Question 3

(a) I think the best thing to if it is easier to unhash passwords is to implement multi-factor authentication. Not just 2 factor, but something along the lines of fingerprint and another method on top of the password. In other words, a form of 3 factor authentication. The knowledge should be publicly released so security is not an issue for any company- you should be putting your resources out there for the security of your consumers who will definitely have private information in other no longer secure services too.

(b) You should divulge all information because if you can figure it out there is a high chance a hacker could solve the algorithm as well. This could have catastrophic long-term implications if the problem is not addressed widely and fast.

Question 4

(a) One negative problem to this is that many security issues will arise even outside of passwords and it will be feasible for hackers to get into the data. Hackers could do similar things as they did with passwords to get credit card data by getting into the database. It is not feasible to hash every single bit of data in the database, so this can lead to vast security repercussions.

(b) One possible problem that we can now solve if P=NP is the travelling salesman problem. This could easily solve problems in Amazon for delivery much faster now that it is able to be run in polynomial time. We can pass in the destinations and based on the polynomial time reduction of whatever graph traversal algorithm we decide to use, we are given a list of what destinations to go in order. This can have impacts on fuel conservation and ethical conditions for drivers who will no longer have to drive in the middle of the night.

(c) I think that the majority of things would remain the same. However, many resources would not have to be allocated to potential flaws in programs in case P=NP, or towards theory based security. I don't think this would affect me personally other than I would learn about how P=NP in class.