ENGR 101 Tutorial week 1

Please think about these questions in advance. We will divide into groups interested in working on the same question, and toward the end each group can give a two minute or so summary of their thoughts. If you can pick your question in advance that would be great.

It would be difficult to deny that computers have made our lives much better overall. They have reduced mental drudgery, increased standards of living, improved safety …. The positives would make a long list. But as with any enormously powerful tool, there are also great dangers. We want to consider some of those today, and think about the resulting ethical issues for engineers.

1) During the cold war, many scientists and engineers worked on the development of nuclear weapons and the means to deliver them, but others refused to work on these projects. Nuclear weapons were and still are so horrible (some individual weapons were equivalent to hundreds of Hiroshima bombs) that many people thought they were unusable even at the height of the cold war. This was summed in the term “MAD” or “Mutually Assured Destruction,” the idea that these weapons could not be used because the destruction of both sides was assured. Fortunately this was never tested, but we came pretty close on a few occasions. Today our entire civilization is controlled by computers (electric supply, sewers, traffic lights, water, banking ….). Some people think that the destructiveness of an all-out cyber war could approach that of a nuclear exchange. This might that the destructiveness of an all-out cyber war could approach that of a nuclear exchange. This might be exaggerated but at a minimum the consequences would be devastating, and it is proving very difficult to prevent the spread of cyber weapons to terrorist groups and rogue countries. The US claims to have solid evidence that hacking groups linked to Russia worked their way into computers of political groups and voting systems and attempted to interfere with the 2016 elections, and other western democracies claim similar attempts by Russia to interfere in their elections. Under what circumstances is it ethical for an NZ engineer to work on cyber weapons for the NZ government? Howbe exaggerated but at a minimum the consequences would be devastating, and it is proving very difficult to prevent the spread of cyber weapons to terrorist groups and rogue countries. The US claims to have solid evidence that hacking groups linked to Russia worked their way into computers of political groups and voting systems and attempted to interfere with the 2016 elections, and other western democracies claim similar attempts by Russia to interfere in their elections. Under what circumstances is it ethical for an NZ engineer to work on cyber weapons for the NZ government? How about for a friendly foreign government? How about a contractor working for one of these governments?

2) Companies are often under huge pressure to get software to the market in a hurry, and sometimes that may mean taking shortcuts with security. There have been demonstrations of hacking everything from webcams in houses to cars to appliances to toys, and of course computers. This can have quite devastating effect on the victims. What are the obligations of software and hardware engineers in this matter? If you are aware that the product your company is about to deliver is not secure, what should you do? That would likely depend on the kind of product involved, but try to develop some guidelines.

3) We now live in a “surveillance society.” We are on camera pretty much any time we are not in our houses and perhaps even there sometimes, our phones track us, and our internet use is stored and scrutinized to an extreme. This has led to a loss of privacy for individuals that would have been impossible to imagine a generation ago. Ask a tutor to show you an

extreme example of this. Extensive surveillance makes political dissent dangerous in many countries around the world. Under what circumstances if any is it ethical to work on data mining tools and other software that invades privacy?

Please submit a one short paragraph or bullet point summary of your ideas.

- Depending on the product (highly sensitive or less important), it is especially important that security guidelines are followed
- There already exists engineering guidelines which products should follow such as the NIST or the OWASP.
- There is a degree responsibility which lies on the engineer and it is their responsibility to uphold these standards.
- Discuss the problem internally, and if the problem persists, raise awareness.