Daniel Rance
49144736
dra124

MBIS623 Assessment 1

Data Handling Ethics Report

"How do you propose to bridge the gap between the Foodstuffs' data management practices for third-party browser cookies and the principles for online data ethical handling referring to the concepts in the OECD Fair Information Processing Guidelines?"

There are various governing bodies, both national and international, that inform data handling enterprises of their obligations in the realms of data privacy and data security. In some nations, these information guidelines exist more as ethical principles and have not yet been passed into law. In an increasing number of countries however, rules and restrictions governing use and misuse of data has been successfully legislated. One such example is the Privacy Act 2020, which the New Zealand government enacted in December of last year. The bill, among other things, sought to "promote and protect individual privacy" by "providing a framework to protect an individual's rights to privacy of personal information".[1] This 218-page document codifies into law a myriad of regulations that all data-handling enterprises in New Zealand, commercial or otherwise, must abide by. One such enterprise is Foodstuffs. Foodstuffs is one of the largest and most profitable organizations in New Zealand, employing over 39000 people in several retail chains across the country.[2] Each of Foodstuffs' retail brands have their own privacy policy but, for the purpose of this essay, they can be considered functionally equivalent. My main source for topics of discussion throughout this essay will the privacy policy for the supermarket chain New World, which can be found on their website.[3] In this essay I will first provide a brief history of the development of information handling guidelines and principles across the world. I will then explore the relationship between the privacy policy of New World (and Foodstuffs as a whole) and the legislation by which they are bound. I will highlight any possible inconsistencies within these privacy policies and how Foodstuffs can improve their systems and policies to best comply with its legal obligations, particularly regarding its data management practices for third party browser cookies. Specifically, I will be discussing any such malpractice in relation to the Privacy Act 2020 (NZ), the OECD Fair Information Processing Guidelines, and the ethical principles outlined in Data Management Body of Knowledge (DMBOK) Volume 2.

There has been a long history of regulatory advocacy and changes leading up to the first recognition and implementation of ethical information use standards. In their 1890 book *The Right to Privacy*, American lawyers Samuel Warren and Louis Brandeis concluded that "the protection afforded to thoughts, sentiments and emotions, expressed through the medium of writing or the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone."[4] As part of their arguments, Warren and Brandeis described information privacy as a fundamental human right, that had precedent in several of the United States Constitutional Rights. While their body of work did not immediately lead to a constitutional amendment, *The Right to Privacy* became a hugely influential piece, even being described as

[1] (Ministry of Justice Privacy Act 2020, New Zealand Parliament)
[2] https://www.foodstuffs.co.nz/corporate-responsibility/
[3] https://www.newworld.co.nz/privacy-policy
[4] https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

"perhaps the most influential law journal piece ever published."[5] Brandeis himself would go on to become a Supreme Court Justice in 1916 and, it was through his work, the work of Warren, and the efforts of the countless others who took up this mantle of information privacy after they were gone, that the eventual enshrinement of these principles into U.S law came to pass.

On the other side of the Atlantic, the first real sign of European information rights came in the form of the *European Convention of Human Rights (1950)*. This convention came against the backdrop of a continent shattered by a horrific war and shocking human rights abuses. In recognition of these atrocities, and in the interests of a new, progressive Europe, the Human Rights Convention sought to describe and enshrine several human rights which they saw as "fundamental in upholding the right to Human Dignity"[6]. Two such rights were the general 'right to privacy' and the specific 'right to information privacy'. This historic convention eventually came to influence and provide precedent for the OECD Principles for Fair Information Processing released in 1980. These guidelines provided a framework and common template for all OECD nations to base their own privacy policies and standards on and, ideally, legislate as such. The guidelines recognized "that although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and free flow of information."[7] As such, in virtually all OECD nation's individual privacy laws, you will find some reference or deferment to the OECD guidelines. This is the case in the New Zealand Privacy Act (2020) which states its purpose of "giving effect to internationally recognized privacy obligations and standards in relation to the privacy of personal information, including the OECD Guidelines and the International Convent on Civil and Political Rights. Given the rapid rise in both data quality and quantity that came with the advancement of the information age, the guidelines had to be adapted, and revisions to the guidelines were implemented in 2013. This acknowledgement of digital flux and the ability to be agile allows the OECD guidelines to remain relevant in a fast-changing digital landscape.

As a New Zealand organization, Foodstuffs is obliged to follow New Zealand law and any/all international convents/treatises that New Zealand holds itself to. As such, Foodstuffs has an obligation to follow the principles set out in the OECD Fair Information Processing Guidelines, including the OECD Privacy Guidelines and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Specifically, there are 8 Principles of National Application that all OECD member states (and the data handling enterprises within those member states) are expected to uphold. These principles are:

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

[5] P. Dionisopoulos & C. Ducat, The Right to Privacy (1976).
[6] https://www.echr.coe.int/Documents/Convention_ENG.pdf%23page=9
[7]https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

By browsing New World's privacy policy, we see many references to these OECD Principles. New World clearly outlines the purpose, application, and specifics of its privacy policy and, at first glance, it appears they are taking their commitment to data use and transparency seriously. If we take a closer look, however, there appears to be at least one principle where New World's privacy does not satisfy the requirements of the guidelines, specifically the **Use Limitation Principle**. In my opinion, New World is not meeting its obligations regarding this principle, most notably through its use of third-party cookies.

The Use Limitation Principle states that:

> "Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
>
> a) with the consent of the data subject; or
> b) by the authority of law.

By inspecting the applications hosted on the New World website we can see that there are four different cookie collectors: New World, hotjar, Qualaroo, and doubleclick.net (Google's ad tracking service). Here we see a good example of 1st party cookies interacting with 3rd party cookies. New World outlines its reasons for collecting your information from you (cookies), namely, to maintain and enhance the services it provides. New World does also make a very brief mention of 3rd party data collectors in its privacy policy, and that they may be contracted to access your data and provide services on their behalf. However, New World does not mention which services are contracted or the physical location of those contractors. New World also does not provide any information relation to the privacy policies of said contracted organizations. Qualaroo, hotjar and Google are all American organizations. For security reasons, data storage specifics are not always made public, but it is reasonable to assume at least a portion of the data that these companies gather is stored in the United States. Ethical qualms stemming from moving data across borders without express consent aside, there exists a further issue to data being stored in America. Following the September 11, 2001 attacks, the United States Congress passed the *Patriot Act* which, among other things, allowed the United States government access to any and all data held within the borders of the U.S or by companies that operate within the U.S[8]. That means that, even if Google were able to find offshore data storage facilities to store all its data, that data could still be subject to investigation. It may seem that someone's muesli bar of choice, or the store from which they shopped on the 3rd of May, may not be of critical importance to the U.S government, and that may be true, but what if was data collected on how much alcohol was consumed in a particular community? Or which communities were most responsive to an increase in alcohol advertisement? Obviously, we want to assume best intentions from our elected officials but there is an undeniable level of risk associated with ill-intended or misguided data operators. Every data point collected from users has an innately human element that cannot be ignored. The disregard and trivialization for what is ultimately quite intimate and personal information appears to be commonplace in most Western enterprises and does not come close to beginning to consider different cultural perspectives.

Companies such as New World will often add statements such as 'your continued use of this product constitutes your consent for us to gather and utilize your data in these areas'. While, legally, this may prevent New World from any kind of recourse, there are some ethical principles here which I believe are being infringed upon. For consent to be truly consensual, it needs to be *informed* consent. There are many situations where someone using New World's physical or online services

[8] https://www.justice.gov/archive/ll/highlights.htm

would not be able to provide informed consent for their data to be collected. Some users with intellectual impairment for example, or other users with limited or no English language ability, limited literacy, different cultural values/beliefs, or even people who did not take the time to read New World's privacy policy. All these groups would be at a significant disadvantage when it comes to making an informed consensual decision regarding the use of their data, further compacting the negative power dynamic that these groups already experience at disproportionate levels.

As treaty partners, it is also of critical importance that we consider the topic of Maori data sovereignty. To many Maori, data and information about people and resources is considered tapu, and the non-consensual extraction and utilization of this data can be seen as a form of digital colonisation. There exists already a significantly gap in the economic resources of local iwi (and countless other indigenous groups across the world) and the large multinational organizations that profit from the data collected from them. Very seldom is this profit invested directly back into the community in question, and it is very unlikely that the individuals in that community will ever realize the full value of their collective data. In my opinion, we have an obligation to ensure equitable outcomes for all New Zealanders, and to strive to not compound and repeat the injustices of the past. I also think that this raises the wider question of *all* non-consensual data collection, and what kind of obligation data collection/harnessing enterprises have towards renumerating or compensating their primary resource – the user. Is the result of user-specific targeted advertising sufficient compensation for the loss of data autonomy? I would say that it is not.

Ultimately there is not much that New World, or its parent company Foodstuffs, can do to alter the wider digital landscape, or the complex and historic social injustices faced by some members of that digital landscape. However, I do believe that they can be much more transparent about their use of 3rd party cookies. Such actions could include providing detailed documentation regarding which 3rd party contractors are used, the scope of each 3rd party contract, the intention of each 3rd party contract and the privacy policy of each 3rd party contractor. I would also encourage them to take a more proactive approach towards obtaining informed consent. Personally, I would recommend an 'opt-in' system, where users were required to read, sign, and submit an application for their data to be collected and whether or not they consented for 3rd party sources to also collect data. I would also encourage Foodstuffs as a whole to develop an Ethical Data Handling Strategy and Roadmap, as outlined in DMBOK Volume 2. Developing a roadmap would allow Foodstuffs to fully analyse its current level of ethical data compliance, as well as the steps required to upskill its staff and improve its systems to reach the desired level of ethical compliance.

Obviously, different organizations will reach different conclusions regarding their desired level of ethical compliance (some may decide that their systems are already perfect) and there is not always a clear economic incentive for an organization to devote the time and resources towards pursuing a more complete privacy policy. While some businesses drag their heels on financial grounds, there has been some movement in the legislative space, where some local municipalities have legislative changes that provide even more empowerment to the consumer through stricter data regulations on businesses. The California Consumer Privacy Act (CCPA) came into force in 2018 and stipulates three key requirements on businesses: users can ask what data a company has stored on them, users can ask a company not to sell their data, and users can ask a company to delete their data. This change makes a significant advancement towards rebalancing the power dynamic between user and organization, as well as instructing organizations to better satisfy the ethical principles outlined in the OECD guidelines. Large private organizations can also be the driving force behind industry wide change. Google recently announced it will be phasing out its use of 3rd party cookies over the next

two years[9]. This move comes with increased significance when considering Google Chrome's 69% market share[10].

I believe that the aforementioned lack of immediate economic incentive is subject to significant change. Increasingly we are seeing a new consumer class that is incredibly motivated to support organizations that most align with their ethical principles. I believe that as we see the growth of this ethical consumer class, more businesses will deem it prudent to invest further in their ethical data standards. Profit is obviously an incredibly powerful metric when it comes to influencing business decisions, so it is likely that, with shifting consumer sentiment, we will eventually see some industry wide movement towards a more consensual consumer/organization relationship. It will be up to New World, and Foodstuffs as a whole, to navigate the shifting digital landscape and work in not only the best interests of their shareholders, but in a manner that best considers ethical principles relating to its consumers.

Word Count: 2466

[9] https://www.business-standard.com/article/technology/won-t-adopt-new-tracking-tech-after-phasing-out-third-party-cookies-google-

[10] https://netmarketshare.com/browser-market-share

Daniel Rance
49144736
dra124

Bibliography

Congress, U. S. (2001, October 25). *The USA PATRIOT Act: Preserving Life and Liberty*. Retrieved from justice.gov: https://www.echr.coe.int/Documents/Convention_ENG.pdf%23page=9

Ducat, P. D. (1976). *The Right to Privacy.*

Foodstuffs, N. (2021). *Here for NZ.* Retrieved from foodstuffs.co.nz: https://www.foodstuffs.co.nz/corporate-responsibility/

Google. (2021, March 3). *Charting a course towrads a more privacy-first web*. Retrieved from blog.google: https://blog.google/products/ads-commerce/a-more-privacy-first-web/

Ministry of Justice Privacy Act 2020, New Zealand Parliament. (n.d.). *Privacy Act 2020.* Retrieved from New Zealand Leglislation: https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html

NetMarketShare. (2021, May 10). *Browser Market Share*. Retrieved from NewMarketShare: https://netmarketshare.com/browser-market-share.aspx?options=%7B%22filter%22%3A%7B%22%24and%22%3A%5B%7B%22deviceType%22%3A%7B%22%24in%22%3A%5B%22Desktop%2Flaptop%22%5D%7D%7D%5D%7D%2C%22dateLabel%22%3A%22Trend%22%2C%22attributes%22%3A%22share%22%2C%22group

OECD. (2013). *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data.* Retrieved from oecd.org: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Rights, E. C. (1950). *European Convention on Human Rights.* Retrieved from echr.coe.int: https://www.echr.coe.int/Documents/Convention_ENG.pdf%23page=9

Warren, S. D., & Brandeis, L. D. (1890, December 15). *The Right to Privacy*. Retrieved from cs.cornell.edu: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

World, N. (2021). *Privacy Policy*. Retrieved from New World: https://www.newworld.co.nz/privacy-policy