**Case Study: Inappropriate Use of Surveys**

In 2018, Cambridge Analytica was in the news in the United Kingdom and the USA (Confessore, 2018) for obtaining and sharing data obtained from millions of Facebook users. They obtained the data through innocuous surveys on Facebook (you may have seen this type of survey and probably participated at times). This is probably the highest profile of surveys used for alternative means and, probably, monetary gains. However, this happens often through various media.

Consider how exactly this happened and why it was used. Find one or two further examples of inappropriate use of surveys and highlight the impact of all these examples from the various ethical, social, legal and professional standpoints that apply.

Record your findings in your e-Portfolio. You can also submit your findings to your tutor for formative feedback.

The whole idea was based on 2014 paper by Cambridge University’s Psychometrics Centre, “Computer-based personality judgments are more accurate than those made by humans”. To make the whole thing work CA needed data so Christopher Wylie first approached Michal Konsinski, one of the co-authors of the original myPersonality research paper in order to access the myPersonality database. But when negotiations failed, another psychologist and one of Konsinski’s colleagues, Aleksandr Kogan offered them a solution that would replicate Stilwell’s and Konsinski’s original research (Cadwalladr & GrahamHarrison,2018). Cambridge Analytica- How 50 million Facebook r

The Facebook data privacy scandal led to the harvesting of millions of Facebook profiles by Cambridge Analytica. The firm was able to get access to private information of Facebook users due to number of factors, mainly including insufficient safeguards against data mining firms, inadequate supervision of developers by Facebook and users excessively agreeing to Facebook terms and conditions. In 2014 Aleksandr Kogan had developed a Facebook app called “thisisyourdigitallife” which allowed people to participate in a personality quiz test and Cambridge Analytica paid for people to take it. This app not only harvested data from the quiz taker’s Facebook account but also the data of their Facebook friends. This led to data harvesting of up to 87 million Facebook profiles (Kang and Frenkel, 2018). Kogan, then shared this data with Cambridge Analytica, a political consulting firm that uses data to determine voter personality traits and behavior. This led to violation of Facebook’s terms and conditions which forbids the sharing or sale of data “to any ad network, data broker or other advertising or monetization-related service” (Granville,2018). Facebook learned about this in 2015 and it immediately banned Kogan’s app from its platform and demanded Kogan and CA to delete all the data that they had gathered illegally. Kogan and CA all certified to Facebook that they deleted the data. However, in March 2018 Facebook learned that the data wasn’t deleted after CA whistleblower Christopher Wylie revealed that the data harvested form Kogan’s app was used for building “psychographic” profiles of people and deliver pro-Trump material to them online (Meredith,2018).CA used the data for clear political purposes- to help conservative campaigns in the 2016 election, including Donald Trump’s campaign (Rosenberg,Confessore and Cadwalladr,2018). Facebook first responded on March 17, 2018 in a F Facebook post by Paul Grewal, VP & Deputy General Counsel, who wrote that, “The claim that this is a data breach is completely false. Aleksandr Kogan requested and gained access to information from users who chose to sign up to his app, and everyone involved gave their consent. People knowingly provided their information, no systems were infiltrated, and no passwords or sensitive pieces of information were stolen or hacked”(Grewal,2018).On the same day Alex Stamos, Facebook’s Chief Security Officer, tweeted (later deleted the tweet) that, “Kogan [one of Cambridge Analytica’s researchers] did not break into any systems, bypass any technical controls, or use a flaw in our software to gather more data than allowed. He did, however, misuse that data after he gathered it, but that does not retroactively make it a ‘breach.’”(Johnston,2018).International Organization for Standardization and the International Electrotechnical Commission – two bodies that regulate global security practices, define data breach as follows “a compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed”(ISO,2015).Since the

.Since the Facebook systems weren’t bypassed and the data was misused by a third party that clearly violated Facebook terms and conditions, the incident therefore doesn’t qualify as a data breach as understood by the global cyber security community. Consumers must realize that their data are worthwhile. Consumers should learn how companies, in particular those offering free services such as Facebook and Google, use their personal data to run their business. Consumers should read data privacy notices and make use of the in- product user controls offered by most tech companies. Consumers should take advantage of their rights to ask a company to have their personal data viewed, edited and deleted because, after all, data belongs to consumers and not companies. If companies engage in illicit or false data handling practices, consumers should file complaints with the Federal Trade Commission (FTC) or any other governing bodies. Lastly, consumers should promote greater transparency and company controls and require their elected officials to do more to protect privacy. Almost, all the companies in the world now process personal data electronically. So, companies ought to learn to better balance privacy risks with privacy controls. The riskier the use of data, the more user controls are necessary. Controls can include user friendly and distinguished privacy notices, clear consent and privacy-friendly default settings. While sharing the data from third parties, companies should make sure that those companies comply with their privacy standards by investing in period audits. Similarly, when receiving data from third parties, companies should make sure that the data was collected a proper manner, not merely believing in vendor’s word, but again, by performing period audits. And eventually governments must reshape outdated laws in order to tackle the current complexities of data usage and transfers The European Union, for instance has set up a global example, through the General Data Protection Regulation that came into effect

on May 25, 2018. “This is a comprehensive piece of legislation that (1) expands data subjects’ rights (2) enforces 72-hour data breach notifications (3) expands accountability measures and (4) improves enforcement capabilities through levying fines of up to 4% of global revenue.” This law is applicable only to European countries, but most multi national tech companies have incorporated these standards for all their customers(Kozlowska,2018). However, time has come that similar privacy protection laws are passed across the globe so that everyone can benefit from the opportunities that the 21st digital economy brings with it.

Whistleblower describes how firm linked to former Trump adviser Steve Bannon compiled user data to target American voters

* [‘I made Steve Bannon’s psychological warfare tool’: meet the data war whistleblower](https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump)
* [Mark Zuckerberg breaks silence on Cambridge Analytica](https://www.theguardian.com/technology/2018/mar/21/mark-zuckerberg-response-facebook-cambridge-analytica)
* We are investigating the circumstances in which Facebook data may have been illegally acquired and used,” said the information commissioner Elizabeth Denham. “It’s part of our ongoing investigation into the use of data analytics for political purposes which was launched to consider how political parties and campaigns, data analytics companies and social media platforms in the UK are using and analysing people’s personal information to micro-target voters.”

the Federal Trade Commission is taking action against Twitter, Inc. for deceptively using account security data for targeted advertising. Twitter asked users to give their phone numbers and email addresses to protect their accounts. The firm then profited by allowing advertisers to use this data to target specific users. Twitter’s deception [violates a 2011 FTC order](https://www.ftc.gov/news-events/news/press-releases/2011/03/ftc-accepts-final-settlement-twitter-failure-safeguard-personal-information) that explicitly prohibited the company from misrepresenting its privacy and security practices. Under the proposed order, Twitter must pay a $150 million penalty and is banned from profiting from its deceptively collected data.

Amazon is facing a fine of £636 million for breaching the General Data Protection Regulation (GDPR). The huge fine is being issued by Luxembourg’s data protection regulator. It is the biggest GDPR penalty issued to date and is more than double every other GDPR fine combined. The ruling was made on 15 July. But the fine only became public knowledge when Amazon published its latest quarterly earnings. AMAZON

The Regulation also sets out how organisations can use your personal information. Very little is known about this case, but Luxembourg’s National Commission for Data Protection claims Amazon’s processing of personal data breaches EU law as its advertising system isn’t based on “free consent”. Under GDPR, “consent must be freely given, specific, informed and unambiguous. To obtain freely given consent, it must be given on a voluntary basis.”

The project faced significant backlash as it became public knowledge that Google was gathering healthcare data from a vast number of individuals without their knowledge or explicit approval. This incident prompted widespread discussions on the ethical considerations of data collection and processing within the healthcare industry, underscoring the essential requirement for transparent and unequivocal consent in all data practices.

**Reference:**

* Cadwalladr.C & Graham-Harrison.E(2018).The Guardian. *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.* Available from: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>[accessed 4 October 2024].
* Henderson, J. (2022) FEDERAL TRADE COMMISSION PROTECTING AMERICA’S CONSUMER*.FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads.* Available from: <https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads>[Accessed 4 October 2024]
* KP/LAW(nd). Keller Postman UK*.Amazon fined £636million for GDPR breach* .Available from: <https://www.kpl-databreach.co.uk/amazon-fined-636-million-for-gdpr-breach/> [Accessed 3 October 2024].
* Rehman,I.(2019). University of Nebraska - Lincoln DigitalCommons. Facebook*-Cambridge Analytica data harvesting: What you need to know*. Available from: <https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=5833&context=libphilprac> [Accessed 3 October 2024].
* Scheble,C. Elger,B. Shaw,B.(2020). National Library of Medicine. *Google's Project Nightingale highlights the necessity of data science ethics review.* PMC7059005.Available from: <https://pmc.ncbi.nlm.nih.gov/articles/PMC7059004/> [Accessed 3 October 2024]