Darpan Dodiya

BUS501 - Strategic Management Foundations

11/25/2019

Ethics

This paper discusses the topic of ethical dilemmas for businesses. Later on, it outlines how our semester business project, 'VitalWatch' could face one of these ethical dilemmas. Lastly, it tried to provide potential solutions to tackle this dilemma.

The dilemma of data privacy

As a part of the BUS501 course project, we are building a smart health watch manufacturing company, VitalWatch. Smart health watch is a wearable device that can track a lot of information about its users, thus I've decided to take up the dilemma of user data privacy for discussion in this paper. A simple example of this privacy dilemma is, whether to be like Facebook to collect and make money on the user data -or- be like Apple to put utmost focus on user privacy while increasing costs.

Position taken by others

This section looks at the positions taken by other reputed publications on the privacy issues.

An article on Financial Times by Frank Buytendijk and Jay Heiser [1] considers the delicate balance between the benefits that big data analytics bring, and the ethical and privacy risks they pose. The article quotes, "Big data, like most innovations, is a double-edged sword. It brings huge benefits. It allows organisations to personalise their products and service on a massive scale; it fuels new services and even business models, and can help mitigate business risks. At the same time, allowing data scientists to run amok can harm individuals and institutions in unanticipated ways." [1] The article concludes with suggestions that we should Initiate debate by posing ethical dilemmas and that an business should have code of conduct.

Second reference is a paper written by Mollie Gerver and published by The London School of Economics and Political Science. [2] It presents challenges of data privacy that an NGO faces to support refugees from third world countries. The paper talks that decisions surrounding data privacy are not easy to make. It concludes with an interesting remark that "Though violating privacy is generally unethical, we should make exceptions in some such cases. This is far from ideal, but is the only way to ensure the principle of consent is upheld." [2]

The third paper is "Technology as a threat to privacy: Ethical Challenges to the Information Profession" by J J Britz. [3] The aim of this paper is to assess the impact of technology on the private lives of people. Per the paper, applicable ethical norms which can act as guidelines as well as instruments of measurement must be formulated to address ethical issues for any corporation. The three suggested ethical norms are:

- Truth. Truth as an ethical norm has a dual ethical application.

- Freedom. According to this norm a person has the freedom to make choices in terms of freedom of privacy and freedom from intrusion.
- Human rights. This norm is closely related to freedom, but can be regarded as a more concretely applicable norm.

Privacy dilemma of VitalWatch

As described in the Financial Times article [1], as a company operating in health sector, our company will have to face privacy dilemma at some point of time. An example given in the article was of a pharmaceutical company. For example, if a pharmaceutical company analyses DNA data, lifestyle data and socio-demographic data, on the lowest level of granularity, and draws interesting conclusions about health perspective then shares this data. But not sharing those insights could be unethical as well. What should the pharmaceutical company do? [1]

Similarly, VitalWatch will also have access to its user's data such as: precise GPS location, contacts list, heart rates, blood pressure readings, stress information, steps information, oxygen saturation information…the list of user data that we could potentially track is endless. So much so that we could possible have much more information than what Facebook or Google has about its users.

The dilemma here is how should we use the data. We could store the sensitive data on the company servers with extreme focus on user privacy. Only the user will have access to the encrypted data, no one else. This would mean that we have to invest heavily on our security systems and since we would not be utilizing the data, we wouldn't have to miss a significant revenue stream for our company. Over 86% of Google's revenue is from ads, which is targeted by using user data. [5]

The counterpart to that is we collect as much data as possible from the wearable device. We could try to anonymize the data and then sell it to interested parties. The interested parties could be hospitals, insurance companies, government agencies, medicine and pharmaceutical companies, research labs and ad targeting companies. As The Economist famously once said, "The world's most valuable resource is no longer oil, but data". [6] There will be no shortage of companies willing to buy extremely detailed user data. Data will bring massive revenues to the table. This would mean that our company would be able to offer products at much cheaper starting prices, for example a watch that starts at $99. Additional revenues would also mean that we'd be able to invest heavily into R&D department of our company. This extra spending on R&D will further decrease costs while bringing more innovations and quality at rapid pace.

How to deal with the dilemma

Many of the referenced sources in this paper have described steps to solve the privacy dilemma. As Frank Buytendijk suggested in his article [1], the first step we'd do is to have organization wide Code of Conduct.

The Code of Conduct will try to make sure that only a handful of people will have access to the user's data and every access to the data will be logged and audited. Ethical guidelines require regular attention and reinforcement. We'll make sure guidelines are part of every business case and proposal and are part of a checklist when running campaigns or other analytical activities, send out reminders to critical staff, and solicit

feedback from people involved on how the principles have been helpful. Guidelines are only effective when they are top of mind and enforced.

Another consideration would be 'opt-out-by-default' method. Our product will require active consent from the user in order to share his/her data to third parties. Almost all products these days have opt-in-by-default data collection and sharing terms. Our company will take opposite stance by giving users control to their private data.

We'll also remain 100% complaint with GDRP (General Data Protection Regulation) and HIPPA (Health Insurance Portability and Accountability Act) laws to steer clear of any potential lawsuits related to data privacy.

For any critical decision involving privacy, we'd take the decision by following Stakeholder Analysis approach as presented in The 10 Day MBA book. [7]

Combining all these considerations, VitalWatch would be able to deal with privacy issues efficiently while not going bankrupt.

References

[1] Confronting the privacy and ethical risks of Big Data, Frank Buytendijk and Jay Heiser
https://www.ft.com/content/105e30a4-2549-11e3-b349-00144feab7de

[2] "Data Privacy: an ethical dilemma" by Mollie Gerver
http://eprints.lse.ac.uk/79196/1/LSE%20Government%20%E2%80%93%20Data%20Privacy_%20an%20ethical%20dilemma.pdf

[3] "TECHNOLOGY AS A THREAT TO PRIVACY: Ethical Challenges to the Information Profession"
J. J. BRITZ
http://web.simmons.edu/~chen/nit/NIT'96/96-025-Britz.html

[4] Resolving ethical dilemmas about privacy and confidentiality. Guidelines for decision making.
Weber LJ
https://www.ncbi.nlm.nih.gov/pubmed/10128838

[5] Google Investor Relations
https://abc.xyz/investor/

[6] The world's most valuable resource is no longer oil, but data
https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

[7] The Ten Day MBA – Steven Silbiger