**Ratio, Moralis, Justus Taylan Unal**

In this ever expansionary time of technology we live in, the humanity of computing must be considered and acted upon. Given our deep dependency on computer systems; ranging from satellite communications, to bank transactions, to the simple POS system at retail stores.

Ethics, Morality, and Legality are three of the many bounds that societies have placed upon its members. To define each of these words in a vacuum would be to ignore each society’s interpretations and acceptances. Each of these bounds are subjective by definition; with Ethics and Morality guiding the individual's decisions during their lifetime, and Legality enforcing accepted societal norms through consequence.

In computer hacking, Ethics defines a set of standards that individuals take on as a part of a real-world society that defines guidelines for their conduct online. Similarly, Morality defines that individual’s ability to take upon themselves the various standards of online conduct presented by society. For example a person on an IRC chat room may be immoral in his ideals, but that doesn’t define the collective sense of proper conduct online. In computer hacking, Legality plays a major role in either encouraging new hackers into the sphere on the count of being a dangerous thrill, or sidelining veterans from performing attacks due to their severe legal implications. In my opinion, the three bounds work in stages, with each increasing the level of societal backlash or punishment endured by the individual.

Hacking is the concept of using and modifying a product for a use not originally intended. Cracking is the concept of gaining unauthorized or elevated access to sensitive information in hopes of personal or monetary gain. I personally believe that there should be a clear distinction between hackers and crackers as these subjects reach mainstream attention.

In the past decade alone, the world has seen an exponential growth in threats such as phishing, ransom ware, malware, and database leaks. More specifically, attackers use SQL injection, CSS, DOS, and social engineering to name a few methods. Additionally, software and firmware exploits are constantly being discovered and used by bad actors around the world. Groups such as Anonymous use some or all of these methods to push forward, in their hive mind, a sense of accelerated social change.

Legislators around the world have gradually introduced more effective measures to deter and punish cyber criminals. In 1986, the Computer Fraud and Abuse Act¹ (CFAA) was introduced as an amendment to the 1984 Comprehensive Crime Control Act (CCCA) that set broad that sought to punish malicious individuals who target protected computer systems. CFAA created a set of federal penalties that range from a year to maximum sentence of 20 years based on the severity of the crime. The CFAA also brought about a path for individuals or entities affected to bring about civil claims for damages caused by the defendant. For example, in the CFAA guidelines, an offense such as trafficking passwords carries a minimum sentence of 1 year with a maximum of 10 years, while simply obtaining national security information without having proper permissions can result in a minimum of 10 years and a maximum sentence of 20 years. At this rate, ex-NSA agent Edward Snowden may face many counts of these offenses if he is ever to be tried in the United States. These counts only define punishments at the federal level, and state punishments can vary.

I believe that I am an advocate for many internet freedoms and liberties that have slowly begun to be pried from the hands of the end user. I use JavaScript blockers, Ad blockers, and VPN’s often in order to mask my identity to advertisers and entities that may watch my web traffic. I disagree deeply with the adage, ‘If you have nothing to hide, you have nothing to fear’, because of its dangerous consequences in terms of widespread surveillance and monetization of consumers.

As long as it remains legal, I use strong encryption as it earns its keep as a deterrent to attackers as well as a safety measure against unjust search and seizure. I also have used torrents in the past to download Linux distributions and support others who may also be downloading content at the same time. I use an ad blocker on Spotify on the web to listen to music ad free and without limits without paying for any services. On all of my Windows 10 devices, I have made sure to block telemetry and Windows tracking software that is built into the operating system. According to the Windows EULA, performing these modifications to the system is considered an improper use of their software. Most of my actions are what can be considered gray-legal and generally are not immoral or unethical.

With the advent of the 21st Century approaching, in 1996, the Digital Millennium Copyright Act² (DMCA) was introduced to protect copyrighted digital works from software to music to movies etc.

Using magnet links from torrent hosting sites like PirateBay or KickAssTorrents to download materials on its own is not an illegal act, but downloading and uploading copyrighted materials on these sites is. The underlying technology running torrents is called BitTorrent and it uses a distributed file ecosystem in which pieces of files are constantly passed amongst the web of active users known as seeders and leechers based on their contribution to the torrent’s distribution and activity. Because tracing an individual’s contribution to the network that hosts and shares a specific piece of copyrighted work, it is difficult for companies and law enforcement agencies to punish individuals sharing materials using the BitTorrent protocol.

These torrent link hosting sites have been taken down and reinstated on mirror sites on many occasions similar to the story of Hercules and the Hydra where once one head is cut off, three heads grow in its place. This ever present resilience of groups of individuals seeking to avoid paying for content has been difficult for law enforcement and content creators alike. Content creators have since turned to streaming services and alternative revenue sources such as donations in order to recover some of the monetary damages caused by content sharing. By turning to streaming services such as Netflix and Spotify, content consumers never truly own a copy of the content, and cannot share it freely.

Fair use is a set of guidelines set by “librarians, educators, and publishers” that seeks to simultaneously reserve content creators rights while allowing for some reproduction within limits (i.e. parody, commentary, critiques). For educators, as long as copyrighted materials are not openly or freely distributed for non-educational purposes, fair use applies. The issue of fair use has become a major concern with content creators who use pieces of copyrighted works in their own content on YouTube and other media distribution networks.

Newly educated hackers are never taught to use penetration testing and network administration skills to cause any intentional damage, except for demonstrative purposes. While in class, though we are allowed to ‘destroy’ systems beyond repair due to the sandbox environment, any actions that students take outside of a sandbox environment can cause real-world damage to critical systems and networks.

Apart from the FCPS guidelines on computer usage in schools and personal devices on school networks, law enforcement will almost definitely be involved in the investigation and punishment for any attacks on school networks. Mr. Bennett likely has a responsibility either ethically, morally, and/or legally to report the student through the proper channels.

As I stated earlier, government officials are beginning to match pace with the expansion of cyber technologies and crimes. Just recently President Obama spoke at the G20 summit regarding the prevalence of and the prevention of escalation of cyber-attacks worldwide. I believe that just as the protocols that govern internet communications (TCP, UDP, etc.) have taken hold, cyber codes of ethics will be developed and accepted by script kiddies and veteran hackers alike.

1: <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf>

2: <https://www.eff.org/issues/dmca>

3: <http://www.msnbc.com/stephanie-ruhle/watch/obama-we-don-t-want-cyber-war-to-escalate-758298179642>

4: <http://www.educationworld.com/a_curr/curr280b.shtml>