I chose to focus on the case of a retailer selling personal information to others for profit. For the systems, I honed in on security standards, legal compliance, technical implementation, accessibility concerns, public relations, and industry compliance. The first question I considered was if users understood and consented to data collection. I found that it violated accessibility and public relation concerns because while legally they signed a Terms of Service, it’s likely not many understood the document and could cause concerns for communicating to the public the choices a user made. Next, I asked if users could guarantee the safety of their data. I recognized this as a broad concern for all categories, because a security system could be faulty and allow for data breaches, which could violate legal standards for security. This would cascade into a public relations crisis. It could also be a problem on how a technical system was implemented, especially with respect to industry standards.

Another question worth considering is who are the clients of said data purchasing. This could violate legal compliance, as such clients may be foreign governments or adversaries, in violation of existing laws. Again, this could cascade into a PR crisis. It is also worth considering the level and magnitude of what is being collected. Existing security systems may not be sufficient to store sensitive information versus less sensitive. It also may constitute a legal violation if said data is protected by law. It also may violate existing industry standards about data collection. Finally, methodology of data collection is important as well. Implementation on a technical level may vary, such as collecting an email address when they log in, versus development of a rootkit to collect sensitive system details. The methodology could violate existing standards set by the industry.