I chose to look at the ethical quandaries surrounding retail stores selling personal information. I identified potential quandaries as: Users’ right to privacy, users don’t know who the data is being sold to, users may be underinformed to consent, and the use of information may go beyond marketing. The simplest, the right to privacy, stems from the fact that most people would likely prefer that information about themselves remain only between themselves and those they actively choose to share it with. A right to privacy is a commonly held belief, and businesses collecting and selling such personal information can easily cause one to feel that right is being infringed. Similarly, even if a user knows their data is being collected, they may not be completely aware who that data is being sold to, if they even know it is being sold at all. Users not knowing who their data is being sold to can raise serious questions, especially if the user would otherwise object to the specific third party receiving their data. Many end users may not even get that far, not realizing that their data is being sold against what they would like, such as consumers who may agree to a EULA or terms and conditions without reading the entire thing—while they agree to it, they may be ignorant to what exactly they agree to, which can cause further ethical debates. Finally, third parties may want the information for purposes outside of what users may expect. For example, a user may be aware that information is being collected to provide more accurate “targeted ads”, but they may not be aware what specific information is being collected and how it is specifically being used.

For some systems that would likely be affected by these quandaries, I identified: The public’s trust in businesses, the process of data collection and targeted advertising as a whole, measures for data security, and the shift towards e-commerce over traditional shopping methods. For users’ right to privacy, I said that the ethical quandary affected public’s trust in businesses, data security, and use of e-commerce. Needless to say, feeling as though a company betrayed your right to privacy would severely damage one’s trust in said company. Data security might also be compromised, especially if the third party does not have the same standard or level of security when it comes to user data. Finally, it affects a consumer’s use of e-commerce, as data collection, at least at a wide-spread level, is more easily done online, so a user who values privacy may opt to not participate in it. Users not knowing the buyers of their data I said only affects data collection and data security, as the other two require some knowledge/awareness to really have an effect. It affects data collection because many a third party, when given anonymity, can enter a market for buying data with little resistance, and that can provide a security risk for similar reasons as stated before. Users being underinformed can affect one’s trust in a business, the data collection process, and also e-commerce for similar reasons stated above, stemming from feelings of being taken advantage of in a uniquely digital space, setting a precedent where companies get away with such practices as consumers unknowingly agree to it. Finally, the use of the information affects data collection, as companies may collect data outside of purely shopping-related analytics for the purpose of selling.