I believe that data security and privacy should be a business or development goal. If the customer’s business needs can only be met at the expense of security or privacy, then it may not be a system that should be developed (or at least not one that I would want to be a part of). From my experience, the best way to come up with security and privacy requirements is first identify the absolute minimum data that your system will require. Then, identify the absolute minimum that your system requires in terms of using or storing said data - don’t store unnecessary data. You should also look at the impact of security from the perspective of different stakeholders. Combining these approaches will help to pinpoint the system security requirements.

This is a conversation I had for one of my current projects at work. We have developed an internal business application that allows our users (employees) to reserve workspaces at our campus, but also tries to provide analytics when your colleagues are on campus so that you are more likely to go to campus. One feature we discussed was to record when a user’s work cell phone connected to the work WiFi and develop an algorithm to automatically detect the days of the week you are likely to be on campus. We would then use this to recommend days your colleagues should come into the office so you are there on the same day. While brainstorming this feature, we discussed what data we would need - linking employees to their work phone as well as when and where on our campus it connected to WiFi, and what data we would store - historical employee location data (only on our campus).

We crafted the requirements for keeping our data secure and protecting employee privacy. We then considered how the employee would feel about us accessing and storing this data. What harm could be done with the data if a bad actor gained access? We ultimately decided not to go with this exact feature, as we considered it to be too much of a risk and an invasion of employee privacy. We decided that we’d allow the user to “self-report” their office reservations and only use and store the data of volunteered information. This allowed us to narrow down our data needs. Considering the data needs from different stakeholders and finding the minimum required data meant we could craft the most accurate security requirements for our system.