Growing up, I often spent my summers at my grandparent's farm in rural eastern Iowa. Every year I would look forward to spending a couple of weeks with my Grandparents doing things like hunting, fishing, and admiring my Grandpa's collection of antique tractors. Seeing my Grandfather cherish these tractors left a profound impression on my idea of consumerism. Every purchase you made in your life was an investment in your future. Items are meant last. With this paper, I would like to focus on the right to repair agricultural equipment and how my cultural background and academic experiences influence my thoughts on this important issue.

The Iowa farmer mindset of working hard and making an honest living is integral to who I am. Self-sustainability is an integral part of Iowa farm culture. Fixing something yourself is becoming more outdated as technology advances. Naturally, this sentiment about disposable technology directly contradicts moral beliefs about consumer products. My Grandpa knew every part of his tractors. There was pride in fixing them himself. Ingrained in my mind is the belief that every person should have the access and ability to modify the products they own as they see fit. Therefore I see a direct moral conflict with the approach of some organizations toward the repair rights of farms. Particularly John Deere.

Since the early 1980's cars and other motor vehicles have become more dependent on electronics; according to an article published by the New York Times in 1984, citing research from the University of Michigan, "10 percent of the total value of an average car will be in electronic devices by 1987. And the figure will be closer to 20 percent for luxury cars" (Times). Now that percentage makes up more than 40 percent of the cost of a new vehicle (car and driver). With this field of computerization from a Cyber Security perspective, it is easy to see how this emerging field could be a massive issue. More computerization often translates to more vulnerabilities and surface areas for hackers to target. Consequently, the security of these devices embedded into vehicles must be of the highest degree. In this class, we have talked about countless examples of the abuse of new/emerging technologies. We have discussed whether products should be secure by design or by the user (Ethical OS Toolkit). A malicious actor should not be able to access a car's internal computer and tamper with the source code; however, what if there is an issue with the onboard computer? This is an issue that the dealership should be able to handle. What if that dealership is in the next state? What if you can't afford to drive your car that far? This is the dilemma that many John Deere tractor owners have recently found themselves in.

More of America's agriculture equipment has become digitalized. Tractors, like cars, have embedded electronics integral to the functions of these machines. Unlike my grandpa's old Case IH, if something on a modern tractor breaks, it is much more difficult to replace. If a part needs to be replaced, it must be done at a dealership. This is due to John Deere's policy on repair technology which prevents tractor owners from adding replacement parts on their own. If a tractor has an issue with a GPS navigation system, that farmer cannot purchase and install a new unit independently. John Deere's internal programming will not recognize the part on the machine until a registered John Deere technician can verify the part and enter it into the system. As a result, farmers have been pressured to resolve these issues using illegal software and repair methods, often coming from eastern European hacking forums(Motherboard). The issue present in the right-to-repair policy is a critical moral and ethical issue. From one perspective, I view this issue as any Iowan would: John Deere is trying to make a quick buck and prevent farmers from doing things on their own and the other side, I view this as a security professional concerned for the safety of the user and organization as a whole.

With the means to repair their tractors, farmers are allowed to use illegal resources. Morally, this stance is not something I have been conditioned to condone. From a professional and ethical standpoint as an engineer, this decision by John Deere is something that I can empathize with. My views on individual rights to use technology have changed through my discussions in this course. During the second week of this class, we discussed the Ford Pinto. The Pinto had a design flaw with the fuel tank that made the car leak gas. If the Pinto was involved in a crash, there was a high probability that the car would catch on fire or explode. Ford faced the dilemma of spending money to fix this flaw or deal with the possible injuries this could cause. Ford choose not to fix the issue. Coming into this class, I believed that organizations made decisions based on the idealogy of "this would make us money; let's do it." The Ford Pinto example stood out to me because Ford calculated the risk and determined the cost of life would be less than the repair cost. How do tech companies apply this rationale? Would opening up an entire system for free control by the owner of that system is a technological slippery slope that could lead to unintended consequences? What is the risk?

From the perspective of John Deere, allowing people to repair and modify tractors as they see fit is a quick path to a lawsuit. If a John Deere tractor is modified to operate using a bootleg crop sprayer that releases excessive amounts of pesticides into the soil, is that the farmers' fault or the tractor's? This is still a primary right; however, there are limitations. Granting users the right to repair their devices could be freeing for an organization. Allowing ease of repair and lower operating costs, but conversely, it could give users too much power that could be abused. Farmers are forced to rely on pirated software and illegal repair shortcuts without these rights. Every situation presents unique moral and ethical dilemmas.

Cultural backgrounds are unique foundations that create the platform from which we view the world. Looking at the world through these lenses creates unique outcomes, especially when viewed by a Cyber Security Engineer. My Grandpa had the right to fix his tractors, but my Grandpa didn't have to worry about the potential for his repair to cause irreparable damage to the company that made it. Technology has become intertwined with every industry and every facet of modern life. The tinkering of one user on a network could inadvertently or intentionally create a sequence of catastrophic events.

Times http://nytimes.com/1984/05/15/business/the-computerization-of-cars.html

Car and Driver https://www.caranddriver.com/features/a32034437/computer-chips-in-cars/

Motherboard

https://www.vice.com/en/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware