1. Identification risk in anonymized data
   a) The datasets I choose are Credit card transaction data (Montjoye et al., 2015) and Demographic, administrative, and social data about students (Zimmer, 2010). For credit card transaction data, as the paper said, the data could be reidentified in 2 ways. One is that if you know exactly someone's previous actions, for example, he or she went to a specific restaurant yesterday, you can search the dataset for the information to find his transaction history (Montjoye et al., 2015, p.537). The other is that if you have some information about someone's approximate price, date and place of previous transactions, even if the resolution is low, it's still likely to reidentify someone with enough points (Montjoye et al., 2015, p.538).

      For demographic, administrative and social data, the paper showed several ways worried by scholars to reidentify the data, for example, some students may have unique nationalities, or have unique pair of nationality and major (Zimmer, 2010, p.316). The re-identification attack is similar in those 2 cases, for the mechanism is that if you have some information about some person, then you can search the dataset for some person having the information, the more the information, the less likely that there is some other one sharing the same information with the target. Besides, more dimensions of released data means there is more information can be used to reidentify some individual.
   b) For credit transaction data, an example of revealed sensitive information is the track of a person. Since the transaction data includes the place and date of transaction, it's easy to know where the target was at specific time and the home address and habits might be inferred from those data. Another example is the price of each transaction and even the goods or services someone bought, which will be a good reference to guess the economic conditions of the target. For demographic, administrative and social data, an example of revealed sensitive information is the political view of a person, which can lead to political persecution. Another example is the private information only public to some friends, the project employed student as RAs to collect data, so the information collected was what the RA could see, which might include something the target student didn't want to show to strangers.
2. Describing ethical thinking

   "'We're sociologists, not technologists, so a lot of this is new to us' and 'Sociologists generally want to know as much as possible about research subjects.'" [Zimmer (2010) citing Kauffman (Sep. 30, 2008b)]

   Rewrite: According to consequentialism and the principle of Beneficence, the dataset provide valuable data to researchers, which dominates the risk of revealing private information.

   "'What might hackers want to do with this information, assuming they could crack the data and 'see' these peoples Facebook info? Couldn't they do this just as easily via Facebook itself? Our dataset contains almost no information that isn't on Facebook. (Privacy filters obviously aren't much of an obstacle to those who want to get around them.)'" [Zimmer (2010) citing Kauffman (Sep. 30, 2008b)]

   Rewrite: Even if the data is not released, it's not more difficult for hackers to get the information directly via Facebook, so the dataset do not harm anyone. Meanwhile, the dataset provide valuable data to researchers. So it is consistent with the principle of Beneficence.

"We have not accessed any information not otherwise available on Facebook. We have not interviewed anyone, nor asked them for any information, nor made information about them public (unless, as you all point out, someone goes to the extreme effort of cracking our dataset, which we hope it will be hard to do)." [Kauffman (Sep. 30, 2008c)]

Rewrite: We do nothing to those people but just collect public information, so we don't need to ask them for consent; besides, we treat them as autonomous. Our actions are consistent with the principle of Respect for Persons.

Reference

Kauffman, Jason, "I am the Principle Investigator...", Blog Comment, MichaelZimmer.org, http://www.michaelzimmer.org/2008/09/30/on-the-anonymity-of-the-facebook-dataset/, Sep. 30, 2008b.

Kauffman, Jason, "\We did not consult...", Blog Comment, MichaelZimmer.org, http://www.michaelzimmer.org/2008/09/30/on-the-anonymity-of-the-facebook-dataset/, Sep. 30, 2008c.

Montjoye, Yves-Alexandre de, Laura Radaelli, Vivek Kumar Singh, and Alex Sandy Pentland, "Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata", *Science*, 2015, *347* (6221), 536-539.

Salganik, Matthew J., *Bit by Bit: Social Research in the Digital Age*, Princeton University Press, 2018.

Zimmer, Michael, "But the Data is Already Public: On the Ethics of Research in Facebook", *Ethics and Information Technology*, 2010, *12* (4), 313-325.