Adrian Zając

e-mail: adrian.zajac@protonmail.com

Wroclaw University of Economics
and Business

Developing Data Protection and Privacy Trends Reshaping the Business Landscape – The Case Study of Apple

DOI: 10.15611/2023.33.6.10
JEL Classification: F20, K30, O33

Abstract: The global pandemic has significantly accelerated the transition of our lives into the digital world. However, with the change, many new threats connected with data protection and privacy have emerged. Due to the fact that many jurisdictions have no or basic privacy laws in place, their citizens are at risk of becoming targets of companies and malicious entities who wish to access their data. This article examines the significance of the data, tracking methods, the threats to the privacy and the response of governments worldwide by analysing various proposed or enforced laws. The main focus was placed on the growing awareness of the problem by users, and the implementation of various techniques and tools to limit data gathering by third-parties. The paper analyses how different forces in the environment are reshaping the business strategies of companies. The subject of the case study is Apple, which has introduced many privacy-related solutions that have affected the market and their competitors.

Keywords: data protection, privacy, Apple, tracking, privacy paradox.

1. Introduction

Big Tech corporations all around the world can become a significant owner of individuals' online activities through mergers and acquisitions with other companies. This gives them the ability to gather a substantial amount of data that can be later used for marketing purposes and to better know its users. Apart from the market movements, todays companies have a variety of tools and methods that they can combine with the products and services that they are offering to be able to track and recognize the same user across multiple offerings.

When it comes to tracking Internet browser activity, one of the oldest and most commonly used techniques are cookies – small files placed in the browser storage whose main purpose is to remember the active user and provide authentication. However, some cookies can store more information about the user, such as behaviour on the website, searches, etc. The owner of the website can also introduce third-party cookies which are placed by the advertising or analytics companies, which by putting their cookies on multiple sites across the Internet can later distinguish the activities of the specific user, thus enabling them to create a profile with the user's interests, sell the data, etc.

Another type of trackers are pixels or web beacons that are loaded into websites in the form of a hidden image or hidden pixel by third-parties. When the website is loaded in the user's browser, the company behind the beacon can track the activities of the user across different sites that are using this technology.

The latest and most dangerous method is called fingerprinting – there are many different approaches to it, but such technology is trying to uniquely identify a person from other users on the Internet by downloading specific information about the monitor resolution, IP address, and location based on the keyboard and language settings and even similar behaviour. According to WhoTracksMe, out of the 6000 top websites 1308 have at least 10 trackers from different companies. The five most common trackers belong to Google, followed by Amazon, Facebook, and Cloudflare (WhoTracksMe, 2022).

The prevalence of different tracking technologies is dangerous for the privacy of users online. The article aims to present a holistic view of the issues connected with privacy, and the influence Apple has on the market. The paper presents the methods of tracking (such as the ones described above), the perception of privacy and the psychological impact of privacy abuse, actions from governments around the world to protect their citizens from exploitation, and how the users can protect themselves – either by holding companies accountable or by using different services. This theoretical background combined with the case study method was used to explore how Apple is changing the perception of privacy and how it influences its competitors.

2. Theoretical background

The data and privacy threats from malicious entities

Companies are sharing data with other companies who pay or provide some tools for obtaining information created by the user on certain websites. In some cases, as shown in Table 1, there are numerous third-parties that are gathering some unspecified data. The users are often unaware of the fact that when accepting the cookies prompts, they are not only allowing the owner of the website to place cookies in their browser, but also those of third-party companies. The data in Table 1 were gathered from the selected popular websites, using the OneTrust Cookie Manager with the Transparency & Consent Framework. The categories appear to be superimposed by OneTrust as they are reoccurring on the websites, as well as the fact that those in bold are set as "always active" and cannot be turned off by using the available buttons, but only by not consenting to the listed vendors.

As can be seen from this table, there are sites with robust cookie managers with numerous vendors, but there are also ones which use a relatively low number of third-party services. Nonetheless, there are companies available on various websites and are gathering data across them, and can also link them back to the user. The

Table 1. Analysis of third-party tracking companies on selected websites

Website	Categories of consent	No. of tracking third-parties	Exemplary information gathered
edition.cnn.com	Strictly Necessary Cookies, Performance Cookies, Targeting Cookies, Functional Cookies, Store and/or access information on a device, Personalised ads and content, ad and content measurement, audience insights and product development, Use precise geolocation data, Actively scan device characteristics for identification, **Ensure security, prevent fraud, and debug, Technically deliver ads or content, Match and combine offline data sources, Link different devices, Receive and use automatically sent device characteristics for identification**	30	Political and worldview opinions
webmd.com		399	Medical afflictions
dictionary.cambridge.org		82	Level of advancement in the language
tripadvisor.com		310	Vacation interests, social class
uk.indeed.com	Strictly Necessary Cookies, Performance Cookies, Targeting Cookies, Functional Cookies	18	Professional experience
Selected reoccurring third-parties on all websites above: Criteo SA; on all except Indeed: Yahoo EMEA Limited, Xandr Inc., Adobe Advertising Cloud, Oracle Data Cloud, Nielsen International, Amazon Advertising, Google Advertising Products, Sovrn Holdings Inc., Simplifi Holdings Inc., Adform			

Source: author's own work.

companies involved in such sophisticated tracking are called data brokers. The data gathered from public records and user's online activity are later sold to companies that wish to use such data for their own purposes. The profile of a user can contain much more information than even a close family member would know.

The privacy paradox and ramifications of privacy abuse

The privacy paradox is the contrast between how people intend to safeguard their online privacy and how they really behave online — and how they do not secure their information online. The term was created in 2001 in a report from Hewlett Packard, where it was observed that individuals fearing for their privacy were using loyalty cards from shops which were tracking their purchases and they were agreeing to it as long as it gave them some benefits (HP Laboratories, 2001).

The problem is that this phenomenon exists not because people are unaware of the unethical practices of the companies who gather data, but rather because of the fact the customers value convenience more than making the changes in the lifestyle to use the online services with privacy in mind. In one study, the participants

were presented with an IoT device and had their trust and privacy concerns measured. After using it, they were shown the evidence of the privacy violations and how much data the device was sending outside and their privacy concerns increased and trust decreased. However, one-third of them continued to use it, another third removed the personal information from it, and the rest only either made complaints on social media or to the manufacturer, or falsified the information. After one month of usage, their attitudes were the same as before the experiment (The Conversation, 2020).

Privacy abuse can have a range of consequences for the average user as the term itself is fairly wide – to help with the categorisation and understanding of such activities, Solove designed in 2006 the "Taxonomy of Privacy". He distinguished four main areas connected with the breach of privacy: information collection, information processing, information dissemination, and invasion (Solove, 2010). The Taxonomy (Figure 1) was further developed in his book published in 2010 – Understanding Privacy.

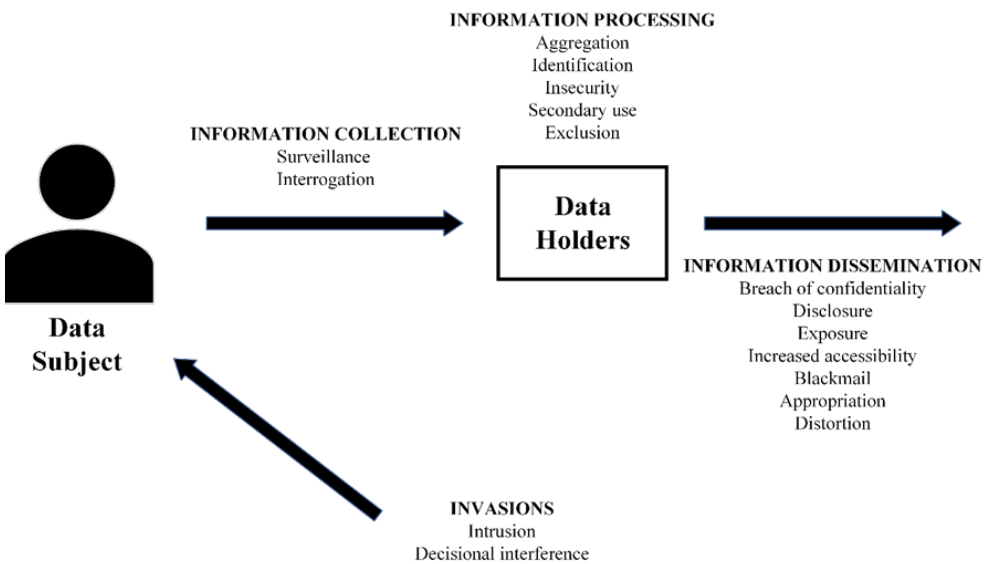

Figure 1. The Taxonomy of Privacy

Source: author's own work based on (Solove, 2010).

The implications of breaches of privacy are substantial. *Surveillance* can lead to self-censorship and inhibition and in the case of strict surveillance "impact freedom, creativity, and self-development" (Solove, 2006). People are less likely to attend certain rallies, speak publicly, associate with some groups and avoid public places. *Aggregation* leads to "increased power that others have over individuals" as such

processes can reveal the information about the person, not expected at the time when the singular examples of data were collected. Such data are subject to *distortion*, which in turn can lead to, for example, a lowered financial score in the banking system as the analysis was based on the incorrect data gathered on the individual.

Global introduction of comprehensive privacy legislation

The European Union's General Data Protection Regulation (GDPR) was the world's first comprehensive data privacy regulation. However, despite being groundbreaking, it has its flaws that make it less successful than assumed. The most serious problem is the lack of enforcement and cooperation between the member countries – the bodies meant to implement regulations are often underpaid and understaffed, which in turn causes a limited number of investigations that can be conducted (Brave, 2020).

In the United States, the State of California enacted the California Consumer Privacy Act (CCPA) in June 2018, and it came into effect on 1 January 2020 (IAPP, 2022). It is a comprehensive privacy law that gives residents of California residents the right to know about the information being collected by businesses and how it is used, and opt-out of the sale of their personal information (Attorney General of California, 2022). On 3 November 2020 a new upgraded version of CCPA – The California Privacy Rights Act (CPRA) was enacted with 56% of voters supporting it (Bukaty, 2021). When the CPRA comes into effect at the start of 2023, it will provide, among others, the right to data minimisation (not collecting more info than necessary) and right to receive notice from businesses intending to use sensitive personal information and to request that they refrain from it. The law also demands from businesses to provide more transparency around profiling and automated decision-making.

The European Union is working on a second overhauling privacy and data protection law called the Digital Services Act, or DSA. The new law will set an "unprecedented new standard for the accountability of online platforms regarding illegal and harmful content. It will provide better protection for internet users and their fundamental rights, as well as define a single set of rules in the internal market, helping smaller platforms to scale up" (European Commission, 2022). The new law, if adopted, will apply to a range of the providers such as intermediary services, hosting services, online platforms, and very large online platforms with each having different obligations.

New trends in societal privacy awareness

The history of the California Consumer Privacy Act described in the previous chapter shows the growing awareness of the importance of privacy protection. The initiative itself was sponsored by Californians for Consumer Privacy (CCP), an organization

that gathered the signatures of 629,000 Californians that resulted in putting it on the 2018 ballot. The same organization put forward a new initiative called The California Privacy Rights Act (CPRA), resulting in 9,384,625 Californians voting in favour of it in the November 2020 ballot (Ballotpedia, 2022).

The new trends are not only seen in the privacy laws around the world, but also in the online activity of users worldwide. According to data published by McKinsey, shown in Figure *2*, the majority of the answers are that a certain data type is an important or somewhat important part of the privacy for the respondents.

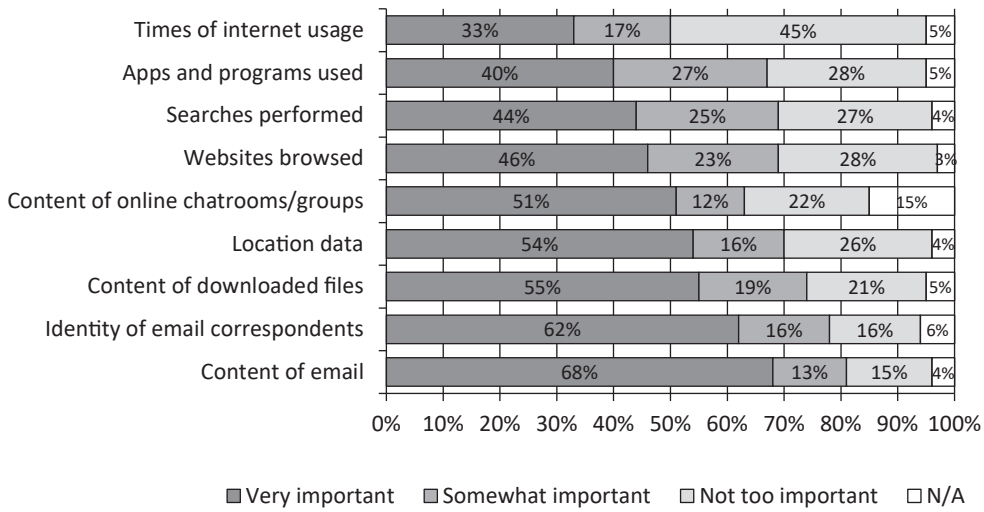

Figure 2. Relative importance by data type (*n* = 792)

Source: author's own worked based on (McKinsey&Company, 2020).

Due to the constant increase in the popularity of the services that protect the privacy of the issues mentioned in Figure 2, it can be concluded that people are taking matters in their own hands and are starting to look for solutions for their concerns. In the area of email communication, one can observe an increase in the usage of the encrypted mail services such as ProtonMail created in 2014. Starting from 5 million users in 2018 to 20 million in 2019, it now has more than 50 million users that are using an encrypted email app (VentureBeat, 2018; TheInformation, 2021). The encryption means that all the data in the mailbox can only be accessed by the owner itself and given that the application is open sourced it strengthens security of it as it can be audited by the security experts around the world. The company also recently introduced their own privacy-oriented and encrypted solutions such as Proton Calendar and Proton Drive that integrate with other Proton products, providing users with a multipurpose privacy platform.

Another category of the tools that observe an increase in the number of the users are Virtual Private Networks (VPN). It is an encrypted connection between a device and a network over the Internet. The encrypted connection aids in the secure transmission of sensitive data. It keeps unauthorised parties from listening in on the traffic and helps disguise the user when browsing websites.

In the area of web browsers, Brave is becoming increasingly popular. The browser is disguising itself as other browsers such as Chrome, which it makes it complicated to track its market share. The official data from the creators show that in 2017, Brave had only 1.2 million monthly active users, and 24.1 million in 2020, which more than doubled in 2021 with 50.2 million users. On an average day there are 15.5 million active users (Brave, 2022). The browser offers protection against fingerprinting, trackers and ads, but also includes its own privacy respecting tools.

In the market of search engines, dominated by Google, one of the most known privacy advocating companies, DuckDuckGo, has created its own engine that has around 0.7% of the market share as of April 2022 (Statcounter Global Stats, 2022). The service does not track separate users, nor the content of their queries, so the company estimates that it has around 50 million users that are running around 100 million queries per day compared with 35 million queries at the beginning of 2019 (DuckDuckGo, 2022). If someone prefers Google-like search results with privacy in mind, another search engine – Startpage offers such a possibility.

For people interested in online security and privacy, there are resources developed by many creators and organizations that teach the basic and more advanced knowledge about the aforementioned topics. PrivacyTools.io is a website where users can find privacy-respecting alternatives to their current service that cover all aspects of their online activity (PrivacyTools, 2022). There are also alternatives to the aforementioned website, such as a guide called Awesome Privacy or The Hitchhiker's Guide to Online Anonymity.

Environmental pressure on privacy-respectful business strategies

A survey conducted by McKinsey clearly shows that companies whose business strategy is aligned with security and privacy of collected data are the most trusted ones (some answers were omitted from Figure 3).

Without the actions at legislatorial level, many companies would not have introduced data protections and limited data gathering to the level comparable with that enforced by CCPA or GDPR. From the privacy perspective, it can be observed how governments are establishing comprehensive privacy and data protection laws as already described earlier in the article. However, there are also examples of small industry-specific or category-specific laws, such as the latest one being reviewed in the state of California – The California Age-Appropriate Design Code that would, for example, force TikTok and Instagram to disable messages between children and adults they do not follow (5 Rights Foundation, 2022).

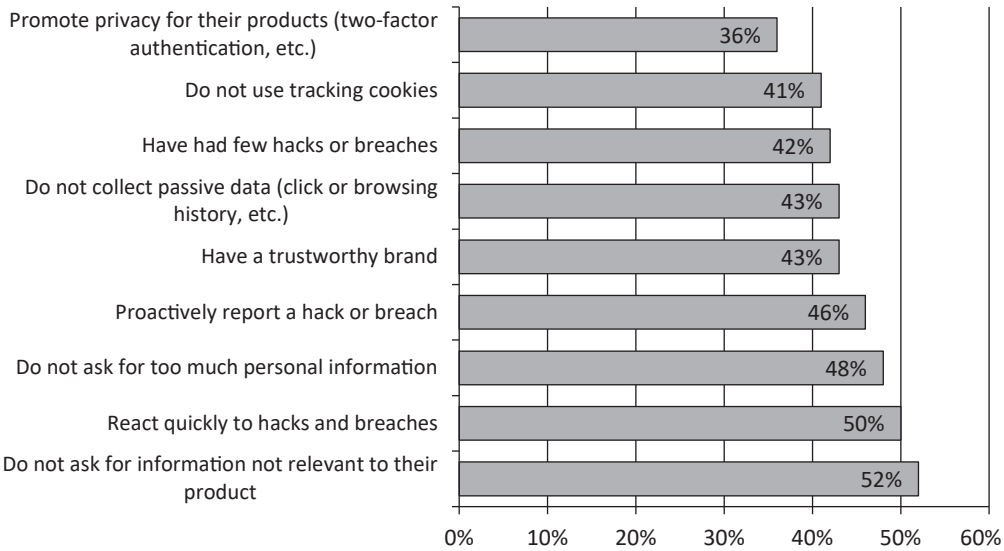

Figure 3. Survey on trust towards companies based on practices (*n* = 1000)

Source: author's own worked based on (McKinsey&Company, 2020).

Another targeted law and its enforcement that has recently caused headlines is Illinois's Biometric Information Privacy Act (BIPA) established in 2008. One of the businesses that claims to have captured more than ten billion face prints, Clearview AI, settled on 9 May 2022 that it will cease from selling its database containing biometric data not just in Illinois, but in the whole United States after the company was found in violation with BIPA.

A different example of the enforcement is the lawsuit against Meta (previously Facebook) by the Texas Attorney General for collecting data for commercial purposes without consent by using face recognition in filters. As a result, the filters stopped working for Texans and people in Illinois at the beginning of May 2022 to be later reintroduced with the opt-in prompt to avoid litigation from the state officials (The Texas Tribune, 2022). In Europe, after being fined by France's data protection agency at the beginning of 2022, Google changed its cookie banners that were allowing easier opt-in but harder opt-out for the users (The Verge, 2022). As a result, the company will introduce "accept all" and "reject all" buttons (previously not existent) to the rest of the European Economic Area, the U.K. and Switzerland (Google, 2022).

Pressure from the environment can be seen in the recent case against Amazon, as it has been already accused over misuse of biometric data, such as fingerprints or voice recordings, and is facing at least 14 class action lawsuits and more than 75,000 civil lawsuits (TechExplore, 2022). In February 2022 a judge approved a $650 million settlement with Meta over its use of the face recognition system

without users' consent that breached Illinois law (CNET, 2021). After the case was concluded, in November 2021, the company decided to shut down its facial recognition system and delete all the data (The New York Times, 2021).

Political actions and lawsuits are important tools in shaping privacy respectful business operations of the companies. However, some companies are innovating and follow a more privacy-oriented stance. This paper presented many tools that are being offered by companies to users, but there are tools created by the users for the users, such as the TOR network established in 2006 by The Tor Project, a US non-profit organization, to create a widely accessible network using the idea of "onion routing" (Jadoon, Iqbal, Amjad, Afzal, and Bangash, 2019). It works as a network of multiple servers called nodes, which route traffic and encrypt it each step of the way. A potential attacker or website can only see the last node through which the connection was made. The network consists of thousands of volunteer-run relays, with an average of 2-3 million users per day (Tor Project, 2022). Some companies have seen TOR as a possibility to increase their customer base and allow users to anonymously use their services. They include, among others, DuckDuckGo, ProtonMail, The New York Times, BBC News, ProRepublica, Facebook and the CIA.

The proactive approach to its user privacy can be seen in how Twitter decided to explain their privacy policy. At the beginning of May, the company released a game called "Twitter Data Dash" which explains different aspects of the company's new updated privacy policy rewritten to "move away from legal jargon" and allows users to adjust their privacy settings while playing (Twitter Safety, 2022). Such actions can shield a company against future lawsuits over the handling of the data and increase the trust that the users have in the company.

3. Research method

Due to the need to analyse the environment of the selected company and its influence, the qualitative research method was selected. The quantitative method was not be chosen as there were no data available that could help answer the research question, however some quantitative data were used in further considerations to strengthen the conclusions. From the available tools in this method, the case study is the most suitable one as it applies the idiographic approach to the research that takes into account different factors from the variety of fields presented in this dissertation (Newhart and Patten, 2018).

The aim of the case study was to explore the different solutions implemented by Apple in their products that protect privacy of their users to answer the following question: "How did Apple influence the perception of the privacy on the market and among the users?". The study analysed different privacy solutions offered by the company, the criticism regarding some of them, and how by using different marketing campaigns Apple presented itself as the privacy leader on the market. Moreover, reactions from the market and competitors were included to show how

the company by its products can affect the business strategies of other companies. The data were gathered using available public resources, such as reports, interviews with experts, official documentation from Apple, etc. ans there is no public access to specific usage and financial data. Some data came directly from the author who has hands-on experience with Apple solutions, however some observations might be subject to bias due to that fact. The analysed period covered all the years in which the company has been operating.

4. Research findings

This article has already explained the importance of data, how it is gathered and the threats the users face when online. It has also showed how different factors in the company's environment can influence its business strategy to treat data as private information that should be only gathered with the clear consent of the subject. There are not many companies on the market that promote themselves as security and privacy leaders in their segments. When it comes to portable devices, the best known company is Apple Inc., established in 1976 by Steve Jobs, Steve Wozniak, and Ronald Wayne, over the years becoming the industry leader in this area and thus having the upper hand over the competition. The company offers different series of products based on the price level to be able to attract as many customers as possible. Just in 2021, around 237 million Apple devices were sold with market share of 22% in Q4 2021 (CounterPoint, 2022) (Business of Apps, 2022).

The company has introduced new privacy features, some of them are described below (MacRumors, 2018, 2022):

- Intelligent Tracking Prevention (iOS 11.0) – active in Safari, uses Machine Learning to block third-party cookies and limits the life span of other data used to track users.
- iCloud Private Relay (iOS 15.0) – works similar to the TOR network by sending encrypted data through two separate internet relays. Works only in Safari.
- App Privacy Report (iOS 15.2) – report to show how many times the app used granted permissions, contacted domains and network activity.

The features described above since 2019 have been widely promoted using a marketing campaign called "Privacy. That's Apple", whose impact can be seen in the steadily rising interest with the term "Apple privacy" since 2010 in the Google search engine (Google Trends, 2022). The campaign started on 14 March 2019, with an ad showing humorous situations from everyday life where different aspects of privacy were seen in simple actions. It shows, for example, a person closing a curtain, window or locking doors. The ad lasts 46 seconds with upbeat, quirky music ending with the sentence: "If privacy matters in your life, it should matter to the phone your life is on. Privacy. That's iPhone" (WebArchive, 2020).

The second ad entitled "Over Sharing" has been published on September 3, 2020 on Apple's YouTube channel and shows different people sharing fairly private

information with strangers. The different examples are connected with the privacy features offered by the Apple apps such as Safari, Maps and Apple Pay. The ad ends with text that says "Some things shouldn't be shared. iPhone helps keep it that way" (WebArchive, 2020).

The third ad, "Privacy on iPhone | Tracked | Apple", explains the App Tracking Transparency feature and was published on May 20, 2021. It follows the life of Felix, who is being followed throughout the day by a group of strangers. Felix decides to turn on the option "Ask App Not to Track" on his iPhone, causing people around him to disappear. The scene is followed by the text "Choose who tracks your information and who doesn't" (WebArchive, 2020).

The latest ad was published on 18 May 2022, entitled "Privacy on iPhone | Data Auction | Apple" explains the term "data brokers" mentioned previously in the article. The main protagonist called Ellie is shown opening the door with a monitor showing "Ellie's Data Auction" with her picture. Behind the door there is an auction with her private data on sale. Ellie decides to press "Ask App Not to Track" on her iPhone, causing individuals on the auction to vanish. She also turns on her phone's "Protect Mail Activity" feature, and the text reads, "It's your data, iPhone helps keep it that way." (Apple, 2022). The videos, some no longer available online, according to Web Archive snapshots had 30, 26, 27 million views respectively, and the most recent one available on YouTube has currently 15 million views.

The advertisements are designed with simplicity in mind to highlight rather overlooked disadvantages of being online by putting them in the context of real-life examples. Such presentations of privacy issues with often unimaginable situations happening, e.g. Felix being followed by a group of strangers, puts the problem into perspective and is thought-provoking for the viewer. Apple tries to create the ads in a way that is at the same time amusing, with upbeat music, but also presents the problem in a memorable manner. When the viewer tries to understand the issue, Apple steps in with their own solution to use in their products that resolves the problem shown in the ad. Apple achieves with their ads the publicity needed for the buzz marketing of their products. The number of views might not seem impressive, but it is rare that someone watches the ad from their own will, and the number of YouTube views does not include the audience from the other sources.

Apart from the marketing campaigns, Apple offers users a wide knowledge database about privacy. Customers can navigate to Apple's page dedicated to privacy to view a detailed summary of the privacy and security features of their software and hardware that not only explains the different features of Apple applications but also warns and educates about different threats to the users.

The main value of Apple – privacy – incorporated in its business strategy, does not only affect its users, but also has an enormous impact on the competitors and the market itself. Meta (Facebook), the company known for gathering as much data as possible about the user's activity on the web, is a staunch opponent of the

Apple's App Tracking Transparency (ATT) feature and was heavily lobbying against it. In 2022, the company announced that the technology will result in $10 billion loss that year. When Facebook was severely impacted by ATT, Google noted an increase in ad sales, as it uses a different type of data than Facebook – customer intent in search queries versus data collected from tracking. Twitter was also able to mitigate the shockwave created by Apple's technology and noted increased revenue as their ads are focusing on brand advertising that does not immediately translate into sales (The Wall Street Journal, 2021).

Flurry Analytics has been tracking the statistics about Apple's App Tracking Transparency feature and as of April 2022, only 25% of the users worldwide, 18% in the US, have opted-in for tracking by the apps. In the first month since the feature was launched, only 11% of the users worldwide accepted tracking (Flurry, 2022). The growth can be attributed to the developers creating prompts asking people to allow tracking, and the benefits they will receive if they agree to do so. More devices running iOS 14.5 could also contribute to the growth.

Google, Apple's primary competitor, is widely seen as an anti-privacy firm that collects large amounts of data. This fact was highlighted in the marketing campaign discussed above. However, the popularity of Apple's solutions forced Google to introduce similar measures in their operating system – Android. Privacy Nutrition Labels in the Apple's App Store were launched by Apple in December 2020 and allow users to have a quick overview of the privacy practices of the developers and can be more detailed if needed. Half a year later Google announced that they will be implementing similar feature in their Google Play Store. Their version is called "Data Safety" and is based on the two main practices: data collection and data sharing. Google also introduced labels that are not present in Apple's version of the feature. Developers need to provide information as to whether an app encrypts data in transit to the servers, provide a way for the data to be deleted or has been verified against some global security standard (Google, 2022).

Privacy Nutrition Labels have a real impact on how users perceive apps in the App Store. According to one study, the app has lost on average around 15% of weekly downloads compared to Android's counterpart after the labels have been introduced. The change was even more noticeable with the more privacy intrusive applications. The research also points out that the most reactive were customers in the US and Canada (-20%) and the UK (-12%). The study also investigated the reaction of the 485 public companies active on the app market and concluded that the introduction of labels had the negative effect on the stock market, with a stronger reaction in the case of companies which rely on data collection (Bian, Ma, and Tang, 2022).

App Tracking Transparency is one of Apple's most sophisticated privacy measures deployed in their system. As it sparked a lot of attention worldwide, Google has decided to implement a similar technology in their operating system, however, the

timeline of the changes suggest that the company wants to delay it as much as possible. The feature will be called Privacy Sandbox and will be implemented in Android in 2024 or later. However, due to the many manufacturers of smartphones that use Android as the operating system and the different life span of updates for their devices, the change will take a few years to be deployed in an impactful number of smartphones.

However, like most companies, Apple has been a subject of a few controversies connected with privacy, dating back to Snowden's revelations in 2013 about the mass surveillance programme called Prism run by the NSA (US National Security Agency), in which Apple allegedly cooperated. Another major privacy and security controversy involving Apple took place in August 2021, when the company announced new features aimed at protecting minors that would automatically scan users' photo libraries in search for Child Sexual Abuse Material (CSAM). After receiving widespread criticism, it seemed that Apple decided to scrap its plans to adopt CSAM scanning, and instead introduced in iOS 15.2 Communication Safety features for Messages that will warn children and parents when any sexual photos have been detected. The company's privacy and security reputation was also damaged when revelations about Pegasus, spyware created by the Israeli NSO Group, emerged in the media in July 2021 stating that the tool was used to hack into potentially thousands of iPhone 11 and iPhone 12 models, even with the newest iOS updates. Two months after the revelations, the company patched the known vulnerabilities used by Pegasus with iOS 14.8 (TechRepublic, 2021).

Apple's App Tracking Transparency framework has also been the subject of criticism, as it was investigated by researchers who have found out in a study conducted in September 2021 that it does not change the number of trackers present in the app nor limit the data gathered by the app (Transparency Matters, 2021). The researchers accused Apple of creating the system on the same basis as Privacy Nutrition Labels, which is honour-based. The developers can choose not to share some information in the App Store, and in this way they can still track a user even after being asked not to. Apple does not check and validate the data provided by the popular developers or how the ATT is being circumvented, all of which can lead to people being given a false sense of security.

5. Conclusions

We are living in times when our digital life is a copy of ourselves – the data we share is being used not only to provide services, but also to gain monetary value from it. Companies have various techniques and technologies that can gather data in every device that is connected to the Internet. Many countries still lack comprehensive privacy solutions. Due to this absence of action, one can observe an increasing

interest in privacy respecting solutions and companies influencing the business strategies of companies that rely on gathering data about users.

The company examined in this article, Apple Inc., is without doubt the industry leader in terms of privacy, which has an impact on the environment. Its developments have a real impact on the revenue of other companies. It has been introducing different measures meant to safeguard its customers for years, with a significant increase in creating new features since the successful "Privacy. That's Apple" campaign was launched. This article utilises only publicly available data published by Apple and other researchers because the iOS system is close-sourced. This gives Apple control over the software and hardware, hindering the work of researchers who cannot independently confirm that the privacy measures are working as intended, and there is no hidden agenda in Apple's approach to privacy. Many entities have already accused the company of hypocrisy, the most recent being the discovery by a pair of iOS developers known as Mysk claiming that an identifier called DSID is collecting information about the user's actions in Apple apps without the option to turn it off, which is later used for internal ad targeting. Future research should focus on analysing how new privacy protections established by governments around the world are influencing privacy, and investigate the security of new privacy solutions available on the market, including Apple's own ecosystem.

Although Apple devices provide a strong foundation for the privacy of the everyday user, there are some fields in which the company should rethink its approach, but overall, its actions have an impact on the users, the market, and the competitors themselves. However, it should not be up to only one company and the will of citizens to secure their data, but every country should implement comprehensive privacy laws. Until then, people are left with using the tools provided by the privacy protecting companies and their own power to have their voices heard by the companies and their governments.

References

5 Rights Foundation. (2022, May 21). *We need to keep kids safe online: California has the solution.* Retrieved May 21, 2022 from https://californiaaadc.com/

Apple. (2022, May 18). *Privacy on iPhone | Data Auction | Apple*. Retrieved June 19, 2022, from https://www.youtube.com/watch?v=NOXK4EVFmJY

Attorney General of California. (2022, May 12). *California Consumer Privacy Act (CCPA)*. Retrieved May 12, 2022 from https://www.oag.ca.gov/privacy/ccpa

Ballotpedia. (2022, May 15). *California Proposition 24, Consumer Personal Information Law and Agency Initiative (2020)*. Retrieved May 15, 2022 from https://ballotpedia.org/California_Proposition_24,_Consumer_Personal_Information_Law_and_Agency_Initiative_(2020)

Bian, B., Ma, X., and Tang, H. (2022, February 06). *The supply and demand for data privacy: Evidence from mobile apps.* United Kingdom.

Brave. (2020, April 27). *New data on GDPR enforcement agencies reveal why the GDPR is failing*. Retrieved April 30, 2022 from https://brave.com/dpa-report-2020/

Brave. (2022, May 16). *Brave passes 50 million monthly active users, growing 2x for the fifth year in a row*. Retrieved May 16, 2022 from https://brave.com/2021-recap/

Bukaty, P. (2021). *The California Privacy Rights Act (CPRA) – an implementation and compliance guide.* It Governance Publishing.

Business of Apps. (2022, June 14). Retrieved June 14, 2022 from Apple Statistics: https://www.businessofapps.com/data/apple-statistics/

CNET. (2021, February 27). *Facebook privacy lawsuit over facial recognition leads to $650M settlement*, E. Moyer (Ed.) Retrieved May 22, 2022 from https://www.cnet.com/tech/services-and-software/facebook-privacy-lawsuit-over-facial-recognition-leads-to-650m-settlement/

CounterPoint. (2022, June 14). *Global smartphone market share: By quarter.* Retrieved June 14, 2022, from https://www.counterpointresearch.com/global-smartphone-share/

DuckDuckGo. (2022, May 16). *DuckDuckGo traffic*. Retrieved May 16, 2022 from https://duckduckgo.com/traffic

European Commission. (2022, 23 April). *Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment*. Retrieved May 15, 2022 from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545

Flurry. (2022, April 04). App tracking transparency opt-in rate – monthly updates. Retrieved from https://www.flurry.com/blog/att-opt-in-rate-monthly-updates/

Google. (2022, April 21). *New cookie choices in Europe*, A. Sammit (Ed.). Retrieved May 22, 2022 from https://blog.google/around-the-globe/google-europe/new-cookie-choices-in-europe/

Google. (2022, June 18). Understand app privacy & security practices with Google Play's Data safety section. Retrieved June 18, 2022 from https://support.google.com/googleplay/answer/11416267?co=GENIE.Platform%3DDesktop&oco=1#data_types&zippy=%2Cdata-types%2Csecurity-practices%2Cother-app-and-data-disclosures

Google Trends. (2022, June 19). *Apple privacy term interest*. Retrieved June 19, 2022, from https://trends.google.com/trends/explore?date=2010-01-01%202022-06-19&q=apple%20privacy

HP Laboratories. (2001). *Studying the Internet experience.* Bristol: Hewlett Packard.

IAPP. (2022, May 12). *CCPA and CPRA*. Retrieved May 12, 2022 from https://iapp.org/resources/topics/ccpa-and-cpra/

Jadoon, K. A., Iqbal, W., Amjad, F. M., Afzal, H., and Bangash, A. (2019, March 18). Forensic analysis of tor browser: A case study for privacy and anonymity on the Web. *Forensic Science International*, 59-73.

MacRumors. (2018, January 09). *Ad firms hit hard by Apple's intelligent tracking prevention feature in Safari*, J. Colver (Ed.). Retrieved from https://www.macrumors.com/2018/01/09/ad-firms-hit-hard-by-safari-tracking-prevention/

MacRumors. (2022, June 16). *iOS 15*. Retrieved June 16, 2022 from https://www.macrumors.com/roundup/ios-15/

McKinsey&Company. (2020, April 27). *The consumer-data opportunity and the privacy imperative*, H. Soller, J. Kaplan, L. Donchak, & V. Anant (Eds). Retrieved June 24, 2022 from https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

Newhart, M., and Patten, M. L. (2018). *Understanding research methods – an overview of the essentials.* New York: Routledge.

PrivacyTools. (2022, May 15). *Privacy guide: Fight surveillance with encryption and privacy tools*. Retrieved May 15, 2022 from https://www.privacytools.io/

Solove, D. J. (2006). A Taxonomy of Privacy. *In U. o. Revie*w, *154 U. Pa. L. Rev.* (477), 477-560.

Solove, D. J. (2010). *Understanding privacy.* Harvard: Harvard University Press.

Statcounter Global Stats. (2022, May 16). *Search engine market share worldwide*. Retrieved May 16, 2022 from https://gs.statcounter.com/search-engine-market-share

TechExplore. (2022, May 13). *Shareholder: Amazon's 'astronomical' misuse of customer data could ruin company,* L. Rosenblatt (Ed.). Retrieved May 22, 2022, from https://techxplore.com/news/2022-05-shareholder-amazon-astronomical-misuse-customer.html

TechRepublic. (2021, September 14). *Apple releases emergency patch to protect all devices against Pegasus spyware*. Retrieved June 18, 2022 from: https://www.techrepublic.com/article/apple-releases-emergency-patch-to-protect-all-devices-against-pegasus-spyware/

The Conversation. (2020, July 29). *The privacy paradox: we claim we care about our data, so why don't our actions match?* N. Aleisa, K. Renaud, I. Bongiovanni (Eds). Retrieved January 20, 2022 from https://theconversation.com/the-privacy-paradox-we-claim-we-care-about-our-data-so-why-dont-our-actions-match-143354

The Information. (2021, April 13). *How protonmail is fighting Big Tech*, J. Sisco (Ed.). Retrieved May 15, 2022 from https://www.theinformation.com/articles/how-protonmail-is-fighting-big-tech

The New York Times. (2021, November 2). *Facebook, citing societal concerns, plans to shut down facial recognition system*, R. Mac, H. Kashmir (Eds). Retrieved May 22, 2022 from https://www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.html

The Texas Tribune. (2022, May 12). *A Ken Paxton lawsuit is why some face filters on Facebook and Instagram were temporarily disabled in Texas,* R. Oxner (Ed.). Retrieved May 22, 2022, from https://www.texastribune.org/2022/05/12/texas-face-filters-instagram-facebook-meta/

The Verge. (2022, April 21). *Google gives Europe a 'reject all' button for tracking cookies after fines from watchdogs*, J. Vincent (Ed.) Retrieved May 22, 2022 from https://www.theverge.com/2022/4/21/23035289/google-reject-all-cookie-button-eu-privacy-data-laws

The Wall Street Journal. (2021, October 27). Why Apple's privacy changes hurt Snap and Facebook but benefited Google. Retrieved June 17, 2022 from: https://www.wsj.com/articles/why-apples-privacy-changes-hurt-snap-and-facebook-but-benefitted-google-11635375190

Tor Project. (2022, May 21). *Tor metrics.* Retrieved May 21, 2022 from https://metrics.torproject.org/userstats-relay-country.html

Transparency Matters. (2021, September 22). *Study: Effectiveness of Apple's app tracking transparency*. Retrieved June 18, 2022 from https://blog.lockdownprivacy.com/2021/09/22/study-effectiveness-of-apples-app-tracking-transparency.html

Twitter Safety. (2022, May 11). *We wanted to fit our Privacy Policy into 280 characters, but there's a lot here. And it's important.* Retrieved May 20, 2022 from https://twitter.com/TwitterSafety/status/1524404760262053889

VentureBeat. (2018, May 13). *How ProtonMail is pushing email privacy standards*, P. Sawers (Ed.). Retrieved May 15, 2022 from https://venturebeat.com/2018/05/13/how-protonmail-is-pushing-email-privacy-standards/

WebArchive. (2020a, May 02). *Snapshot of https://www.youtube.com/watch?v=A_6uV9A12ok&feature=youtu.be*. Retrieved June 19, 2022 from https://web.archive.org/web/20200502221734/https://www.youtube.com/watch?v=A_6uV9A12ok&feature=youtu.be

WebArchive. (2020b, September 03). *Snapshot of https://www.youtube.com/watch?v=A_6uV9A-12ok&feature=youtu.be*. Retrieved June 19, 2022 from https://web.archive.org/web/20200502221734/https://www.youtube.com/watch?v=A_6uV9A12ok&feature=youtu.be

WebArchive. (2020c, November 01). *Snapshot of https://www.youtube.com/watch?v=8w4qPUSG17Y*. Retrieved June 19, 2022 from https://web.archive.org/web/20211209180100/https://www.youtube.com/watch?v=8w4qPUSG17Y

WhoTracksMe. (2022, June 24). *Learn about tracking technologies, market structure and data-sharing on the web*. Retrieved June 2022, 24 from https://whotracks.me/

Zmiany w zakresie postrzegania prywatności przez użytkowników oraz przetwarzania danych osobowych przez organizacje – studium przypadku firmy Apple

Streszczenie: Globalna pandemia znacznie przyspieszyła przeniesienie naszego fizycznego życia do świata cyfrowego. Jednakże wraz z tą zmianą pojawiło się wiele zagrożeń związanych z ochroną danych osobowych i prywatności. Ze względu na to, że w wielu jurysdykcjach nie obowiązują żadne lub obowiązują tylko podstawowe przepisy dotyczące prywatności, obywatele są narażeni na ryzyko, że staną się celem firm i podmiotów, które chcą uzyskać dostęp do ich danych. W artykule badano znaczenie danych, metody ich pozyskania, zagrożenia z tego wynikające oraz działania rządów w tym obszarze. Główny nacisk położono na wzrost świadomości problemu wśród użytkowników oraz na rozwiązania ograniczające gromadzenie danych. Zbadano również, w jaki sposób różne czynniki z otoczenia firmy wpływają na ich strategie biznesowe. Przedmiotem studium przypadku jest Apple, które wprowadziło wiele rozwiązań związanych z prywatnością, wpływając tym samym na cały rynek i swoich konkurentów.

Słowa kluczowe: ochrona danych, prywatność, Apple, śledzenie, paradoks prywatności (*privacy paradox*).