity of punishment if they are not followed. Working with the technical and social sectors, the national government needs to come up with a cohesive, detailed and extensive plan that protects user privacy on web, mobile and social media applications.

Part V: Social Measures that Need to be Implemented by the Consumers

In the user study done by Irshad and Soomro (2018), they emphasized the fact that social media users do not realize that they are making themselves easy targets to crimes such as identity theft, when they irresponsibly and haphazardly share their information online. Similarly, Bilton (2010) published an article about burglars using information from Facebook statuses that their neighbors had posted, in order to coordinate their crimes with their vacation times. Data breaches

tend to generate a positive impact on users' tendency to get educated of the dangers associated with excessive information disclosure, and we have had many such scenarios in this past year itself. This awareness will eventually lead to controlled information sharing online, as recommended. On the other hand, social rewards and incentives make users want to share their information online, which overrides the fear of privacy concerns (Fatima et. al., 2019). As a society, the best way to prevent these attacks and keep the users engaged is to constantly raise awareness and reminders among all groups of people that we need to be careful in oversharing information online, be wary of the people and groups that we connect with virtually, and be fully aware of the types of attacks that are performed on web and mobile applications and social media platforms.

Even if the technical and legal sectors put their best foot forward, none of their positive changes will take effect if we as a society, are unaware and fail to take the proper steps against our information being stolen or misused.

Conclusion

The rise of data collection is inevitable in a society where technology is becoming increasingly integrated in our daily lives, and we need to ensure that our privacy is being upheld and that our information is not being collected wrongfully or without permission.

Through this paper, I have highlighted the common ways in which mobile applications, web applications, and social media platforms are used to collect user information without our consent and how they disseminate it to third parties. The paper describes the far-reaching consequences for almost all humans around the globe, as a result of these data breaches and

attacks. It emphasizes the problem for the readers, in an attempt to raise awareness and for them to recognize the different online attacks.

The second portion of the paper encourages the technical, legal and societal aspects of the problem and these three sectors to unite against the problem and come up with a cohesive solution. The technical sector, which includes the technology companies, engineers, and researchers developing advanced tools for the users to defend themselves from these attacks, must work with the legal sector, such as the national and state government, to find an effective solution with all fronts covered. The legal sector also needs to take a plan of action that aligns with the latest technologies and research to prevent any outdated or irresponsible actions on their end, and they need to come up with national legislation that is strongly enforced. Most of all, the social sector, which comprises of all users of the mobile and web applications and social media platforms, need to be proactive in sharing their information and be aware of their online actions, in order for the steps taken by the other two sectors to work.

References

Acar, Y., Backes, M., Bugiel, S., Fahl, S., Mcdaniel, P., & Smith, M. (2016). SoK: Lessons Learned from Android Security Research for Appified Software Platforms. *2016 IEEE Symposium on Security and Privacy (SP)*. doi: 10.1109/sp.2016.33

Bilton, N. (2010, September 12). Burglars Said to Have Picked Houses Based on Facebook Updates. Retrieved from https://bits.blogs.nytimes.com/2010/09/12/burglars-picked-houses-based-on-facebook-updates/

Chandler, A. (2015, June 14). The Hacking of Federal Data Is Much Worse Than First Thought. Retrieved from https://www.theatlantic.com/national/archive/2015/06/federal-data-hacking-worse/395807/

Diao, W., Liu, X., Zhou, Z., & Zhang, K. (2014). Your Voice Assistant is Mine. *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices - SPSM 14*. doi: 10.1145/2666620.2666623

Edwards-Levy, A. (2018, December 28). Most Facebook Users Don't Trust The Site With Their Data. Retrieved from https://www.huffpost.com/entry/facebook-users-data-trust-polling_n_5c267e13e4b08aaf7a904697

Facebook's data-sharing deals exposed. (2018, December 19). Retrieved from https://www.bbc.com/news/technology-46618582

Fatima, R., Yasin, A., Liu, L., Wang, J., Afzal, W., & Yasin, A. (2019). Sharing information online rationally: An observation of user privacy concerns and awareness using serious game. *Journal of Information Security and Applications*, *48*, 102351. doi: 10.1016/j.jisa.2019.06.007

Fisher, D., Dorner, L., & Wagner, D. (2012). Short paper. *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices - SPSM 12*. doi: 10.1145/2381934.2381945

How Cybercriminals Target Social Media Accounts. (n.d.). Retrieved from https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/cybercriminal-social-media.html

Irshad, S., & Soomro, T. (2018). Identity Theft and Social Media. International Journal of Computer Science and Network Security, 18, 43–55.

Johar, A. (2017, October 30). Internet security 101: Six ways hackers can attack you and how to stay safe. Retrieved from https://economictimes.indiatimes.com/tech/internet/internet-security-101-six-ways-hackers-can-attack-you-and-how-to-stay-safe/articleshow/61342742.cms

Khan, M. A., Sargento, S., & Luis, M. (2017). Data Collection from Smart-City Sensors through Large-Scale Urban Vehicular Networks. *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*. doi: 10.1109/vtcfall.2017.8288308

Lake, J. (2018, September 25). Pony: A Breakdown of the Most Popular Malware in Credential Theft. Retrieved from https://www.acunetix.com/blog/articles/pony-malware-credential-theft/

Malwarebytes. (2018, June 26). New Research: Traditional Antivirus Failed to Protect Nearly 40 Percent of Users Using Two or More AV Solutions from All Malware Attacks. Retrieved from https://www.prnewswire.com/news-releases/new-research-traditional-antivirus-failed-to-protect-nearly-40-percent-of-users-using-two-or-more-av-solutions-from-all-malware-attacks-300543625.html

O'Connor, N. (2018, January 30). Reforming the U.S. Approach to Data Protection and Privacy. Retrieved from https://www.cfr.org/report/reforming-us-approach-data-protection

Privacy and Security. (n.d.). Retrieved from https://www.ftc.gov/tips-advice/business-center/privacy-and-security

SMITH, BRAD, BROWNE CAROLE ANNE (2020). *Tools And Weapons: the promise and the peril of the digital age*. S.l.: HODDER & STOUGHTON LTD.

Sobers, R. (2020, January 28). 107 Must-Know Data Breach Statistics for 2020: Varonis. Retrieved from https://www.varonis.com/blog/data-breach-statistics/

Steinke, G. (2002). Data privacy approaches from US and EU perspectives. *Telematics and Informatics*, *19*(2), 193–200. doi: 10.1016/s0736-5853(01)00013-2

Whittaker, Z. (2019, May 20). Millions of Instagram influencers had their contact data scraped and exposed. Retrieved from https://techcrunch.com/2019/05/20/instagram-influencer-celebrity-accounts-scraped/

Zhang, N., Yuan, K., Naveed, M., Zhou, X., & Wang, X. (2015). Leave Me Alone: App-Level Protection against Runtime Information Gathering on Android. *2015 IEEE Symposium on Security and Privacy*. doi: 10.1109/sp.2015.61

Zhang, Y., Yang, M., Xu, B., Yang, Z., Gu, G., Ning, P., … Zang, B. (2013). Vetting undesirable behaviors in android apps with permission use analysis. *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security - CCS 13*. doi: 10.1145/2508859.2516689

Zhou, Y., Zhang, X., Jiang, X., & Freeh, V. W. (2011). Taming Information-Stealing Smartphone Applications (on Android). *Trust and Trustworthy Computing Lecture Notes in Computer Science*, 93–107. doi: 10.1007/978-3-642-21599-5_7