Social Media and the Loss of Data Privacy

Introduction

Even before the worldwide pandemic of COVID19 plunged us all into what seems like a dystopian society, individuals as well as organisations have been moving rapidly toward home working and greater interaction via social or business networking platforms. However, in our rush to collaborate and share, are we giving away our personal information to commercial organisations and Central Government? What are the implications of this and is it too late to take back ownership of our own personal data?

This paper is aimed at students and it explores several key issues surrounding data privacy including not only how legislation should protect us, but also how commercial organisations attempt to get us to give up our rights and why.

Finally, it makes some high-level recommendations as to how we, as students, may be able to protect our privacy.

The Issue

Most people now live their lives to a greater or lesser degree via the Internet. If you don't have an online presence, then you miss out on a lot of what is happening socially. Most students play computer games and interact on social media. Even before the COVID19 outbreak we were being set schoolwork online. COVID19 has not only accelerated the volume of our online interactions, it has also focused concerns as to how much of our personal data we are effectively giving away to commercial organisations. Below are some of these examples:

On-line Group Collaboration and Group Chat

Group chat applications have been around for a number of years and are widely used. Following the COVID19 pandemic use of these group chats, and now video chat groups have exploded within families, schools and business in an attempt to maintain 'business as usual'. As with the social media apps many of these apps under their terms and conditions have access to all of your messages, irrespective of whether they are private or public and appropriate or inappropriate. With this, they can monitor your messages or calls, photos and videos to ensure that people are safe and that no one is in any danger of getting hurt. This information may also be useful for police departments investigating criminal activity if granted access by a court.

Some of these on-line messaging platforms have accessibility to spy into your personal life based on how much of it you share using the platform. Whatever message, photo, video or call you send/make they too have access to it.

Mobile games

Some games can be extremely popular, sometime exceeding 100 million downloads. The vast majority of us ignore the privacy policy supplied when we begin playing this interactive game. However, if you actually look into what is being said, you are allowing the company to access your general location, details about your phone including the IP or MAC addresses. Although we should know this, we still let them do this as millions of us rush to play a highly anticipated game.

Looking into it with more depth, if you have accepted the privacy agreement, the company have now gained access to a few things such as mobile device identifiers (this is essentially your device ID), or your advertising ID (a unique identifier that allows mobile applications running on android operating systems (OS) to gather data about specific customers to improve both personalization and customer analytics), and also your IMEI (which uniquely identifies a device on a mobile network).

When comparing popular mobile games, there is a common pattern in their privacy policies: they store/ have access to your bank card details so you can buy "upgrades" or "packs" in the game. They can also track your location through your Google account or GPS which is a daunting thought as your location may have no relevance to any of the games. Furthermore, they have access to your device's IP address and MAC address as well as a unique in-game user ID so they can track and follow your progress in the game.

But have you ever asked yourself why these companies are so aggressive about collecting your personal data? Well, data can help the companies get to know their customers. From a business perspective, customers are the critical centre piece to a successful business. By collecting information on their customers' preferences, interests, behaviours and demographics (the data reflecting to a specific group of people in the population), they can improve the relationship between seller and customer and the services which they provide. This can be done by keeping track of customers purchases or placing cookies on your devices or their websites to track their online behaviours. This information is then used to better meet their customers' needs and focus and improve their product development efforts. Companies also use this information to help identify and block fraudulent activities by detecting unusual patterns in usage.

Fitness apps

Fitness apps are widely used by people looking to get in shape. These companies often say that they are very good at keeping your PII (Personally Identifiable Information) confidential, such as policies that states "we guarantee that your PII will only be used for contacting you and improving our services". However, once they have your PII, they again have access to your location and personal information including your name, date of birth and email address.

When comparing multiple fitness apps, they all have access to your location and your constant movement. Many of these health apps share your information with third parties and this may

not have always been made explicitly clear when you signed the usage agreement. There are anecdotal stories of insurance companies asking people to supply information from Fitness apps to assist them in making insurance decisions. This health data is very important to these insurance companies, as it helps determine which customers are low risk for life insurance and who is high risk (in other words, the likely profitability of an individual).

Moreover, fitness apps can access your GPS to track your jogging and cycling routes which they can then store and potentially share/sell it to third parties, marketing firms, advertisers in line with the data privacy agreement you have signed up to. This data allows those third parties to advertise and promote their products in more populated areas.

The Government Response

The Government aims to protect people against the misuse of your personal data by implementing laws. One of the most important laws is the General Data Protection Regulation (GDPR).

The European Union introduced the EU General Data Protection Regulation on May 25th 2018 and the Data Protection Act (DPA) 2018 is the UK enactment. The regulations showed great promise during development; they were intended to harmonize privacy and data protection laws across Europe. It was designed to help EU citizens to better understand how their personal information was being used and encourage them to file a complaint if their rights were violated. In greater depth the GDPR helps to increase the privacy of EU residents, as well as helping them understand use of their personal data. It also granted regulatory authorities' greater powers to take action against organisations or businesses that breach the data protection regulations. The GDPR also helps to generalise the boundaries for business's within EU countries, as they are all having to follow the same protection regulations making it harder for loopholes or schemes to appear.

Moreover, some may be concerned that Britain leaving the EU will affect the rules and regulations of this policy in Britain. However, there is a simple answer which is that it will not. The GDPR applies to all companies based in the EU and those with EU citizens as customers, therefore it will still apply to British companies or other businesses.

Conclusion

A famous quote states that "If you are not paying for it, you're not the customer; you're the product being sold" which has been attributed to numerous people. Commercial organisations do not develop social media apps for altruistic motives, they develop them to harvest personal information that can be sold for profit. It may be that we, as students, see this as an acceptable trade-off for the benefits that the apps provide. However, before we make these trade-offs, surely we need to know exactly what we are agreeing to and ideally the government should put

in controls to allow us to take back control of our data when we want to regardless of what rights we may have signed away in our rush to gain access to the latest app or game.

It is bad enough that commercial organisations are taking control of such vast amounts of our personal data, but how much more terrifying would it be if our own government did the same?