MUNESCO

Forum: GC5
Issue: The question of technological privacy in social media with a special emphasis on facial reconnaissance and audio-based data
Student Officer: Mete Hergül
Position: President Chair

Introduction

The development of affordable handheld devices capable of fast internet networking has capacitated an unparalleled spur in the usage of social media networks over the last decade. To quantify how things stand, Facebook had just over 100 million users in the third quarter of 2008. Exactly ten years later, the number of Facebook users has exceeded 2.2 billion (Statista, 2018). This surge is not exclusive to Facebook, with the numbers of users of networks like Twitter increasing exponentially, and the birth of relatively new networks like Instagram and Snapchat, which are used by hundreds of millions of people around the world. There are also social networks that are used mostly in certain countries, such as VKontakte in Russia or WeChat and Weibo, some with user bases expressed in numbers above 400 million. As social media networks are integrated more and more into people's daily lives, these networks grow to contain personal information in various contexts, that other people can easily access. With technological innovation outpacing the rate at which social, political, economical, and most importantly legal, bodies and organs can operate, governments, corporations and other large-scale organizations have gained access to our private lives like never before. Therefore, the main threat to privacy in social media is not constituted by maligned individuals, but the aforementioned organizations for purposes of surveillance. Furthermore, emerging artificial intelligence-based technologies that can identify, analyze and differentiate between faces and audio patterns help social media networks acquire much greater importance than they had a decade ago, especially in this context. In a world where privacy must be an irrevocable right for any and all individuals, this question remains one to be prioritized through whatever means possible.

Definition of Key Terms

Algorithm: A process or progression of rules set to be followed by a computer or an individual in order to perform a particular task.
Anonymization: The process of removing specific identifiers (often personal information) from a dataset.
Big Data: Large volumes of data, structured or unstructured, that can be analyzed to identify patterns, correlations or associations, especially in the context of human behavior.
Digital Ethics: The ethics of how users and participants in online environments interact with each other and the technologies and platforms used to engage.
Digital Privacy: The concept of privacy that concerns three privacy: information privacy, communication privacy, and individual privacy.
Privacy Policy: The document that discloses how the party of agreement makes use of the data provided by the other party of the agreement.

Background Information

As background information on this topic is delivered, the delegate will see a range of events and concepts that are of relevance to the topic. These cases are provided in abstract chronological order. It would be proper to note that the concentration of these events in developed countries are not of coincidence, since this topic is purely technological. However, the emergence of these technologies at the current rate requires action at this relatively premature stage. Notwithstanding, these cases constitute significant examples as to how the international community must act on this topic.

The Dot-Com Bubble:

The emergence of the World-Wide Web in the last decade of the 20th century was seen as a great field of development for capital investments, as investors sought to capitalize on this new sector with unseen potential for growth. When Yahoo! made its initial public offering (IPO) in 1996, the trading price of a single stock doubled in a single day, from $16 to $33. Many other companies in the sector, although smaller in size, capitalized on this trend, increasing the value of the technology financial market drastically. However, after just three years in 2000, the National Association of Securities Dealers Automated Quotations (NASDAQ) index plummeted, causing many tech companies to go bankrupt while bringing down more than a trillion dollars' worth of investments with them (Kenton, Will). This incident came to be known as the Dot-Com bubble, and connoted the requirement for a strong revision of business models for WWW-based companies.

The new business models that was come up with by these companies, was an advertisement-oriented atmosphere created online, with the monetization of certain elements that provided additional access to services. In order to maximize profits made from the advertisements, the companies needed a method in hand that allowed them to generate user-oriented advertising. This requirement was first fulfilled with data that came from search engine and website entry patterns. Nowadays, social media, with all its involvement in our lives, provides a much larger data set on each and every individual, from their political tendencies to the brands they're interested in and even to their sexuality. This enables these networks to cater to Big Data companies that utilize this information for all purposes from algorithmic analysis to targeted advertisements. These unconsented intrusions, in return, provide optimized revenues and a great upper hand to be marketed. Even though the Dot-Com Bubble as an incident has become obsolete in the present day, its aftermath is what laid foundations for this unethical practice that has become a growing threat today.

The National Security Agency (NSA) and XKeyScore:

It has been speculated before that the National Security Agency violates the privacy of individuals by tapping into their phone calls and storing them. XKeyScore, an algorithm developed by the Agency and first revealed in a February 2008 leak by whistleblower Edward Snowden (Greenwald, Glenn) is capable of recording all the behavior and actions that an individual exhibits online, such as but not limited to their web searches, social media accounts and e-mails. The NSA has even gone to the extent of declassifying this program and bragging about its capabilities in various training documents. Given the role and importance of the NSA not only in America but globally, the accumulation of such private information in the hands of the government is a huge threat to the privacy of many individuals, as it can be used to spy on people without the need for authorization.

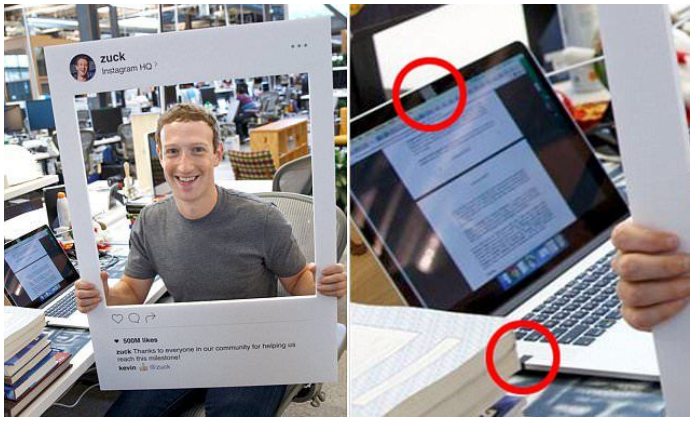
Facebook, its History, and its New Web of Privacy via Instagram and WhatsApp:

Facebook, initially a matchmaking website exclusive to the Harvard student community, was founded by Mark Zuckerberg in 2004. A decade and a half later, the network stands as the largest social media platform in the world, with over 2.2 billion active users. The network earns 98% of its revenue from advertising (Wagner, Kurt). However, the network is also known for getting involved in various scandals and controversies regarding user privacy. The social media network is known for actively generating profiles of its users regarding a number of matters, including preferences in purchases and politics, in order to generate targeted advertisements and sponsored posts. Nevertheless, these profiles cannot be likened to 'cookies', which are much simpler in nature and intend to store user preferences on a much more exclusive basis. They are much more comprehensive, and the data contained in these profiles can also be sold to third parties. This practice, however, is not unique to Facebook: other social media networks, such as Twitter, are known to sell user data to third parties.

The acquisition of Instagram, the photo sharing platform, and WhatsApp, one of the most popular messengers in the world, by Facebook in 2012 and 2014, for $1 billion and $19 billion respectively, can be interpreted as efforts by Facebook to expand its access to user data. (Wagner, Kurt) Given the fact that Instagram provides access to the faces of millions of people, this could further enable the developments of facial recognition technologies. As for WhatsApp, Brian Acton, former co-founder, has stated with remorse, "I sold my users' privacy (Sanders, James).

Patents issued to Facebook regarding facial recognition technologies date back to 2011. However, the latest technology developed by Facebook in 2014, DeepFace, is capable of matching faces with 97.25% accuracy. The algorithm is also stated to constantly look for the faces of individuals in all the photos on Facebook and automatically tag them, even if not requested by the user (Chowdry, Amit).

Webcams and Software Exploits:



Mark Zuckerberg's photo with his laptop's webcam and audio jack taped in the background, circa 2016. Source: dailymail.co.uk.

People that can be considered of great importance on this matter, including Facebook CEO Mark Zuckerberg, are known to tape the webcams of their personal computers. James Comey, Former Director of the Federal Bureau of Investigation, has stated that "It is a sensible thing to do" (Macias, Amanda). In fact, a vulnerability related to Flash that allows a third party to access the webcam of a computer without asking for permission. Unless these platforms employ serious security measures

such as end-to-end encryption, these exploits can also easily occur on social media platforms; potentially resulting in substantial video and audio leaks from private conversations.

The Cambridge Analytica Scandal:

Mark Zuckerberg during his testimony in the Cambridge Analytica Senate Hearings. Source: marketwatch.com.

Cambridge Analytica is the Big Data company that became renowned with the scandal involving itself and Facebook. The build-up to the Cambridge Analytica scandal can be attributed first to the 2011 Facebook-US Finance and Trade Commission agreement. The FTC made an eight-count complaint against Facebook, alleging that the networking company had failed to maintain the privacy of its users, ensuing several instances that dated back to 2009. In return, Facebook settled these complaints, reaching a formal agreement with the FTC that from then it would protect the privacy of its users and asking for any and all permissions from the user before sharing their data with third parties.

Nevertheless, the scandals that would combine Facebook and privacy wouldn't stop there. In 2013, Alexandr Kogan, a data researcher from Cambridge University, created an application titled "This is Your Digital Life", or as it is often stylized, *thisisyourdigitallife*. The application had the purpose of having Facebook users do surveys that would be used for academic purposes. However, the application capitalized on a flaw found in Facebook's algorithms, and not only gained access to the private information of the people who participated but also their entire friends' list. This app was then provided to Cambridge Analytica, a big data company founded by Steve Bannon. This name is another area of concern, since Bannon was also the founder of Breitbart, the alternative-right media outlet that openly advocated for the United Kingdom's exit from the European Union (will be referred to as Brexit thereafter), and endorsed Donald Trump's presidency back in 2016. Bannon later became the White House Senior Strategist, which he resigned in late 2017.

Cambridge Analytica had maintained ties with Ted Cruz, a Republican Senator of Texas, in which Cruz utilized data provided by the company during the 2014 Senate elections, as reported in 2015 by Harry Davies of The Guardian. The 'Vote Leave' campaign of the Brexit Referendum and the Trump Presidential Campaign were also partnered by Cambridge Analytica. Back then, Facebook was aware of the problem yet simply asked Cambridge Analytica to get rid of the data.

Meanwhile, whistleblower and ex-Cambridge Analytica employee Christopher Wylie and Carol Cadwalladr of The Observer partnered in various articles, including the 2016 "The Great British Brexit

Robbery". Even though Facebook first waived off this scandal stating that they were looking into the problem. It blew up again in 2018, when the case was mentioned in major news outlets including The New York Times and Channel 4 News. The stock price for Facebook plummeted and the company lost more than a hundred billion dollars in value. As a result, Facebook CEO Mark Zuckerberg was compelled to testify in front of the US Senate, where he admitted Facebook's fault in the scandal and pledged to adopt EU's General Data Protection Regulation program not only in the EU but worldwide. Nevertheless, the implications of the scandal were not undone. The Brexit Referendum and the 2016 US Elections remained largely influenced, as the UK struggles with the lack of a Brexit deal and the Mueller investigation into the Trump Administration alleges Russian collusion in American politics.

The Cambridge Analytica scandal illustrates the magnitude of repercussions of the handling and use of big data obtained through social media by maligned entities, and the case marks an unparalleled example on why the way big data is obtained, handled and distributed requires revision.

Voice Assistants:

Since the release of Siri by Apple back in 2011, voice assistants have become more and more of a part of the daily lives of millions of people. Google, Microsoft and Amazon have all created their counterparts of this technology, and smart speakers featuring these assistants constitute a sector of high demand and competition. However, the presence of these speakers at homes while they are constantly connected to the Internet has caused speculation regarding these gadgets, on whether they can be used to constantly listen to people. Technically, all these assistants are only activated in case a keyword is said out loud, but this doesn't mean that the issuers of these assistants cannot access and store voice recordings or that these assistants cannot be accessed by maligned individuals or parties. Furthermore, the assistants technically have access to a range of customer preferences, further strengthening the possibility of a violation of privacy.

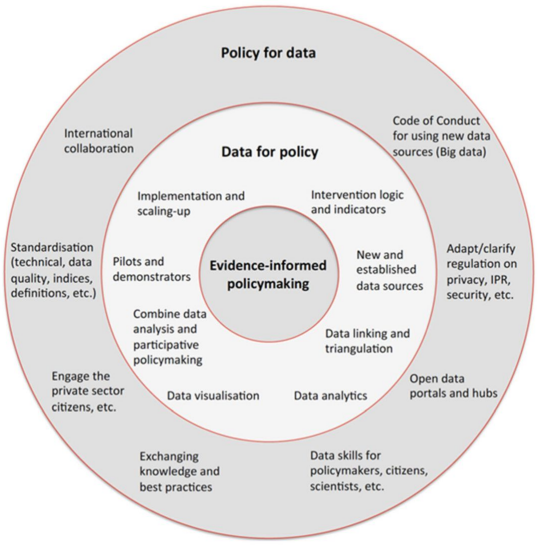
Apple and the FaceTime Controversy:

Apple's CEO, Tim Cook, has been an outspoken critic of Facebook's privacy policy when the Cambridge Analytica incident surfaced. He has advocated for the conservation of the rights of the user to privacy, and the treatments of the users as "customers and not as the product". (Wong, Julia Carrie)

In light of these statements, Apple's video conferencing app, FaceTime, has very recently experienced problems where some devices are able to hear from the other side that is being called without the opposite side answering the call on the latest version of their mobile operating system, iOS 12.1 (Mayo, Benjamin). Although Apple has addressed this software issue, this case with FaceTime, one of the main reasons why people prefer Apple devices, demonstrates how a little mishap could lead to potentially disastrous violations of privacy.

Sustainable Development and Big Data:

The UN Economic and Social Commission for Asia and the Pacific defines Big Data as one of the most efficient auxiliary elements when it comes to the fulfillment of the Sustainable Development Goals.



The Scope of Data and Policy, per the UNESCAP.

Data with regards to the population and its characteristics is essential in the fulfillment of the Sustainable Development Goals, as it is a precursor in the extent of plans and actions that are to be implemented. With proper handling and use, Big Data can prove itself as an irreplaceable asset in the transformation of our planet for the better. The roles of governments and large-scale international organizations gains great importance, due to the fact that there is a lack of entities that can conduct the collection of data However, with recent scandals involving Big Data and its use, the extent of collection and storage, and openness of Big Data are crucial matters to be discussed and determined, not only for the sake of user privacy but also for a sustainable future.

Timeline of Major Events

March 2000	The Dot-Com Bubble.
February 2004	Facebook, which grew to be the largest social media network globally, founded by five Harvard students, including current CEO Mark Zuckerberg.
February 2008	XKeyScore mentioned in a document leaked by Edward Snowden, whistleblower and former Central Intelligence Agency/National Security Agency analyst.
2011	First investigation on Facebook prompted by the US Federal Trade Commission (FTC), regarding Facebook's usage of user data. Facebook enters into a consent decree.
October 2011	Apple's Siri, the first mainstream smart voice assistant, becomes available.
November 2011	A patent for facial recognition technology issued under Facebook in the US Patent and Trademark Office, with the code US9087273B2.

April 2012	Facebook acquires Instagram for $1 billion.
July 2013	The Guardian mentions XKeyScore as part of NSA's official training materials, as an algorithm that collects all the activities of individuals on the internet, including social media, web searches and e-mails.
March 2014	Facebook unveils facial recognition algorithm "DeepFace", that can match faces with 97.25% accuracy.
October 2014	Facebook acquires WhatsApp Messenger for $19 billion.
November 2014	Amazon unveils its smart assistant Alexa, as well as the first commercially available smart speaker Amazon Echo, kickstarting the sector.
March 2018	Exposé published regarding the Cambridge Analytica scandal, on which Facebook threatened to sue The Guardian and The New York Times. The FTC re-initiates investigation regarding the 2011 agreement, with Facebook facing fines expressed in billions of dollars.
April 2018	Mark Zuckerberg appears before the United States Senate, testifying regarding the Cambridge Analytica scandal.

Major Countries and Organizations Involved

United States of America:

Although previous cases of concern have mostly happened in the United States, .the country is no longer a member of UNESCO, as of January 1 2019. American policy relating to privacy in social media has become an area of concern globally, since three of the most used social media networks, Facebook, Twitter and Instagram, originate from the United States. Furthermore, the XKeyScore data collection algorithm of the NSA, an organization that has unprecedented access to information not only in the United States but also worldwide, becomes an area of concern due to the threats it poses to the privacy of millions of social media users. The importance of the Cambridge Analytica scandal also renders the US as a party of greatest concern on this matter. The country's expertise on facial reconnaissance and its development through academic institutions and corporations like Facebook can be evaluated as an asset in maximizing the protection of privacy concerning these technologies.

People's Republic of China:

The importance given to Big Data and surveillance by People's Republic of China makes the country a serious case of concern for regarding the topic. Practices such as the Social Credit System, that aims to assess citizen behavior in all aspects of life, including in social media, render China one of the most intrusive entities in the lives of its citizens. As China strays further away from personal privacy than it

ever was, the country becomes one of the most important examples of to what extent Big Data can be utilized.

Russian Federation:

With rumors that Kremlin is attempting to create a surveillance state, the Russian Federation is a state of great concern on this matter, with the greatest number of Internet users in all of Europe and large-scale endemic social media platforms. Russia implemented a new data retention law about seven months ago, which forces all telecommunications company to store phone calls, short text messages and internet usage patterns for six months, for the sole benefit of Russian intelligence. Although the legislation does not cover foreign networks, VKontakte, Odnoklassniki and Yandex, three of the most active websites in Russia, are covered (Meyer, David).

Facebook:

Despite its previous involvements in scandals of user privacy, Facebook remains as the largest social media network in terms of its number of users. Its previously exemplified mistakes concerning privacy strategy and management, as well as its unrivalled facial recognition technologies might enable the determining of strategic roadmaps to outline the future of Big Data use and its restrictions. Due to its size and possession of Instagram and WhatsApp, change in its policies and practices might constitute important examples for other social media networks. In other words, wherever Facebook and its subsidiaries go in terms of user privacy for good, the others will surely follow.

Office of the United Nations High Commissioner for Human Rights:

The OHCHR has been the main institution under the United Nations to particularly discuss cyber data privacy and address it. With the September 2013 and February 2014 statements released by the High Commissioner, special attention was drawn to how electronic surveillance may impede the right to privacy. The High Commissioner organized a panel on the request of the Human Rights Council, yielding the September 2014 outcome report.

Previous Attempts to Solve the Issue

- The International Covenant on Civil and Political Rights
  (UN General Assembly, December 1966)

- Resolution 68/167
  (UN General Assembly, December 2013)

- Resolution 28/16: The Appointment of a Special Rapporteur on Privacy
  (UN Human Rights Council, April 2015)

Possible Solutions

The revision of privacy policies of social media platforms to be considered with the cooperation of States and any and all international organs, including the usage of facial recognition algorithms and sharing of data with the direct consent of the user.

The revision and amendment of all international legislative framework regarding privacy for the comprehension of cases of violation of privacy through new media.

Guidelines with regard to an international consensus on the governments abstaining from private data collection via the Internet unless necessitated for authentic purposes of security, such as a terrorist threat.

Mutual efforts of the States and/or companies in the development of security measures regarding voice assistants and webcam technologies.

The complete anonymization of data collected by any and all entities, and the prohibition of sales to third parties involved with ongoing investigations pertaining to Big Data or if the entity has previously failed to maintain anonymity.

Ensuring the openness of any and all accumulations of Big Data under the possession of governments, that do not pertain directly to national security threats.

Useful Links For Further Research

You can find the aforementioned OHCHR reports here.
https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx.
An academic article titled “Social Media Surveillance”.
http://fuchs.uti.at/wp-content/DS.pdf:
More technical; provides a better understanding of how Facebook’s DeepFace works. Notice the academics who participated.
https://www.cs.toronto.edu/~ranzato/publications/taigman_cvpr14.pdf
Purely technical, for those who want to see one of Snowden’s documents: https://edwardsnowden.com/wp-content/uploads/2013/10/2008-xkeyscore-presentation.pdf:
The UNESCAP report on Big Data and Sustainable Development Goals:
https://www.unescap.org/sites/default/files/1_Big%20Data%202030%20Agenda_stock-taking%20report_25.01.16.pdf

Bibliography

Chowdhry, Amit. “Facebook's DeepFace Software Can Match Faces With 97.25% Accuracy.” *Forbes*, Forbes Magazine, 18 Mar. 2014, www.forbes.com/sites/amitchowdhry/2014/03/18/facebooks-deepface-software-can-match-faces-with-97-25-accuracy/#6c80a98754fc.

“Facebook Users Worldwide 2018.” *Statista*, Statista, www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

Greenwald, Glenn. “XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet'.” *The Guardian*, Guardian News and Media, 31 July 2013, www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

Jingtuo, Liu. *Targeting Ultimate Accuracy: Face Recognition via Deep Embedding*. Baidu Research – Institute of Deep Learning, arxiv.org/pdf/1506.07310.pdf.

Kenton, Will. “Dotcom Bubble.” *Investopedia*, Investopedia, 13 Dec. 2018, www.investopedia.com/terms/d/dotcom-bubble.asp.

Macias, Amanda. “FBI Director Says He Covers His Webcam and Shares Other Security Recommendations.” Business Insider, Business Insider, 14 Sept. 2016, www.businessinsider.com/fbi-director-covers-webcam-2016-9.

Mayo, Benjamin. “Major IPhone FaceTime Bug Lets You Hear the Audio of the Person You Are Calling ... before They Pick Up.” *9to5Mac*, 9to5Mac, 30 Jan. 2019, 9to5mac.com/2019/01/28/facetime-bug-hear-audio/.

Meredith, Sam. “Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal.” CNBC, CNBC, 10 Apr. 2018, www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html.

Meyer, David. “Russia's 'Big Brother' Data Law Now in Force: Kremlin Spies Are the Big Winners.” *ZDNet*, 2 June 2018, www.zdnet.com/article/russias-big-brother-data-law-now-in-force-kremlin-spies-are-the-big-winners/.

“Privacy & Technology.” *American Civil Liberties Union*, Aclu, www.aclu.org/issues/privacy-technology#current.

Sanders, James, and Dan Patterson. “Facebook Data Privacy Scandal: A Cheat Sheet.” *TechRepublic*, www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/.

Wagner, Kurt. “Facebook May Be Facing a ‘Record’ Fine from the FTC. Here's Why.” *Recode*, Recode, 23 Jan. 2019, www.recode.net/2019/1/23/18193314/facebook-ftc-investigation-explained-privacy-agreement.

Wong, Julia Carrie. “Apple's Tim Cook Rebukes Zuckerberg over Facebook's Business Model.” The Guardian, Guardian News and Media, 28 Mar. 2018, www.theguardian.com/technology/2018/mar/28/facebook-apple-tim-cook-zuckerberg-business-model.