REPORT ON DATA PRIVACY AND PROTECTION

Module: Technology and innovation Management

B00122875

Vimal Jaswal

TU Dublin - Blanchardstown Campus

Contents

Abstract

The digital age can be characterized by hyperconnected services. Whenever we use an app, which is usually provided by a platform, we are likely to engage with a wider set of actors. Precisely, we are engaged with an interconnected system service that poses specific regulatory challenges to personal data privacy and its protection. With the introduction of GDPR, we seek to understand its implications for privacy in such ecosystems. Interconnected services can provide the dissemination of personal data and thus impede individual's privacy rights. In this report I will elucidate the flow of personal information in service ecosystems by considering 'Facebook and Cambridge Analytica Scandal' case. In this report I will explain about digital services that leaked and misused information for political power and gains and violated democracy of public. I will shed some light on brief history of case, its implications and the steps taken by consumer advocates and data protection regulations by entertaining new laws to avoid such unethical issues in future. I would also provide recommendation based on my opinion.

Introduction

There have been several reports of Facebook having a major impact on the dissemination of personal data. These are connected by the fact that Facebook has illegitimately shared user data with at least 60 device manufacturers in data partnerships with different companies. In addition, Facebook shared information with apps, although this was previously revised technically and should prevent such critical transmission of privacy. The most controversial case that has become public can be called the case of the misuse of Facebook user data by Cambridge Analytica. The privacy - invasive access of data affected approximately 87 million Facebook users. This data was subsequently delivered to Cambridge Analytica, which placed targeted election advertisement on Facebook based on personality analytics.

Figure 1 : Facebook Cambridge Analytica Scandal

Source: Adapted from[8]

History and Background of Facebook and Cambridge Analytica

Mark Zuckerberg launched Facebook in Harvard on February 4, 2004 with his co-founders. Facebook attracts many hearts in Harvard university and soon it was expanded and open for other colleges as well. Facebook was being popular among millions of users by the end of year 2004 and was opened to anyone above age of 13years. Facebook added News feed in application in September 2006 with additional features to see friend's relationship, photos, groups in a news format. He then promised to give Facebook users better control of their profile and privacy in its use. Facebook launched Beacon service in 2007 to allow Facebook users share information from their shopping portals. Some liked it, and some criticised this feature. Beacon was shut down by Facebook in 2009 under a lawsuit filed. In 2009, Facebook made changes to make public information that users had kept as private such as Friends lists. Also, in 2009, the American Civil Liberties Union (ACLU) released a warning about Facebook quizzes. The warning includes this:

"Even if Facebook profile is private, when you take a quiz, an unknown quiz developer could access everything in your profile: your religion, sexual orientation, political affiliation, pictures, and groups. Facebook quizzes also have access to most of the info on your friends' profiles. This means that if your friend takes a quiz, they could be giving away your personal information too." In 2013 most of Facebook's revenue generated by mobile ads and the stock price rose again. [1]

In May 2015, Instant articles were introduced by Facebook, which contained content from the major publishers that they have been partnering with, so users need not click their newsletters and wait until articles are loaded. Facebook grew so rapidly that it takes much more than the Internet itself leaving behind information and communication technologies such as TV or film or radio. Targeted advertising was an important part of the business model of Facebook. Facebook advertised its ads manager. "You can target people who are right for your business with our powerful audience selection tools. You can connect to people like your clients using what you know about them–like demographics, interests and behaviour. You can choose your audience on Facebook with three options. Advertisers could manually select a core public based on age, location, interests, and behaviour, upload their Contact list on Facebook to connect with customers or use their customer information." Federal legislation prohibits advertisements which exclude people based on sex and other sensitive factors. Facebook was also accused in September 2018 of helping entrepreneurs to discriminate by sex by allowing women to be expelled from targeted advertising for employment. Targeted publicity was used by political campaigns to reach voters. Targeted political ads such as targeted ads as these were not trackable and monitored. Critics claimed that these ads could be used to encourage or suppress voting. In the UK, for example, the successful 2016 Brexit campaign examined targeted Facebook ads. [2]

Cambridge Analytica - a British consulting firm specialized for marketing and political campaigns. The company had a tagline "data drives all we do". "By better knowing your constituents, we achieve a greater influence while cutting overall costs," it promised for political campaigns. This enterprise which was largely financed by the US Republican donor Robert Mercer and co-founded by the former Trump advisor Bannon. It was revealed that Cambridge Analytica had collected and used personal

data of millions of Facebook profiles without their consent for political purposes. Aleksandr Kogan, Russian-American psychology professor, developed an app called –'This Is Your Digital Life' for Cambridge Analytica. Cambridge Analytica arranged a personality survey in which millions Facebook users participated. This app retrieved personal information of Facebook users and their friends. The Observer and New York Times reported that dataset had 50 million Facebook users' records. But had 87 million users records as per Facebook. Different political organizations have used data breach information to try to influence public opinion. [1]

- Political Campaigns of Donald Trump and Ted Cruz (United States 2015,2016).
- Brexit vote (2016).
- Mexican general election (Institutional Revolutionary Party 2018).

Harry Davies reported that Cambridge Analytica worked for Ted Cruz and used data from millions of Facebook accounts collected without their consent. Facebook declined the story except to say that it was investigating. (The Guardian Dec. 2015) Further reports and articles were published in The Guardian, The Intercept and followed in the Swiss publication Das Magazin. Facebook declined all the articles claims. In March 2018, the scandal unfolded by Christopher Wylie, an ex-employee of Cambridge Analytica. In 2017, he was an anonymous source for an article 'The Great British Brexit Robbery' in The Observer by Cadwalladr. [2]

This article was viral, but it was disbelieved in some states. Cadwalladr later published Channel 4 News in the UK and The New York Times because of threats. Simultaneously, the three news organizations published on March 17, 2018 and caused a huge outcry from the public. More than $ 100 billion has been knocked off the share price of Facebook in days and politicians in the United States and the United Kingdom have asked Facebook CEO Mark Zuckerberg for answers. The scandal eventually led him to testify before the U.S. Congress. The scandal provoked public debate on ethical standards for politicians, political consulting companies and social media organizations. Consumer advocates demanded greater privacy and protection rights of users in online media and restrictions on misinformation. A turning point in public understanding of personal data has caused a massive drop in the stock price of Facebook and calls for tighter regulation of the use of data by tech companies.

Figure 2 : The great British Brexit Robbery

Source: Adapted from [9]

President Trump also tweeted allegations that Google was skewing search results and then later, in response to a reporter's question, expounded further that They tread on very, very disturbed areas, Google and Twitter and Facebook. They need to be careful. It is not fair to many of the people. [3][4]

This tragedy explains that bigger organisation is shaking hands to generate their revenues by targeting audience and violating democracy and selling product and services by personalising targeted customers. These organisations are making profits and growing their businesses by violating customer's personal data and privacy and democracy.

In my opinion, the scandal was not only a breach of data but a breach of social trust, breach of law and order, breach of democracy and an event of violating political system.

Data Privacy and Protection Issues

Collaboration: The media and the Internet industry were once considered as separate industries. All have now converged around one data model. Users provide their own data for use of the service under this model. Data is then used for the publicity and marketing purposes in large quantities. Users provide their personal data for using service which is then used for advertising and marketing for revenues. Facebook, Amazon, Uber etc. are some examples. For target transactions, Amazon uses customer data. In order to develop independent vehicles, Uber utilized customer data. The problems, challenges or risks related with the data model of the industries are growing exponentially.

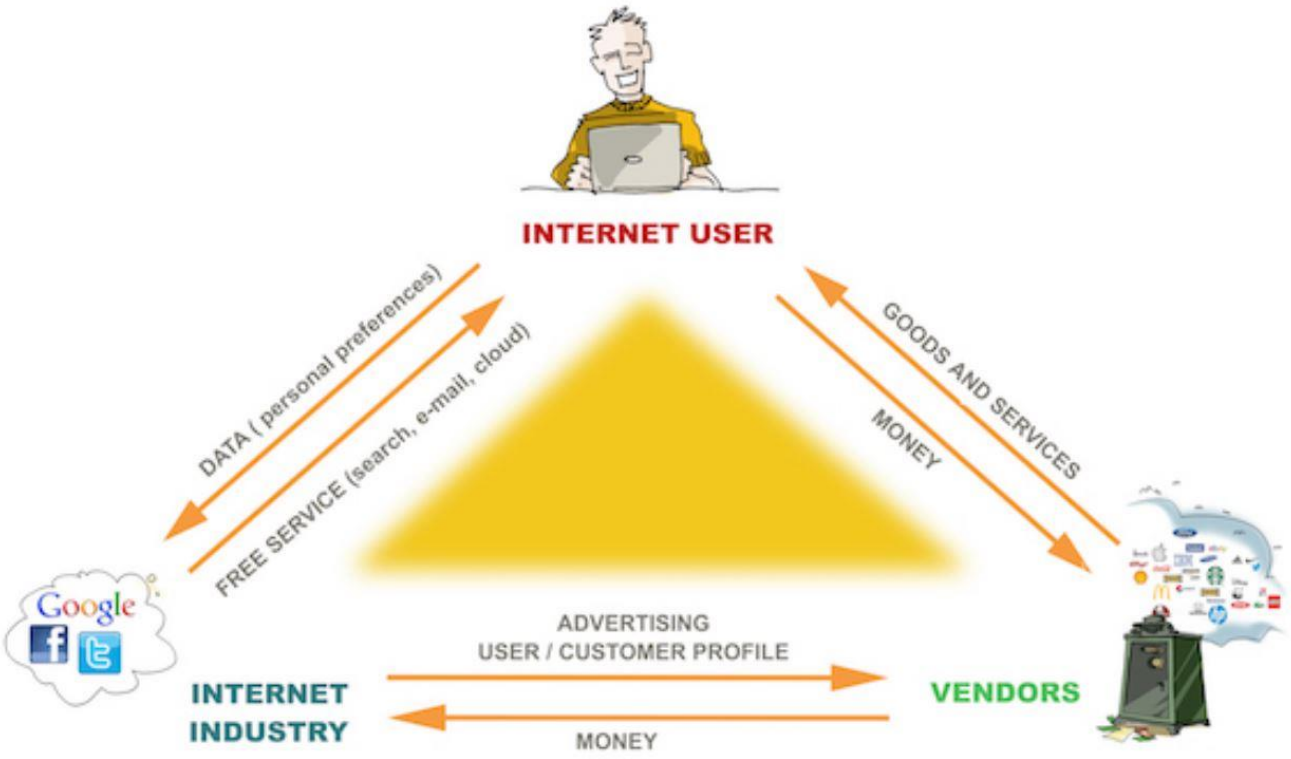

Figure 3 : Collaboration of Organisations
Source: Adapted from [10]

Intermediaries: Application Users, Facebook (Social Network) and Third Parties were involved. One important issue concern intermediaries ' responsibility for the information they collect and user's rights to their personal information.

The Cambridge Analytica data trail reveals that it was the network and the third parties (researcher Cambridge Analytica and the political campaigns) which had been involved in the two main actors. It raises various questions as well:
- Why did the Facebook allow friends data to be automatically collected?
- How potential data breaches can be addressed?
- Who is responsible if the terms between Facebook and third parties have been violated?
Data violations, data misuse and user rights violations are inherently linked**.[5]**

Content Issue: Much data is collected by Facebook and other companies. Facebook records not only the "Likes" but also geographical information of users based on GPS or WLAN signal, website information and apps the user logs in through his Facebook login credentials. The user also allows Facebook to access any contact information. Included in other data, Facebook also creates non-user shadow profiles. A major criticism of both Internet companies and public authorities is that companies can harvest large quantities of data. There are legal and ethical issues concerning the collection of type of personal data, its use and data analysis.

User Awareness and protection Issue: Although a great deal of criticism relates to the practices of the industry, most data are gathered from the users who agree to provide the data for the good or service. Therefore, it is essential to ask that if users understand the terms and conditions of internet applications. This raises issues of awareness of the terms and conditions and implications of consent

and user's data rights protection. Generally, the data is given by the users in exchange for a good or service. The major questions in this context are:
-who should protect the user's position on the Internet industry's negotiating power?
-Who should make sure that users are well informed about the impacts and possible alternatives of their consent?

Data privacy and protection: The network did not inform the users that their data has been transferred to the Cambridge Analytica researcher when it agreed that their data should be given to Facebook. Whilst data transfer may be legal because of the general terms of data policy of the company, the absence of disclosure could violate the laws of the UK and of many American countries in this case. The link to the US elections may also be illegal for Cambridge Analytica.[5]

Economic Issue: The practice of data collection by users in exchange for services or content also raised concerns regarding the reimbursement of data from users. Without financial compensation, users provide significant amounts of data. The data has greatly contributed to the Internet industry's revenues. Compensating users in case of data violation or revenue generation is an issue. This also put forward the challenges of taxing the digital economy.

Data Security Issue: Data breaches are increasing, and users are usually only aware of a data breach after the companies have revealed it. In some cases, notifications of an infringement are issued long after. Kogan found a loophole in the Facebook API that enabled to collect information of users and their all Facebook friends which raised security concerns.

Breach of Social Trust: The Cambridge Analytica and Facebook scandal brought forward a big breach to the trust of people who use their services and who were working for these organisations as well. The original data source from remote freelancers, who were paid little money, was collected by Cambridge Analytica and exchanged their data. While the case has not raised any direct problems with remote workers, it highlights the social dimension associated with workers in the gigantic economy. **[5]**

All of the above issues are required to be resolved and are critical matter of concern. These issues should be prevented first by spreading awareness among people about privacy usage of social network accounts. People should avoid using social accounts for login into any other website or application so that their data may not spread on any other platform. Moreover, people can choose privacy settings in their account relating to what information they want to share with public, friends, friends of friends, social groups, websites such as search engines and other applications. People must read the terms and conditions before surfing into any website over the internet to avoid any kind of personal data breach.

Facebook Reaction and after effects to deal with Scandal

Facebook was showing that the idea that all user data is violated has been rejected. People have deliberately provided information; no systems have been infiltrated and no passwords or sensitive information have been stolen or hacked. Facebook reports that it has hired the digital forensic company Stroz Friedberg to audit Cambridge Analytica. Zuckerberg announced further measures such as a historical audit, banning apps and developer that are not agreeing to a consistent audit and

committing themselves to telling all users whose data has been misused. Facebook apologizes for the data scandal in newspapers in the US and UK. To make it easier to find and use, Facebook announces changes in privacy settings. It also states that terms of changes in services to increase transparency – all probably related to GDPR compliance - are on the way. The bulk deletion tool is released by Facebook following the scandal. This does not allow users to choose any options yet but makes the process much less tedious than before. It says that Facebook will inform users whether their information has been transmitted by dropping a report into the News Feed from now on to Cambridge Analytica. It also provides a tool for manual inspections. [6]

Facebook Claims that:

- In December 2015, they immediately banned Kogan's app from their platform and demanded certifications that they had deleted all improperly acquired data.
- In April 2018, Facebook announced a series of changes to data handling practices and API access capabilities.
- May 2018, about 200 apps were banned from Facebook as a part of an investigation into if companies have abused APIs to harvest personal information.
- In June 2018, Facebook discontinued the trending feature.
- In a July 2018 interview with Recode, Zuckerberg stated that he believed his company had taken all the right steps in the wake of the scandal. These included cutting ties with data brokers, rewriting its terms of service, and undertaking to audit third-party developers that could access Facebook user data.

GDPR

A regulation in EU law concerning privacy and data protection for all individuals in the European Union and the European Economic Area is the General Data Protection Regulation- GDPR. It also covers rules and regulations for personal data exports outside the EU and EEA. The GDPR's main motive is to provide control to individuals ' personal data and simplifying the international business regulatory environment by unifying regulations within the European Union. [5]

On 14 April 2016, the GDPR was adopted and became effective on 25 May 2018. As the GDPR is not a directive, it is directly binding and applicable, but gives flexibility to adapt certain aspects of the regulation. Personal data controllers must establish appropriate technical and organizational measures to implement the principles of data protection. The processes which handle personal information must be developed and developed with respect to the principles and must provide safeguards to protect data (e.g. by pseudonymization or full anonymization where applicable) and by default use the highest possible privacy options to prevent data from being made public without explicitly and informed agreement and to prevent the identification of a subsection. No personal information may be processed unless the data controller or processor has received an unambiguous and personal confirmation of the data subject's consent on the legal basis laid down in this regulation. This consent is to be revoked at any time by the data subject. Any data collection should be clearly disclosed to a processor, the legal basis and end of the data treatment should be declared, and the length of retention and shared data with a third party or external to the EEA shall be specified. Under certain circumstances data subjects have the right to request a portable copy and the deletion of

their data from the data collected by a processor, in a common format. The Data Protection Supervisor is responsible for managing GDPR compliance and is required by public authorities and undertakings whose core activities are focused on regular or systemic processing of personal data. Businesses must report any infringements of data within 72 hours if their impact on user privacy is adverse. In certain cases, GDPR violators may be punished for an undertaking, whichever is higher, with up to 20 million € or 4% of the annual international turnover in the preceding financial year. [5]

GDPR – Data Protection Act Amendments in brief

Individual Rights: Individuals have right to access, withdraw consent, change, restrict and delete their personal data.

Informed Consent: Consent should be mentioned in a clear, shorter and easy to understand and easy to withdraw as well.

Breach Notification Messages: Organisations have to report any breach notification within 72 hours of stipulated time.

Data Transfer: Personal data cannot be transferred without permission of customer. Customers can transfer personal data from one company to another but only customer has to specify the data that need to be transferred.[6]

Liability: Data Processors and Controllers will be directly responsible in case of breach.

Supervision and Enforcement: Organisations outside EU and handling EU data can face sanctions and higher penalties. Any national regulator can take action under 'one stop shop' approach. Higher penalties for data breach and any other regulation relevant with respect to GDPR with a maximum fine of €20 million or 4% of organisation's worldwide turnover whichever is applicable. For lesser offences it is nearly half reduction in penalties.[6]

The GDPR gives authority and control to the individuals for use of their personal information. This means customers have right to object against the action on their personal data by internet organisations and can file a complaint against them. It is very important that customers are aware of their new rights by which they can control and handle the privacy and effectively protect their personal data in compliance with GDPR's new regulations.

GDPR and Internet of Things

One must have to take account of Internet of things project where personal data is being used, as GDPR is applicable in IoT communications as well. However, a lot of people speak about the privacy Regulation from the point of view of the Web, cookies, email and all other sort of electronic communications. For the Internet of Things also the principle of confidentiality applies to current and future means of communication. It is necessary to have certain data privacy and protection means in machine-to-machine communications case of IoT communications. Whether all Internet of Things use cases are not just about personal user data but in many other use cases for example in the

Industrial Internet of Things it is required. The GDPR mentioned a range of online identifiers including Radio Frequency Identification (RFID) tags. Therefore, Internet of Things use cases are always about data so it's crucial to see where exactly in IoT applications personal data is being used.[7]

However, at the same time there is also track and Analyse the specific risks of the Internet of Things from both GDPR and breach risks and the loss or theft of personal data risks. However, Internet of Things still is in its early days, there are various areas where personal data is being used. There is also the risk of intruders, hackers and attackers and other security, privacy and protection risk involved in case of Internet of things communications.

IoT using organisations must be aware of the personal data they collect and process. Understand consent and provide consent to the customer related to personal data. IoT using companies must consider that consent can be deleted and withdrawn as well and there must be effective solutions for that too. There is mandatory requirement to record everything that is needed to meet the requirements of GDPR. IoT technology-based organisations need to take a great care of the need for privacy and protection of personal data by design. Every organisation must assign a data protection officer in their data controller and processing centers to keep an eye on privacy breaches and must be reported to GDPR in compliance with regulations.[7]

Ethical implications of GDPR for the Internet of Things.

- New instruments such as data protection impact assessments have been largely welcomed in the market. All risks cannot be removed, but data protection impact assessment can to investigate and mitigate other data protection dangers, plan for the implementation of any measures to those dangers and check the viability of a data project at an early stage.
- Strong device authentication practices that are incorporated in the design phase can provide cryptographic proof of when and how a device has been tampered with. Authentication tokens used for accessing web applications that are high in security are welcomed in Information and Communication Technology industries.
- Public Key Infrastructure (PKI) and digital certificates can prioritize security without diminishing the user experience. Certificates for login into web application with yearly expiration for all users along with authentication measures can also reduce the risk of data leak.
- New tools, such as customer-accessible data profiles and notification practices, developed in response to the GDPR provide a clear pathway for users to understand how personal data is acted upon to improve both the data collection system and interactions with it.

Recommendations and Personal Opinion

After studying the whole case it is clear that there were many parties involved in the Scandal instead of Facebook and Cambridge Analytica. But there were no solid proofs against them as the awareness about the Scandal took years to appear in front of law and legislation. First person that is responsible is Aleksandar Kogan himself because he developed an app that breaches personal data of Facebook users. He could have prevented Scandal if he would have acted responsibly by reporting this breach before misuse. The second responsible party is Facebook because their application allowed large amount of personal information of people who gave consent and others as well who did not give their consent but were friends of those who used the application. The third responsible organisation and undoubtedly most unethical organisation is Cambridge Analytica because the firm sold the personal data to politicians and interested persons for generating revenue. The other persons are those who bought personal data for influencing people for votes. This include Donald Trump, Ted cruse, Mexican leaders, Leaders conducting votes for Brexit. There are no legal proofs against them.

The Scandal breaks through very late and arises only with the involvement of media and press release worker's effort otherwise it would never have been recognised. Facebook also knew that the data has been misused but keep on denying the fact since 2015 to prevent their status in Digital Market, its popularity and annual revenue.

The action taken by GDPR is necessary to protect people's personal data and information because people should have rights to where their personal data is being used and for how long it should be stored by someone. The action taken by GDPR will prevent future happenings like this Scandal. Although the investigation did not prove some people's involvement, but it brings fear among other who are also involved in such kind of activities as the punishment decided by GDPR.

I would recommend awareness about the digital marketing and platforms among people is essential as all the platforms are now moving on to cloud and internet technology and is on the server. So, it is necessary that people know how they can prevent their personal data over the internet and their personal data rights in case of any misuse and the compensation that they will get in return**.**

I would also recommend that the organisations should also have legal certification and a written consent for any data leak from their organisation due to any reason before collecting personal data.

Conclusion

The overall report clarifies that the personal data platforms like facebook bear a great responsibility for the diffusion of personal data in interconnected systems. The case of Facebook and Cambridge Analytica has been widely covered under the study of case. This shows how democracy is violated and voting system is being manipulated by personal data misuse. It can be concluded that there is a strict regulation acts required to maintain a fair system in political environment wherever public opinion matters. This also opens the data protection regulation eyes for other organisations that are buying audience data for gaining benefits in their business. This manipulation and violation of technology and personal data in an unethical manner is a punishable misconduct and must give strict preference in each aspect of parties involved in case of personal data and digital communications and transactions. GDPR amendment is a great initiative for consumers to better know their privacy and data protection rights.

References

[1]H. Davies, "Ted Cruz campaign using firm that harvested data on millions of unwitting Facebook users", *the Guardian*, 2019. [Online]. Available: https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data. [Accessed: 09- Feb- 2019].

[2]C. Cadwalladr, "The great British Brexit robbery: how our democracy was hijacked", *the Guardian*, 2019. [Online]. Available: https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy. [Accessed: 09- Feb- 2019].

[3]F. Staff, "Cambridge Analytica trabajó con el PRI: Channel 4 News Forbes México", *Forbes México*, 2019. [Online]. Available: https://www.forbes.com.mx/cambridge-analytica-mexico-pri-enero-2018-channel-4-news/. [Accessed: 09- Feb- 2019].

[4]"How Trump Consultants Exploited the Facebook Data of Millions", *Nytimes.com*, 2019. [Online]. Available: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. [Accessed: 09- Feb- 2019].

[5]"Cambridge Analytica explained: The facts, implications, and open questions | GIP Digital Watch", *Dig.watch*, 2019. [Online]. Available: https://dig.watch/trends/cambridge-analytica. [Accessed: 09- Feb- 2019].

[6]*Ibe.org.uk*,2019.[Online].Available:https://www.ibe.org.uk/userassets/briefings/ibe_briefing_62_beyond_law_ethical_culture_and_gdpr.pdf. [Accessed: 10- Feb- 2019].

[7]Rolf H. Weber, Internet of things: Privacy issues revisited, Computer Law & Security Review: The International Journal of Technology Law and Practice (2015).

Figures:

[8]"Summary -> Facebook Suspends Cambridge Analytica For Failing To-wsj", *Yousense.info*, 2019. [Online]. Available: http://yousense.info/66616365626f6f6b/facebook-suspends-cambridge-analytica-for-failing-to--wsj.html. [Accessed: 06- Apr- 2019].

[9]C. Cadwalladr, "The great British Brexit robbery: how our democracy was hijacked", *the Guardian*, 2019. [Online]. Available: https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy. [Accessed: 09- Feb- 2019].

[10]"Cambridge Analytica explained: The facts, implications, and open questions | GIP Digital Watch", *Dig.watch*, 2019. [Online]. Available: https://dig.watch/trends/cambridge-analytica. [Accessed: 09- Feb- 2019].