

When a retailer sells your personal information to others for profit, it raises many ethical quandaries. One of those quandaries is how personal is the data being sold? This affects the retail customer because if the data is very personal, such as credit card numbers or SSNs, the customer is at risk of their identities being stolen or at the very least, much of their money. This can affect the data buyer as well, as if the data is less personal, the company or individual buying the data may not be able to analyze the data to its full potential. This also obviously affects the data content, because depending on how personal the data is, it could include certain fields such as full names, dates of births, etc. The ethical quandary of “Is the data anonymized” raises the same concerns as the first quandary on my grid, and has many of the same checked boxes. This question affects the retail customers, data buyers, and data content in much of the same ways, but also can affect the software involved. For example, if the data was to be anonymized before being sent to the data buyer, the retail company would have to make software to take out every name in the data either after obtaining the data or before sending it.

How willing the retailer is to sell the data of its customers also raises an ethical dilemma. If the retailer is too willing to sell the data, and sells it to anyone that matches a certain asking price, customers could be negatively affected as their phone numbers may be added to multiple call lists, leading to many being annoyed and some losing money. This could also in turn negatively affect the retailer, as if the information got out that they were loosely selling their customers information, they would most likely lose many customers. Also, the data buyer’s ease of access to the data would be affected depending on how willing to sell the data the retailer is. The final ethical quandary I put in the grid is “Does the data require consent to be sold”. This is important to the socio-technical system of the laws protecting one’s privacy because if the data does require consent that means there is a law in place that the retailer must follow. This also impacts the retailer because it makes them need to add a step to gain consent from their customers, which usually means a change in the retailer’s software. This also affects the customer because it helps contain those that do not want their data to be public to keep it private and secure.