Your Data is your Recourse

An essay about the ethical dilemmas surrounding data ownership and privacy

Group 94
Lukas Jigberg

Introduction to data science and AI - DAT405

Chalmers tekniska högskola

Mars 2022

Contents

1 Introduction

"X lives on *generic street*, forth floor, sixth door on the left and is currently living alone."
"X is not more searched for than any other. We have currently this month left out 0 information about him"
"With our new service can you find about X personal economy totally anonymous!"

These quotes are from the websites that first appear when googling any Swedish name. There is surprisingly many services that market themselves to knowing a lot about Swedish inhabitants and proudly display titles and quotes such as "Number 1 in knowing people facts" or "Best to know about people". 20 to 30 years ago would it be weird if a stranger knew or could acquire personal information about anyone, like an address or number, but today would it be weird if the tools weren't available. The scary or scarier part however is not the fact that there is some basic information freely accessible by many, but rather that there might and probably is stored information about a person that infringes on their private life hidden, only accessible by some. Personal interests, favourite shows and shopping records all gathered and saved in hopes about learning more about the user. This information can't be seen and even if one could might he or she not understand it, but it is out there on a server waiting to be used or sold. This is a willing risk that internet and application users may or not realised that they take whenever they create an account, accept a cookie or simply visits a website.

2 Cookies

Cookies are nowadays a fundamental part of any website. Their task is to save user data to enhance future visits to the same website. For example, if the user chooses to pick a language will the "*website*" remember it, making it so that the user won't have to pick it again. It is however not the actually website that stores it but the users web browser. The data is saved in small text files, the "cookies", that can be deleted if wanted to. The website then simply receives the data once the user tries to access it. If this was the only way cookies could be used would there be no actually danger of data breaching.
There is a lot of types of cookies that hold more than just language settings on most browsers. Cookies for marketing, statistics and the infamous third-party cookie. These are cookies that belongs to a different service than the actually website that the user is visiting, these are usually the ones that cause the most problem and ride the line between ethics. Creating the problem that the user may give away their cookie data to a completely unknown party.
To stop or halt this problem was the ePrivacy Directive [1] created in the 2002 and put into action 2011 with new laws regarding data tracking, including cookie usage. The following is a summary from EU GDPR [2] information centre detailing the requirement to abide the law.

- Receive users' consent before you use any cookies except strictly necessary cookies.
- Provide accurate and specific information about the data each cookie tracks and its purpose in plain language before consent is received.
- Document and store consent received from users.
- Allow users to access your service even if they refuse to allow the use of certain cookies

- Make it as easy for users to withdraw their consent as it was for them to give their consent in the first place.

Allowing the user to decide themselves if the convenience on the website is worth potentially giving away data. Truth be told the contracts on most websites are often to long and complicated to be read easily. It is a nice option to have, but it becomes to inconvenient to read the terms and services of cookie on every website the users visits. Users usually just agree or disagree to the terms, which still doesn't fix the actually main issue of secret data gathering.

3 Profiling

With the data that is collected are profiles created. Much how a market company tries to understand its targeted audience do *unknown* website try to understand a singular user. Saving details and facts until a resume is formed which can be dissected to for example show the user a marketing poster that they would love clicking on. Marketing is the most common usage of our gathered data. Market companies earn more money by showing us ads that we are more likely to click on. Which is why its important for them to correctly calculate what a user might end up clicking on. If the user seems to be interested in dogs and their health the add company will send them adds about dog food and dog health cures. But could a user be add free if they totally avoided all cookies?

4 Application Gathering

A study done by Oxford University [6] (summarised and rewritten in article form by SurfShark [5]) ranks the application on smartphones to visualise and demonstrate which of them gathers the most unnecessary data. This is where the real problem lies, as most of the apps that gathers the most data for third-parties are the ones that are being used by most people. Meta's applications (Facebook, Messanger, Instagram), Googles (Gmail, Youtube, Chrome), Linkedln, Paypal, Wish, Klarna, Tiktok, Tinder and the list goes on. Even more disturbing is that intimate apps like Ovia a period tracking app and Grow Nurture a Pregnancy tracking app are among those who track the most data. Same for Metas and Googles children apps 'Youtube Kids' and 'Messenger Kids', they are supposed to be better alternative then their adult counterpart but still collects unnecessary data for the supposed reason to better entertain the user.
Many of the apps above claim that their data gathering is safe and doesn't affect the user at all, since they don't ask or use for their name, address etc, claiming that they remain anonymous. Tiktok is one of the biggest video and entertainment apps in the world and was created by the Chinese company ByteDance. Working under very different jurisdictions then the rest of the world did Tiktok first appear with a bang, showing immediate red flags about its users security. In a news report in 2020 by BBC [7] do they tackle the issue of how countries have been banning the app fearing that it is to unsafe for the country and its inhabitants. Believing that the app being Chinese does gather to much data and that Chinas laws and government doesn't do enough or anything to make sure that the data isn't used inappropriately. The news conglomerate BBC who made the video and done multiple article on the topic have since joined Tiktok creating and posting their first video 2020, proving that they saw less risk and more to gain on venturing on to Tiktok, strengthening the apps reputation and usage as it gains the worlds biggest news media as a content creator.

5 Risk and Venture

The BBC has never claimed that they wouldn't go on Tiktok and would do so only if they thought is what the right thing to so, "We're only going to go on to these platforms if editorially we think they're the right platforms to be on and we can create the content that would work on this platform and work for BBC News."[8]
The BBC had a similar instance back in 2014 when they joined the still growing app and network Instagram. Today is BBC the leading news covering content creator on Instagram which proves that there is a big audience for them on these risky applications. Proving a very necessary point on how all users and companies are faced someday with the choice if they want to stop following the trend band wagon and exclude themselves from the latest most popular technology subsequently being left behind, or subscribe to more data gathering services. BBC joined Tiktok because their was a new modern audience their and because other news outlets where already on it. Private users join Facebook, Instagram, Snapchat, Tiktok because its where the new large content is created and most users friends are already on it. Creating this domino effect where an application with a good concept keeps on gaining users as those users attract more users. Making an application with real visible drawback become sought after only because a majority of people has it.

6 Protection

If cookies and data service terms and condition are available for their user should there really be any problem? Every user can themselves choose if the venture outweighs the risk. If they are willing to give up personal data in favour of using an application. Don't like Facebook? Don't use it.
The problem isn't that there is a risk, but rather that the risk still remains unknown to most or is still purposely hidden. Similarly to the cookie issue, most users instantly accept the risk with an app without actually realising that there is one to begin with, adding unaware users to the domino effect some apps receive. Many also seems to believe that their personal information is safe due to the fact that their should be laws and restrictions against it, referring to GDPR and common decency laws in their respective country. GDPR[3] does incentives companies that receive European users to upheld the laws to not suffer costly lawsuit consequences, but its still okay to sell data to third-party members as long as that is mentioned in the terms and service of the application or website. Facebook for example states in their long overly complicated terms and condition document[4] that the user have the ability to choose to turn off cookies, their first-party cookies. A user can turn off the settings that remembers the chosen language but not that their data is being transferred to another company. Facebook also provides which companies uses the cookies and writes that you can 'say no' to them, this is not expanded on and there seems to be no information on how to do so.

This process of mapping where the users data wanders isn't water tight either as anywhere along that road can the data be *'stolen'* or simply illegally stored or sold somewhere else. This is the main doubt with Tiktok as many believes that China simply lacks the laws and services to properly maintain good data security. To reiterate GDPR only forces companies to properly show data usage and will not stop them from selling user information. GDPR ultimately gives the user the materials to decide themselves whatever they want to sell their own data to use an application.

7 Conclusion

The difficult part of personal data privacy that there is not clear standard for what is bad and what is good. Some users do know about what they give away and will happily do so others look for alternatives to the data hungry websites and apps. Its however pretty clear that most users doesn't care or realise what potential intimate security they are giving away. In a time where apps fight for user attention with popups and notices is it easy to see how our own data and attention has become a recourse. A valuable recourse that we can potentially loose forever if its not properly taken care of. To try and stop or halt the data gathering could we push for better data security initiatives. Teach people more of what they subscribe and use to make more aware that the world is going in a direction where personal privacy and the internet usage doesn't mix. Push for laws that tackle the source rather than controlling the middle man and spread awareness that the most used applications and website are those who should be trusted the least.

References

[1] EUROPEAN DATA PROTECTION SUPERVISOR, *ePrivacy Directive*, 2022. [Online]. Accessible: `https://edps.europa.eu/data-protection/our-work/subjects/eprivacy-directive_en`, Acquired: 2022-03-10.

[2] Cookies, the GDPR, and the ePrivacy Directive, *ePrivacy Regulation*, 2022. [Online]. Accessible: `https://gdpr.eu/cookies/`, Acquired: 2022-03-10.

[3] General Data Protection Regulation, *What is GDPR, the EU's new data protection law?*, 2022. [Online]. Accessible: `https://gdpr.eu/what-is-gdpr/`, Acquired: 2022-03-10.

[4] Facebook Cookies, *About Cookies for Facebook-pixel*, 2022 [Online] Accessible: `https://www.facebook.com/business/help/471978536642445?id=1205376682832142`, Acquired: 2022-03-10.

[5] Surfshark, *Uncovering the Apps That Actually Respect Your Privacy*, 2022 [Online] Accessible: `https://surfshark.com/apps-that-track-you`, Acquired: 2022-03-10.

[6] University of Oxford, *Third Party Tracking in the Mobile Ecosystem*, 2018 [Online] Accessible: `https://arxiv.org/pdf/1804.03603.pdf`, Acquired: 2022-03-10.

[7] The BBC, *What's going on with TikTok? - BBC News*, 2020 [Online] Accessible: `https://www.youtube.com/watch?v=98jZ_9BlDMY`, Acquired: 2022-03-10.

[8] The PressGazette, *How BBC News topped 20m Instagram followers - and why it has stayed away from TikTok*, 2022 [Online] Accessible: `https://pressgazette.co.uk/bbc-instagram-strategy-tiktok/`, Acquired: 2022-03-10.

Ps. I am now getting pregnancy test adds, thanks google