1. I think in this case WTP is driven mostly by the convenience of service, the quality of search result, and (for some) the accuracy of ads deployment. So, google may have a higher WTP for most. And the cost is driven by the privacy given up by the user combined with how much the user is acknowledged about it. In this aspect, google have a higher cost but because asymmetric Information, this cost is not very high for most because they are not aware of how google treat privacy. Also research show that the willingness to pay for privacy is not very high. So, for most people the utility from Google is higher than utility from DuckDuckGo and they choose to use Google. However, if someone is well-informed about how google mistreat privacy and if he values privacy a lot. It is possible that the utility from Google is lower than the utility from DuckDuckGo) and he choose to use DuckDuckGo.
2. As is discussed in question 1. Asymmetric Information is very important when it comes to privacy. Apple is forcing all apps to disclose what information they are tracking and allow for users to ask app to not track any data. This will make the user more informed about the privacy cost of using an APP and this can help customers make better decisions. And being able to ask app to not track any data can be seen as a way to cut down privacy cost. So this is why apple's action can benefit users. The reason why what apple is doing is unique and different is that most companies make profit on gathering privacy data. And they are more than happy to keep the Asymmetric Information.
   One possibility that this may end up negatively affecting users is that the quality-of-service app can provide may drop. And this may harm user experience. For example, if a user chooses to share approximate location information with Uber. He may be unable to find his uber driver.

3. I don't agree with Carnegie Consortium and I think Rep. John Doe should support the Secure Computing Coalition. Carnegie Consortium's opinion have two main flaws. Firstly, security incidents happened due to user failure does not only hurt the user itself. It also has social costs. Take ddos for example. If a user does not follow good security procedures and his computer is attacked and became a zombie computer. His computer will be used to attack servers or government. Secondly, relying on the market completely is not a good idea. Because there is no way market punish vendors that produce defective software automatically. There is information involved. If the market always have full information of whether a vendor's software are defective, the market may be able to regulate. However, this is typically not the case. So, I think it is unwise to say we can completely rely on the market to regulate. On the other hand, the Secure Computing Coalition's plan is a form of mandated standards. One potential problem is that this may inflict cost for users with small direct damage. In this case, the computing resource cost and time cost for installing firewall even if you will not be the target of an cyberattack. However, I think the cost is low enough compared to its potential benefit. Given it is a very easy task by using automatic system update.