Brown Data

- Are the Brown data *complete*? In other words, are there any data you expect Brown to have collected on you that you do not see on the dashboard?

  The dashboard displays only the ten most recent *Duo Authentication Events*, however I know for a fact I have signed in with this service more than ten times, suggesting the display omits all but the ten latest attempts.

  While the dashboard includes data on connections to the Brown wireless network, it does not show details on resources or websites accessed through this connection. However, as the owner of the network, it's likely that Brown does collect this information, even if it is not displayed.

  Additionally, I would expect Brown to record the location of each ID swipe, as this data could be valuable for tracking an individual's whereabouts in certain situations. For instance, if someone loses their ID or it is stolen, they could see where it was last used. In cases where a security or behavioural issue arises, location data might provide useful context for identifying who was in a specific area at a given time. However, despite the fact that this information is likely collected, it is not available on the dashboard.

  Finally, while Brown could potentially access all emails sent from a student's school email account—perhaps for investigating policy violations or serious incidents—this data is also absent from the dashboard.

- Do you think all the data Brown has about you should be made available on your personal dashboard, or is there some information you think Brown should not provide?

  When considering whether all data Brown collects should be made available on your personal dashboard, it's essential to weigh transparency against potential privacy and security risks. No system is entirely secure, and there is always some risk—however minor—that unauthorized individuals could access the displayed information. This could happen in various ways, from someone using your laptop without permission to a cyber attack from a remote location.

  For sensitive data like browsing history, while Brown may have access to this information, it's highly personal and most people would likely feel uncomfortable with it being displayed, even privately. Similarly, extensive records of location data, such as swipe access locations, could feel intrusive. If individuals want to monitor this information themselves, they already have tools available, like browser history or Google Maps Location History. Thus, displaying such data on the dashboard may offer little benefit while introducing unnecessary privacy and security risks.

Instagram Data

- **Is it clear what each field represents? Do you think any groups of people might have trouble understanding the data?**

    Yes, the information was very difficult to parse, requiring navigation through obtuse file systems and unintuitively named files. Additionally, it was even difficult to find the online resource where I could download the files in first place.

    I think most individuals without explicit technical knowledge would struggle to thoroughly understand the full scope and implications of the data—particularly if they do not have a particular interest or concerted motivation to do so.

    Both facts are likely somewhat intentional. Facebook is a greatly resourced company, and it is well within their capabilities to create an integrated GUI with which to intuitively navigate this information if they so wished. However, they would likely prefer customers stay ignorant to the true quantity of information recorded about them.

- **What were you surprised by/Was there data you did not expect to see? Why?**

    It was somewhat surprising to see a full log of all advertisements displayed in the last couple weeks. My negative reaction to seeing this information, particularly with regards to just the sheer length of the list, would likely be shared by most users. Hence, I was surprised by the fact that they still share it—however, they would likely prefer not to, and only do as a legal requirement.

    I was surprised to see the full list of synced contacts. I try to reject any request to sync my contacts, and I thought I did with Instagram's request too. But I guess at some point my vigilance accidentally slipped. In this record are contacts I forgot I had, or thought that I had lost with old phones—yet there they were in the list, feeding into Facebook's algorithms: my father's work email, alongside my teachers phone number and my friends full name.

- **Are there dangers inherent in some of the data? Relate this to the Healy article.**

    Yes, a full record of every contact I've ever had in my phone, alongside every single Instagram follower gained, reel watched, and Instagram DM sent, is an *incredibly* potent data set. The quantity of data that could potentially be derived from this data set is truly worrying. I am sure my gender, address, family, occupation, former employment, high school, interests, friend groups and more could be derived. This could help me be identified for targeted ads and content algorithms, alongside potentially more sinister applications such as profiling, stalking, or even social engineering attacks, where this personalized knowledge could be weaponised for manipulation or deceit.