##### November 2021

## How social networking platforms sparked the Great Privacy Reckoning - or lack thereof

##### Alysha Maulidina, Sulthan Syuza Prabowo, Rizky Dimas Budi Ardiansyah, Christopher Owen, Jisu Kim

##### Computer Science, Binus International University

##### 

###### Background

Data privacy concerns the adequate handling of data - consent, notice and regulatory obligation - and the right of individuals to have control over how personal information is being used or collected. The rise of alerts about cookies and consent is the result of an ongoing debate over digital privacy, and the big question of who should own data and be responsible for protecting it.

###### Possible Threats and Privacy risk in Social Networking sites

Data privacy has proven to be challenging since companies must take into consideration the use of data without violating an individual's privacy preference and personal information. That is why, despite recent advances in data privacy laws and practice, consumer's privacy continues to be breached, compromised, and invaded by companies and governments alike. According to the Pew Trust, 13 percent of Americans have had their social media accounts taken over by an unauthorized user (Smith, 2017). And in the age where information is continuously shared everyday, social networking platforms pose additional privacy challenges.

Data mining is arguably one of the biggest social media threats. When someone visits social media websites, such as Facebook, it is common to see a pop-up or notification informing them that the page is using cookies to track them, and asking them to agree to let it happen. In said pop-up, it may prompt the user to read its cookie policy, and may tell them how tracking it "enhances" the web browsing experience. Cookies are text files with small pieces of data that are built specifically for web browsers to monitor and save personal information about users as they interact with the platform. Data collected from a user's cookies, amongst many other methods of data surveillance, are stored and leveraged by companies to better personalise advertising to their users. The problem arises, however, when companies share users' data with third-party entities, often without the users' knowledge or consent. Other forms of social media threats to privacy include, but not limited to: phishing (e.g. the 2019 phishing campaign targeting Instagram users to log into a false Instagram page), malware sharing and DDoS attacks.

The revelations about Cambridge Analytica, and its breach of Facebook data that kickstarted a privacy awakening around the world, demonstrated how private data from social media can be used to manipulate opinions for the benefit of a few. The personal data of 50 million users was taken without consent to build personality profiles to target US voters for the 2016 US election. And similarly, when the Russian government was accused of interfering in the 2016 election by using social media to spread "cyber-propaganda" and disinformation that started conflict and polarized users. These events have deteriorated public distrust and led some to argue if consumers have truly lost control over their own data.

When people register a new social media account, only few bother to read the lengthy terms of service, privacy policies and other agreements that often pop up on their screens. An experiment conducted by the European Comissions found that only 9.4 percent of consumers read the terms and conditions (European Commision, 2016). However, much of what is included in those terms often grants companies the right to track, use and sell personal information to third parties, as well as passive location tracking or harvest digital identifiers. This begs the question if companies such as Facebook should consider people's clicking of "Agree", to legal terms that an average individual may not comprehend, as deliberate and full consent.

###### Literature review

Online privacy has become an important part that we have forgotten day by day, people just click buttons without paying attention to what that button will do to your data once they get a hold of it, more and more software and websites are leaning towards collecting user data before asking them if we could. This can be demonstrated by a website called privacyspy.org, which lists a ranking of how safe your privacy is in a certain website or application. However, there are times when data collected by companies can become useful, an example of this is recommendations by the customers’ recent viewings.

When it comes to data collection there are few obvious outcomes, the good and the bad. Masts (2020) suggest that there are times when online data collection becomes essential, such as the COVID-19 pandemic when Apple and Google got together to make hotspots so that people would know which locations are dangerous. Another good example is when a company called Withings decided to collect data based on the sleep schedule when the quarantine is happening, which leads to some data that some of us might not even realize. However, there are also ‘The Bad’ when it comes to data collection. Masts stated that there are numerous breaches in 2019 alone, and that came from high-profile companies such as Adobe. Mental Floss (2016) can further clarify that by giving away user’s data it can lead to online thieves to steal personal information such as credit cards. Not only that, Masts (2020) states that Google might face an antitrust suit from the U.S Department of Justice due to how they use the data that is being collected. Google might even sell the data to other companies which correlates to Mental Floss’ (2016) statements, in fact, since data is very valuable, it might be huge sums of data.

These findings conclude that the data that is being collected are chipping away the users’ privacy. By collecting data and not protecting whilst anonymizing it, companies will be hurting its consumers by telling the world that they have very valuable data and are willing to sell someone’s private information to other companies.

###### Findings and discussions

The objective of this study is to investigate the drawbacks and benefits of a social networking site in data collection, given two main stakeholders: the social networking company and its users. We have chosen Facebook, one of the leading giants of social media, in our examination. Facebook has faced a number of privacy concerns in the past decade. But despite the recent revelations about the company's misuse of customer data, user growth and engagement continued to increase -- Facebook claims that the number of people who logged into its site at least once a month jumped 9% to 2.32 billion people since the Cambridge Analytica scandal in 2018 (Lee, 2019). According to Chadwick Martin Bailey, users became complacent about Facebook because information sharing through social media and making public details about personal information has become a part of people's life - 1.5 billion to be exact - suggesting that people care less about how social media might be collecting, sharing and using their information, and therefore expect less privacy. Like any other social media platforms, Facebook acts as a platform to provide emotional (the positive effect from finding, sharing, liking and commenting on posts), identity (connecting with others), and functionality (such as Facebook marketplace) benefits to users (Zilla-Ba, 2021). This relationship between people's intentions to disclose personal information vs. their actual personal disclosure behaviours is coined the term *privacy paradox* (Norberg et al., 2007).

Let's examine the user's privacy decision making processes, firstly their perception of risk. Research shows that "automatic judgement of risks (affect) and momentary feelings play a significant role in risk judgment and behaviour" (Nyshadham & Von Loon, 2014). Their findings suggest that people are more inclined to perceive risk through their intuitive feelings, driven by emotions such as joy, fear and danger (namely risk-based on feelings) instead of logical reasoning and scientific deliberation (namely risk-as-analysis) because it is much more slower, effortful, and requires conscious control. This explains people's behaviour that are contradictory in regards to privacy concerns.

As mentioned previously, complacency stems from the ever-growing trend of information sharing. People voluntarily disclose information because of the indirect ways in which sensitive information is collected (Namara & McGregor, 2019), mainly from the lack of knowledge in privacy policy. For example, the following phrase buried within Facebook's Terms of Service agreement states that "We collect information from or about the computers, phones, or other devices where you install or access our Services, depending on the permissions you’ve granted. We may associate the information we collect from your different devices, which helps us provide consistent Services across your devices." which among other device information, the company collects attributed such as operating system, device settings, device locations including "specific geographic locations such as through GPS", and connection information such as the name of user's mobile operator, timezone, language, phone number and IP address. Furthermore, in Facebook's Data policy, the company allows third party apps to receive information and access regarding a user's public profile and information of their interaction within Facebook. Because of Facebook's indirectness and lack of disclosure of how it collects and uses information, people are more willing to share sensitive information.

From the business perspective, private information is essential in drawing insight and meeting their customers' demand. By analyzing behaviour, companies can modify their digital presence and services to improve user experience. The F8 developer conference 2015 revealed three major sources where Facebook determines a user's news feed input: interaction with friends, content, and activities on a certain post. Facebook will try to fill in gaps in a user's profile page, such as interest, education, workplace, residing city, based on their activity and engagement as well as geotracking. According to Facebook, it uses cookies - small pieces of text file containing the user's browsing activity - for analytics and advertising as well. However, Facebook's biggest cash flow is targeted advertising - the company reported advertising revenue of $40 billion in 2017 (Wagner, 2018). In 2010, Facebook's CEO Mark Zucherberg stated that *"people have gotten really comfortable not only sharing more information and different kinds, but more openly and with more people"* (Menn, 2010). Paradoxically, people have seemed to have accepted the sharing of personal data with online companies in exchange for a personalised experience.

###### Conclusion and recommendation

Given the risk using applications and websites such as Facebook and Instagram pose, companies can do better to protect us and we can do better to protect ourselves. On one hand, some may argue that users should know what they expect companies are tracking about them. On the other hand, asking them to check a box when it is likely that they have a faint idea on what they're agreeing to doesn't seem to be an ideal solution. As for what companies can do, terms and conditions need to be reformatted as many are essentially huge walls of text that can both be difficult to comprehend and read in its entirety. As for us as users of these services we need to make 3 things common practice: password managers, 2FA, and private browsers. Password managers have the ability to generate passwords and manage your many passwords across many different accounts and will often recommend you to change weak or duplicate passwords. The second practice to always do is to set up two-factor authentication (2FA); with 2FA whenever you login to an account it will prompt you to enter a code that is sent to your email. This in turn would mean anyone trying to breach your account would need access to both something like your facebook or insta information and your email information. The last practice is to use extensions to improve your privacy while using the internet. Examples for this are uBlock origin which blocks ads and duck duck go which is a search engine that doesn’t track you like Google does. In the bigger scheme of things, law makers should consider crafting strict data and consumer privacy regulations that would control how data is used. For example, the EU's General Data Protection Requirements (GDPR) lay out rules for data collection, usage and sharing for companies, and it has been successful in the way businesses are disclosing their methods of capturing and analysing consumer data -- take, for instance, the increase use of cookie alerts when opening a new website on your device.

Despite precautions both users and companies can take to safeguard user privacy, there will always be a risk of a breach no matter how many steps are taken to do so. That is the unfortunate risk of using services such as Facebook and Instagram. However, far too many services take privacy too lightly and should do far more to protect us. In conclusion, while the users can take steps to minimise their risk when using services that collect data it remains mostly the responsibility of the companies that handle our data to ensure that the data remains safe. For now, people will continue to use services provided by Facebook, Instagram and other social networking platforms alike at the cost of their own personal data, it is not likely that they will change their behaviour towards privacy breaches anytime soon.

###### 

**References**

European Commision. (2016). Terms and Conditions Final Report. *Study on consumers’ attitudes towards Terms and Conditions (T&Cs)*, *-*(-), 175. https://ec.europa.eu/info/sites/default/files/terms\_and\_conditions\_final\_report\_en.pdf

Guynn, J. (2020, January 28). *What you need to know before clicking 'I agree' on that terms of service agreement or privacy policy*. USA Today. https://www.usatoday.com/story/tech/2020/01/28/not-reading-the-small-print-is-privacy-policy-fail/4565274002/

Lee, D. (2019, January 30). *Facebook users continue to grow despite privacy scandals*. BBC. Retrieved November 21, 2021, from https://www.bbc.com/news/business-47065972

Menn, J. (2010, July 28). *Technology and society: Virtually insecure*. Financial Times. Retrieved November 21, 2021, from https://www.ft.com/content/46250b7a-9a7a-11df-87fd-00144feab49a

Namara, M., & McGregor, S. (2019, May 11). *Why people continue to use Facebook despite the privacy scandals.* Medium. Retrieved November 21, 2021, from https://medium.com/@Namzo098/why-people-continue-to-use-facebook-despite-the-privacy-scandals-1914baa64524

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007, Summer). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviours. *The Journal of Consumer Affairs*, *41*(1), 100-126. https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1745-6606.2006.00070.x

Nyshadham, E. A., & Von Loon, G. (2014). An Affect Primary Framework for Privacy Decision Making. *Southern Association of Information Systems Conference Proceedings*, *-*(-), 9. https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2419533

Smith, A. (2017, January 26). *Americans and Cybersecurity*. Pew Research Center. Retrieved November 21, 2021, from https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/

Wagner, K. (2018, April 11). *This is how Facebook uses your data for ad targeting*. Vox. Retrieved November 21, 2021, from https://www.vox.com/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg

Zilla-Ba, K. (2021). *Why We Still Use Facebook Despite Privacy Concerns*. Chadwick Martin Bailey. Retrieved November 21, 2021, from https://www.cmbinfo.com/insights/why-we-still-use-facebook-despite-privacy-concerns/

Mast, S. (2020, June 23). *Council post: Data collection: The good, the bad and the ugly*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2020/06/24/data-collection-the-good-the-bad-and-the-ugly/

*11 ways your online data is being used right now*. Mental Floss. (2016, August 26). https://www.mentalfloss.com/article/84790/11-ways-your-online-data-being-used-right-now.