# Reflective Activity 2

**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.

---

Cambridge Analytica was able to collect such a vast array of information because of permission settings on sponsored quizzes presented to unsuspecting users. The personality quiz used to collect the data “required users to grant GSR [Global Science Research, the company who administered the test in cooperation with Cambridge Analytica] access to their Facebook profile, which granted access to users’ friends data through the Facebook open API” (Isaak & Hanna, 2018). This is in clear violation of multiple ethics codes concerning the use of data outside of the scope of permission (ACM, 2018; BCS, 2018; IEEE, 2020).

But this also underlines the reach of the permission requirements various applications enforce to access their content, and a lack of inertia for change on behalf of the public who uses these products. In part because of the fallout of the Cambridge Analytica scandal, it is now hardly a secret that advertisers are the true clients of IT companies and users’ details, attention, and data are the product (Kourtellis et al., 2017). As such, there would be an advantage to embed the ability to access as much as possible a user’s information to meet the required expectations of data

volume by companies willing to pay. Users, for their part, often exhibit behaviours characteristic of the ‘privacy paradox’, wherein “users claim to have privacy concerns but do not behave accordingly as they engage” (Barth et al, 2019) with media that requires the release of sensitive information in trade for basic access. The discrepancy in abstract opinion and applied behaviour could be due to the immediacy of application use and the abstract nature of ‘privacy’ in the digital age. In combination these two aspects prime unscrupulous companies to use collected data in unintended or illegal ways.

Though, inappropriate use of data is not confined to the world of social media and online commerce. Statistics Canada caused a major scandal nationally when “it announced it was requesting personal banking data for a sample” (Grenville, 2018) to provide a ‘big data’ survey on Canadian household spending in 2018. The data was requested of banks and credit card companies “of at least half-a-million Canadians without their knowledge or consent” (Zimonjic, 2018). Ultimately the request was halted by the Office of the Privacy Commissioner of Canada (OPC), and StatCan was instructed to overhaul its programs “so as to respect its lawful authority and the principles of necessity and proportionality” (OPC, 2019) in regards to transparency and data privacy.

These examples, though they are dissimilar in scale and outcome, present the ability for data to be shared to scale without proper authorisation of the data subject in order to satisfy conclusions for predetermined variables. In the Cambridge Analytica scandal, researchers were interested in personality profiles to sway voting behaviour; in the StatCan scandal, government officials were looking to fast track the traditional survey through use of ‘big data’. Both felt justified using unauthorised data inappropriately to these ends.

The StatCan scandal highlights how any dataset can be acquired and repurposed without user consent; this has big implications for healthcare data and the security of companies who have access to unauthorised datasets. If StatCan databases were breached, would the department be held legally responsible to the subjects whose data were stolen, as there was no granted permission to be in possession of the data in the first place? Litigants often need to have evidence of “probabilistic harm strain […] intangible harm strain [or] temporal strain” (Haley, 2020: 1193) to sue successfully, and since breached data is often sold in the dark web evidence of harm may never surface. Protection of the individual, who must provide personal information to function in society, should come before ease of data acquisition.

To prevent the type of data misuse conducted by Cambridge Analytica, an immediate deterrent puts the onus of responsibility on the user: s/he must stop giving excess permissions to applications. Companies will not curtail their ability to make money, so the user must limit the supply to the demand. If users are the product, their their consent is their power. But again, the onus is on the user who may not have a desire to change their application usage. Governments do regulate data privacy (GDPR, 2018), yet the ability and rate of data sharing is changing quickly as API use becomes more ubiquitous (Siriwardena, 2020), and may once again outpace legislation. Permissions denial may be the surest way to prevent another data scandal of this nature.

References

ACM. (2018) ACM Code of Ethics and Professional Conduct. [Available Online] https://www.acm.org/code-of-ethics

Barth, S., de Jong, M. D. T., Hartel, P. H., Junger, M., & Roppelt, J. C. (2019) Putting the Privacy Paradox to the Test: Online Privacy and Security Behaviors among Users with Technical Knowledge, Privacy Awareness, and Financial Resources. *Telematics and Informatics*, 41: 55 – 69

BCS (2022) Code of Conduct for BCS Members. Available at: https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf

GDPR (2018) General Data Protection Regulation (GDPR). *General Data Protection Regulation (GDPR)*. [Available Online]: https://gdpr-info.eu/

Grenville, A (2018) *Scandal*, *Surveys and Statistics – An Example of the Transformation of Insights | Linkedin*. linkedin.com. [Available Online]: https://www.linkedin.com/pulse/scandal-surveys-statisticsan-example-transformation-andrew-grenville

Haley, T. D. (2020) Data Protection in Disarray. *Washington Law Review*, 95 (3): 1193 - 1252

Hanna, M. J. & Isaak, J. (2018) User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, 51 (8): 56 – 59

IEEE (2020) IEEE Code of Ethics. [Available Online]: https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/corporate/ieee-code-of-ethics.pdf

Kourtellis, N., Laoutaris, N., Papadopoulos, P., Rodriguez, P. R. (2017) If You are Not Paying for It, You are the Product: How Much do Advertisers Pay to Reach You? In: *2017 Internet Measurement Conference*: 142 - 156

OPC (2019) Statistics Canada: Invasive Data Initiatives Should Be Redesigned with Privacy in Mind. Office of the Privacy Commissioner of Canada. [Available Online]: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2018-19/pa_20191209_sc/

Siriwardena, P. (2020) Advanced API Security: OAuth 2.0 and Beyond. 2nd Ed. New York, NY, USA. Apress.

Zimonjic, P. (2018) *Privacy Commissioner Launches Probe into StatsCan over Collection of Financial Data | News*. CBC. [Available Online]: https://www.cbc.ca/news/politics/personal-financial-information-statistics-canada-1.4885945