Many companies have a business model oriented around selling user data. In the words of Richard Serra, “if something is free, you’re the product.” This couldn’t be more true today, with many companies offering a service to their users for no or little cost, which serves the dual purpose of being a data collection platform. The selling of user data has become more and more concerning as people begin to consider data to be owned by its subjects, especially when said data is used to influence political campaigns. These concerns leave companies with ethical questions — how to continue making a profit without infringing on users’ digital privacy rights?

On one hand, were these companies to stop selling their users’ data, except that which is explicitly allowed by the users, the company may suffer in terms of profit. Moreover, the relationships these companies have with others that buy the data may suffer as well. On the other hand, continuing to sell the data is likely to make the companies’ relationships with their users suffer, as they will be less willing to use the platform knowing that their every move is watched, recorded, and sold. Furthermore, storing all of this data and keeping it secure poses its own dilemma. Time and time again companies take the hot seat as news comes out that there was a data breach, and some millions of people’s personal data are turned over to malicious actors. As our ideas about the ownership of digital data evolve, so do the requirements to maintain all of this data and keep it secure.