Ethics:

Taylor Rongaus

Introduction: *the reality of present digital ethical code and the "grey area" between right and wrong*

Today, much of technology is used for the general good of society or to help improve some condition of life. The problem, though, with technology, is that it's an uncharted, new territory. We have a general ethical "code" in society that has been there for centuries, always changing but somehow ingrained in us all. Technology transcends this- there is no strict set of guidelines on how one should navigate the web, so people take it upon themselves to determine what exactly they think is "right" (or really, just not "wrong").

I've always found this topic fascinating. I feel like a pioneer in a way, just trying to wrap my brain around how to define an ethical code where one does not already exist. I really discovered how deep my interest in it was, though, on my first day of Basics of Unix this semester. My professor, Dr. Bui, told us a story that really caused me to question how black and white I had previously seen this issue.

In short, Dr. Bui was a freshman at Notre Dame while his girlfriend at the time (now his wife) was a senior in high school waiting to hear back on her application to Notre Dame. When she heard that she was accepted, Dr. Bui went out of his way to hack into the Office of Housing's database and download the class, dorm, and roommate list to give to her before they released it themselves. Eventually, though, word got out, Notre

Dame realized they had been hacked, and they were able to track down Dr. Bui. They gave him some community service… and also a job offer to fix the holes in their system.

When Dr. Bui told us this story, I was first and foremost impressed that this man was able to do such a thing during his freshman year of college. But as he continued to speak about what we would be learning in his class, I realized that what he had done was not out of the realm of possibility for someone like me. I then questioned my initial impression of this act: was I right to be impressed? Sure, what he had done was impressive, but was it *right*? He hadn't caused anyone physical harm, but maybe he gave the Office of Housing a bit of a headache. I determined that I personally thought what he did wasn't "wrong," but it certainly wasn't "right."

To me, this lack of distinction between "right" and "wrong" is what is so interesting about digital ethics. Ethics is emerging and sides are forming on the issues, but presently, there's a grey area in which anyone can act as they choose and feel completely justified in their actions. I hope to expand upon this example and further expand upon my idea of the grey area and what can be done to create some sort of ethical spectrum within it.

Ethical vs. unethical hackers: *discussions on motives, criminal hackers, Anonymous, and everything in-between*

Recently in Hacking Life class, we had a debate over certain issues of hacking: whether or not Anonymous should be able to illegally publish data on immoral companies, whether or not the NSA should be allowed to collect data on everyday

citizens, and whether or not DNA hacking should be illegal. What was interesting about the debate was that teams were randomly assigned, but everyone was still able to make a solid case for whatever side they were instructed to argue. I walked away after thinking back to the last time I had engaged in a debate of some sort and realized that it was likely way back in high school. In the technical field that I'm in, I'm usually told how to do something and to just do it, so I sit and code behind a screen without really thinking much about the ethical implications of my actions.

From this I came to realize that my mentality probably wasn't very uncommon, this "behind the screen" way of thinking. In fact, I felt like that must be the reason why hackers exist in the ethical "grey area" that I mentioned- they couldn't possibly take time to think long and hard about the implications of their actions. They exist behind a screen. You don't see their face. They're invisible. And their actions are tied back to their IP address, something that all good hackers obviously take care to hide.

Now stop right there. Take a second now to digest what I just said, and picture in your mind what a "hacker" looks like. At this point in time, this was almost the exact image that was in my mind:

 [1]

The problem, though, is that this vision I had was extremely stereotypical of what a "hacker" really is. And the bigger problem is how easily my mind jumped to this idea. These stereotypical hackers do exist (I happen to know a fair few myself), but society perpetuates the stereotype so strongly to the point where it becomes difficult to think of a hacker as anyone other than that geeky kid who sits behind his parent's computer. And if you still don't believe me, note that the image above was taken from *Jurassic Park*, one of the most well-known movies of the century. Sources like The Guardian, however, take care to point out how archaic this stereotype is: one of their articles explains that, "according to research carried out by the online payments company Jumio in 2013, 43% of criminal hackers are aged between 35 and 50 years old. Only 8% of criminal hackers are under 18. Almost a quarter of criminal hackers are women…" [2]. This article, though, also makes the claim that "we can teach young hackers humility and empathy."

[1] Critical Commons Manager. *Hacker Stereotype in Jurassic Park*. Digital image. *Critical Commons*. N.p., n.d. Web. 17 Apr. 2016.
[2] Parkin, Simon. "Ghosts in the Machine: The Real Hackers Hiding behind the Cliches of TalkTalk and Mr Robot." *The Guardian*. The Guardian, 31 Oct. 2015. Web. 8 Feb. 2016.

The question that I take from this though, is do these criminal hackers *want* to learn humility and empathy? Success and fame in hacking is often attributed to the illegal; our stereotypical society devotes headlines to the antisocial kid who was able to break into a multi-million dollar company from his bedroom. You never see the news reporting on people who legally obtain secret information, if that is even possible at all. Is there recognition in playing by the rules?

Similarly, just the word "hacking" has connotations of its own. It's *cool* to be able to hack: imagine if you were able to brag that you could break into any system in the world. Is it as cool to use those powers for good instead of evil?

Ian Reynolds, a security consultant cited in the aforementioned Guardian article, says that "hacking in its purest form attracts highly technical, creative people," and that "they must get a kick out of [it]." [3] And in fact, we, the general computer science community, do. When I personally write even the smallest and most meaningless of codes, there's an immediate, strong sense of satisfaction that comes from when it works. Imagine the thrill and magic in doing something much, much bigger. Think about the little kick you get when you pick a basic lock on a door. It's so similar, but to a hacker, there's so much more to secretly picking these grandiose locks, not having it traced back to you, and being able to watch your work unfold in the public eye.

These thoughts don't answer any questions about digital ethics, and in fact, they raise even more. They do help, though, to understand the mindset of a criminal hacker,

[3] Parkin, "Ghosts in the Machine"

the “why” behind every hack. *Sometimes, it’s just for the thrill.* And is it really so wrong to want to have a little fun?

Keep in mind, though, that *not all hackers are into illegal thrill seeking*: some unethical ones, though, will tend to pursue this route. However, thrill seeking is prevalent still in the most ethical, innocent of hackers. Think of the thrill a policeman gets as he throws on his sirens and chases down his perp. It truly is not a very different feel for those in cybersecurity; if anything, their job to track their perp is much more difficult, and to them, just as thrilling.

Consider the famous hacktivist group Anonymous. One could argue that their role is thrilling, but in reality, whether or not it is has nothing to do with the controversies that their organization brings to light. Anonymous is often in the spotlight for fighting against what they perceive as immoral: they’ve taken down the website for the Westboro Baptist Church, they’ve fought on the darknet to take down child pornography sites, [4] and most recently, they’ve “released” the personal data of Donald Trump to the public. [5]

While the first two of these examples may seem like no-brainer instances of “good” hacking on their part, they all involve Anonymous taking a stance on a moral issue of some sort. They believed the Westboro Baptist Church was hateful and intolerant, so they retaliated. But their retaliation was not necessarily moral either, unless you believe that anyone should be able to take down the website of something

[4] Love, Dylan. "8 Things That Anonymous, The Hacker 'Terrorist' Group, Has Done For Good." *Business Insider*. Business Insider, Inc, 27 Apr. 2013. Web. 21 Mar. 2016.
[5] Hqanon. "How Anonymous Just Fooled Donald Trump, the Secret Service, and the FBI." *AnonHQ*. AnonHQ, 20 Mar. 2016. Web. 21 Mar. 2016.

they don't personally agree with. Not many people want to go to bat for the Westboro Baptist Church, so many people believe that Anonymous was completely in the right to do what they did, and many in fact applaud them for it. But by doing so, are you supporting a less-than moral form of "hacking?"

The example, though, of how Anonymous "released" the personal information of Donald Trump is different from the rest, and is in fact a great example of how society can get caught up simply in the "hacking" mindset. Anonymous is well-known as a "hacktivist" group, i.e., they hack for a cause. So when they declared cyber-war on Donald Trump, the world assumed that they would simply hack into his system and release his information. And they did release his information. And the Trump administration immediately retaliated. But Anonymous actually didn't "hack" anything to get his information: all of what they released was online for years for anyone to see- they just did the digging to find it. Legally, this is not a crime, but higher-ups in the government were quick to see it as one. Is this, then, what "ethical hacking" is- just digging for information that others might not be so quick to see?

When it comes to "hacking" as a concept, there is *much* more than what meets the eye. As you can see, society still tends to get caught up in the word "hack," but this stereotype is not always true: hackers can be anyone at all with Internet access and the drive to learn. The idea of "hacking," though, has transcended beyond this stereotype, to places like the medical industry, the business and banking worlds, artificial intelligence, and even the government.

This is why the discussion on the ethics of technology and "hacking" is so important but so difficult. We are living in a brave new digital world. But as we begin to immerse ourselves in this new world and learn how to embrace it, the ethical issues that we originally brushed over begin to come to light. There is now a discussion on ethics: people are taking sides on the tech stories in the news, like whether or not Apple should hand over their encryption technology to the FBI [6], or like how Anonymous should act and who they should target. This brings about the necessity of a digital ethical code of sorts: when technology gets to such a relevant and extensive point in all of our lives, society as a whole needs to take a step back and define the rules of what is socially acceptable and what is not.

Digital Ethical Code: *an attempt to define one for technology today*

Before I go into attempting to define a digital ethical code for our modern society, it is important to first make some necessary distinctions and study some related ethical codes. In my opinion, it is necessary to look at technology as a whole from two perspectives: as a user and as a developer. "As a user" is your everyday person using a previously created technology in some way, and "as a developer" is someone who is setting out to create a new type of technology. I believe it is important and necessary to make this distinction because these groups of people will ultimately be using technology in very different ways. A user has control over how they use a technology: it's a more personal decision. A developer, though, has more power to create something that can be

[6] Cook, Tim. "A Message To Our Customers." *Apple*. Apple Inc., 16 Feb. 2016. Web. 17 Feb. 2016.

used by people in different ways. For example, if a developer decides to program a robot with a "self destruct" button, it is up to the user of the robot if they would like to press that button or not. Similarly, it is up to a user if they would like to buy their goods via Amazon, Ebay, or other major online shopping websites versus on the deep net in places like the Silk Road.

This "as a user" perspective is commonly referred to as "cyberethics," because most of what a user will do with technology involves using the Internet in some way. Simply put, cyberethics is a code of behavior on the Internet. The company Microsoft, one of the biggest names in technology, has a section of its website devoted to instructing users to "practice cyberethics," and they offer a few suggestions as to how to do so:

- Use the Internet to communicate and interact with people.
- Don't use the Internet to be a cyberbully and don't encourage cyberbullies.
- Use the Internet for research and information, games and music, etc.
- Don't use copyrighted information as your own or download/ distribute it.
- Use the Internet to shop, bank, pay bills, etc.
- Don't share your personal information too readily.
- Use the Internet to expand your networks.
- Don't lie. [7]

Most of these, it would seem, are common sense good judgment calls. But if you reflect on yourself, you will likely recall an instance where you violated one of these

[7] "Practice Cyberethics." *Microsoft: Safety & Security Center*. Microsoft Corporation, 2016. Web. 23 Mar. 2016.

practices. And it's not hard to violate them- that's simply the nature of the Internet. Everything is open source and free-flowing, so it becomes easy to even accidentally illegally download a file or anonymously say something rude to another. In my opinion, though, Microsoft nails this definition of "as a user" ethics. If anything, I personally would add the clause "Don't intentionally harm others." While this may not seem very relevant for simply browsing the Internet, it is more so when talking about using more physical software, such as artificial intelligence, automobiles, banking, medicine, etc.

When it comes to writing software, i.e., "as a developer," it becomes more difficult to determine the boundaries of right and wrong. IBM provides us with an "ethics landscape" [8] of sorts to help us solidify the vast concept of ethics in software development. They break up this concept into several subsets: privacy, encryption, trust, freedom of speech, and intellectual property, and I will touch on these concepts in a way of my own.

According to IBM, the issue of privacy consists of the ideas of freedom from intrusion, control of personal information, and freedom from surveillance. Basically, all human beings have the right to be left alone and control their personal information. The problem with the digital age, though, is that privacy in that regard is essentially impossible. With technology, our information is everywhere online, bought and sold and spread across the globe. Advertisements permeate every website we visit, and millions of computers are part of a botnet of some sort. While it may be impossible to attain pure privacy, it is possible to control what we create. It's possible to create a software that

[8] Pollice, Gary. "Ethics and Software Development." *Ethics and Software Development*. IBM, 15 May 2006. Web. 23 Mar. 2016.

does not collect personal user data and that does not spy on its user's lifestyle, so I propose the following:

Taylor's Digital Ethical Code

1. Create software to be as nonintrusive as possible. Avoid collecting personal user data, and always ask the user before anonymously collecting any of his or her data whatsoever.

If we are creating software, then, to be as nonintrusive as possible, it becomes important to safeguard that privacy. This is where encryption comes into play: if a user decides to use a product, then they expect that the product is safe, so they place their trust into the one who creates the product they are using. Using a product should not intentionally cause any harm to the user, and a company should do their absolute best to protect the user's information, possessions, and overall livelihood. Therefore, I propose:

Taylor's Digital Ethical Code

2. Protect the user: encrypt data, information, and anything else needed to secure privacy. Similarly, do not break another's encryption. Respect the privacy and integrity of others, and always remain trustworthy.

Freedom of speech and freedom of expression are important tenets of any well-functioning society. In the United States, they're important enough to be the First

Amendment of our Constitution. When it comes to technology, though, it may seem like this issue is irrelevant. But in fact, the Internet itself is made up of free speech ranging from blog posts to activism to non-profits and everywhere in between. Similarly, software and products are made with a similar freedom of expression and creativity: you have the right, as an intellectual, to create as you please. However, there need to be limits on this free-flowing creation, so I propose the following:

Taylor's Digital Ethical Code

3. When it comes to developing software, browsing the web, or using technology in any way, you have freedom of speech and freedom of creativity. However, do not use this freedom to cause harm to others, and do not infringe upon the freedom of others.

Because developers and people in general should have the right to create, they also should have to right to own what they create. This is the extremely relevant and important issue of intellectual property. Intellectual property is very difficult to protect in a digital world. Software is generally considered a form of intellectual property, much like we consider music or writing or paintings. However, unlike vinyl records or hardcover books or canvas paintings, software can be replicated and stolen. This is true of these physical examples too: you can create replications of paintings, for example. However, the digital world is open source, and for the most part, software can be viewed, downloaded, copied, expanded upon, changed, or redistributed with extreme

ease. Whether or not is should be, though, is a very hotly debated issue. For the most part, the technological community agrees that a free software should be able to copied, expanded upon, etc: that's part of the beauty of it. Free software should be able to be modified to fit the user's needs. However, consider a TV show that airs on a specific channel that you pay to have access to. It is not fair to the owner of the network and the show that you record the episode and distribute it online for everyone: you're violating their right to make a profit from their intellectual property. Therefore, I propose the following:

Taylor's Digital Ethical Code

4. If the developer does not intend for free distribution of their software, then respect their decision. However, if a software is intentionally made available to the public, feel free to use and alter it as you please.

Obviously, what I have proposed does not encompass every single ethical issue in technology. It is not a black and white set of guidelines on how to act. It is, though, an attempt to solidify the grey area in a slightly more concrete manner. We can use it to look back on some the examples I previously mentioned: Anonymous, by my code, was completely in the ethical right to re-post Donald Trump's information online because it was already out there for anyone to find. However, they were not in the ethical right to shut down the website of the Westboro Baptist Church, because by doing so, they infringed upon the church's right to freedom of speech.

This will make people upset, I'm sure. It bothers me too. But when it comes to digital ethics, it is best not to fight fire with fire. It is best to educate about what is right and what is wrong and to practice what is right. By doing so, I hope and believe that we will be able to create a culture of acceptable growth and usage of the technologies available in our digital world.

Conclusion: *there are no answers, only questions*

While researching into the ethics of technology as a whole, I've tried to determine some thoughts of "big name" scientists, engineers, and figures on the subject; after all, this is a fairly common and important topic to be looking into. I came across some pretty big names almost immediately: people like Stephen Hawking and Elon Musk have a lot to say on the topic. And in fact, Elon Musk recently donated $10 million to the Future of Life Institute, which is an institute based in Cambridge, Massachusetts dedicated to studying and discussing the social and ethical dimensions of technology.

According to their website, The Future of Life Institute's mission is "to catalyze and support research and initiatives for safeguarding life and developing optimistic visions of the future, including positive ways for humanity to steer its own course considering new technologies and challenges." [9] They do research into the developments of AI, biotechnology, nuclear, and climate changes alike, and they are backed by some big names in the field: ranging from celebrities like Stephen Hawking, Elon Musk, and Morgan Freeman to professors from Harvard, Cambridge, MIT, Oxford, and more.

[9] The Future of Life Institute. *FLI - The Future of Life Institute*. Web. 17 Feb. 2016.

What's important about institutions like The Future of Life is that they aren't trying to limit or hinder technological development; instead, they're trying to protect its integrity. Elon Musk's donation to the institution was "to run a global research program aimed at keeping AI beneficial to humanity." [10] As technologies develop so rapidly, it becomes more and more important to research on the ethical implications of those developments and where it becomes necessary to draw the line. Musk has similarly helped another organization, OpenAI, who currently has $1 billion in backing in order to create an open-source institution that is dedicated to promoting shared research into the AI field, proving the need for the balance between development and ethics.

Clearly, though, beyond AI and beyond the world of "hacking" behind a screen lie vast ethical dilemmas that concern *technology as a whole*. When is enough enough? How do we build human ethics into machines? And should these ethics be set in stone? To give an everyday example, consider a typical person driving a car. It might be easy to imagine, but in reality, everyone drives differently. How do you personally react in a crisis scenario on the road? Do you give more space to a cyclist on the road if it means driving closer to another lane of traffic, or vice versa? What about a self-driving car? How do we determine what the car will do in such a scenario if there's no set human rule of what should be done?

It's exceedingly difficult, but exceedingly important nonetheless, to try and determine a concrete way of answering questions like these. There likely won't be a right answer that satisfies every person's beliefs and the law: my ethical code certainly does

[10] Thornhill, John. "Brave New Era in Technology Needs New Ethics." *Financial Times*. The Financial Times Limited, 20 Jan. 2016. Web. 17 Feb. 2016.

not. But by simultaneously researching into the science and ethics of these topics, we can create a more accepted standard for people to abide by, which, in my opinion, is much better than having freely growing technological development with no censorship whatsoever.

Endnotes:

Cook, Tim. "A Message To Our Customers." *Apple*. Apple Inc., 16 Feb. 2016. Web. 17 Feb. 2016.

Critical Commons Manager. *Hacker Stereotype in Jurassic Park*. Digital image. *Critical Commons*. N.p., n.d. Web. 17 Apr. 2016.

Hqanon. "How Anonymous Just Fooled Donald Trump, the Secret Service, and the FBI." *AnonHQ*. AnonHQ, 20 Mar. 2016. Web. 21 Mar. 2016.

Love, Dylan. "8 Things That Anonymous, The Hacker 'Terrorist' Group, Has Done For Good." *Business Insider*. Business Insider, Inc, 27 Apr. 2013. Web. 21 Mar. 2016.

Parkin, Simon. “Ghosts in the Machine: The Real Hackers Hiding behind the Cliches of TalkTalk and Mr Robot.” *The Guardian*. The Guardian, 31 Oct. 2015. Web. 8 Feb. 2016.

Pollice, Gary. "Ethics and Software Development." *Ethics and Software Development*. IBM, 15 May 2006. Web. 23 Mar. 2016.

"Practice Cyberethics." *Microsoft: Safety & Security Center*. Microsoft Corporation, 2016. Web. 23 Mar. 2016.

The Future of Life Institute. *FLI - The Future of Life Institute*. Web. 17 Feb. 2016.

Thornhill, John. "Brave New Era in Technology Needs New Ethics." *Financial Times*. The Financial Times Limited, 20 Jan. 2016. Web. 17 Feb. 2016.