Mandatory Sentencing in Cybercrime

Madalyn Breach

Westminster College

PLSC203 Courts and Law, M. Zarkin

June 2, 2021

Mandatory sentencing has been a tool utilized in the United States since 1984. It was first established in the Comprehensive Crime Control Act to set minimum sentence lengths for like crimes, helping eliminate bias and preventing inconsistency among sentences of similar crimes. Mandatory sentencing can be useful to both judges and offenders, both aiding in sentencing guidelines and a line of deterrence. Although sometimes not as useful, areas of law like cybercrime could use the guidelines. Cybercrime sentencing is challenging because similar crimes in nature can have very different characteristics. The realm of technology is ever growing, and fast. Due to this, cyber legislation is constantly needing to catch up. Punishments for cybercrimes are very inconsistent because of a lack in clarity and overgeneralization of current legislations. These regulations have set maximum sentence lengths along with a number of sentence adjustments based on damages and the weight of the wrongfulness of the crime; the problem is that this scale still allows for bias and inconsistency. In order for mandatory sentencing to be effective and proportionate in cyber laws, current cyber legislation should be rewritten in terms that are clear--giving no room for discrepancies, capital loss should have a more refined range of additional sentence years, and minimum sentences should be added in combination with maximum sentences. Reforms of this kind would set cyber legislation on a path for success, preventing disproportionality in sentence lengths.

Cybercrime is often very different from traditional crime. The vastness of the internet creates a broad range of types of crimes, types of criminals, access and opportunity to commit crime, and the amount of damage caused by them. Because cybercrime is so unique and individual, it is difficult to chart wrongness on a scale and to create fitting, consistent punishments for it. The first attempt at creating laws for computers was enacted in the Comprehensive Crime Control Act (CCCA) established in 1984 as well as the Counterfeit

Access Device and Computer Fraud and Abuse Act (CAD-CFAA) also established in 1984. The policies involved were specific to issues regarding unauthorized access to personal financial information and unauthorized access to government information and computers. Although the limitations of these computers weren't known at the time, the policies outlined by the CCCA and the CAD-CFAA were slim in the scope of the internet. The CAD-CFAA was amended in 1986 to encompass a variety of cybercrimes, referred to as the Computer Fraud and Abuse Act (CFAA) of 1986 (Sharton, 2018). The CFAA has outlined distinctions between different cybercrimes and maximum sentencing guidelines for the different offenses as shown below in Figure 1.1.

Table 1: CFAA Sections and Maximum Sentences

Section	Description	Max. Sentence
1030(a)(1)	Obtaining national security information	10 (20)
1030(a)(2)	Obtaining information	1 or 5 (10)
1030(a)(3)	Accessing government computers	1 or 5 (10)
1030(a)(4)	Computer fraud	5 (10)
1030(a)(5)(A)	Intentional damage	1, 10, 20, or life (20 or life)
1030(a)(5)(B)	Reckless damage	1 or 5 (10)
1030(a)(5)(C)	Negligent damage	1 (10)
1030(a)(6)	Trafficking in passwords	1 or 5 (10)
1030(a)(7)	Computer extortion	5 (10)

Note: Maximum sentences for a second offense are listed in parentheses.

Figure 1.1 (Graves, 2019, pp. 318)

The factors considered in these sentence lengths include the characteristics of the crime, loss/damages, severeness of the crime, and the defendant's previous criminal history (Jones, 2019). The "base offense" level is the starting point for determining a sentence, composed of a range based on the offense level and the history of the defendant, which is dependent on the maximum sentence punishment as defined above. Offense levels rise and lower with every adjustment made to consider the scope of the crime, the intent of the offender, the type of information involved in the crime, the number of victims impacted by the crime, and financial/physical loss caused by the crime (Graves, 2019). These adjustments are referred to as "level increases." The vastness of the criteria for making adjustments proves it difficult to put a

definitive number on a defendant's sentence, however the range of inconsistencies caused by these adjustments result in too harsh or too lenient punishments.

Inconsistencies happen too often in cyber punishments. There are many crimes that are similar in wrongful nature but differ in characteristics of the crime. For example, *subject a* hacks into an unauthorized system at 16 years old by guessing a password of "1234," and finds a file he thinks looks cool and downloads it to a flash drive. *Subject b* also hacks into an unauthorized system but is 32 years old, uses a computer program to calculate all the possible passwords, works under the table as a private hacker for an opposing company, and gains access into the system to steal the salary information of all their top tier workers to use against them. Both *subject a* and *subject b* committed a crime of gaining unauthorized access and stealing information. Should both subjects be charged the same? That seems highly unfair. Charging both the subjects with the sentence suggested for a breach of access could impose an unfair extensive sentence on the 16 year old and even possibly an unfair lower sentence for the 32 year old. The characteristics of the crime can create bias in a system that currently utilizes maximum sentences. These maximums are good, but could be better used in combination with minimums. A maximum and a minimum punishment would ensure that a judge isn't punishing too harshly while still keeping a consistent base for the punishment of wrongfulness. This way, there is less room for inconsistencies but still plenty of range for adjustments. Using both these techniques together would prevent disproportionate sentences and still allow the judge to consider the scale of the crime.

Aaron Swartz was a computer programmer that was arrested for violating the CFAA by illegally downloading 4.8 million articles from the online directory JSTOR (Graves, 2019). In this specific case, Swartz was not responsible for unauthorized access or damage to any physical

property therefore the only factor considered here was the total financial loss the JSTOR had suffered. Each pdf downloaded cost $19, resulting in a total estimate of $91 million lost, escalating Swartz's punishment from a plea deal arranged at an estimate level 4 increase (as they had drastically underestimated the amount of loss) to the accurate 24 level increase, reaching up to the maximum punishments defined for level 24 cybercrimes. Swartz's actual sentencing was calculated by the base offense level (6), the estimated loss (+16), having "sophisticated means" (+2), and using "special skill" (+2) resulting in a final offense level of 26--estimating 63-78 months imprisonment, disqualifying him from probation or other lower punishments allowed by specific offense levels as outlined in the CFAA (Fakhoury, 2013). After being sentenced to 35 years in prison, over $1 million in fines, forfeiture, and restitution and his denial of a plea bargain--Aaron Swartz was found deceased by suicide in his apartment.

Aaron's punishment was on the harsher end of cybercrime inconsistency, so harsh that it led to his death. One of the issues at play in his case, and all cyber cases, is the verbage used by the current CFAA legislation. Graves states in *Perception Versus Punishment in Cybercrime* that "CFAA sentences escalate rapidly as (easily inflated) losses increase. But this escalation may be rapid not only in an absolute sense, but in disproportion to other attributes of the crime" (Graves, 2019). If Aaron Swartz was to illegally download one file, he would be convicted under a much lower offense level due to the estimated loss even though he committed the same criminal act. If Swartz had gained the same access to these files in a more "unauthorized way" then the vagueness of the CFAA would allow judges to interpret his sentence at a higher offense level. What if Swartz were to download millions of files that were locked and were inaccessible? Would he then be sentenced the same if he didn't have the same kind of access to the documents he was unauthorized to have?

Aside from implementing maximum sentences, the CFAA can reform the loss adjustment to have a narrower minimum and maximum length to prevent excessive punishment. In Aaron Swartz's case, his sentence was drastically increased since the estimated capital loss was so high. Not only was his sentence inflated "proportionally" to the amount of loss but he was also forced into forfeiture of the files. The wrongness of the crime wasn't impacted by the amount of loss, and yet his sentence was still drastically affected. Cyber punishments would be much more consistent and fair if the adjustment in years based on loss was maxed out (or even removed) and restitution and forfeiture were mandated. Oftentimes cybercriminals are young amateurs lacking in the financial ability to pay back restitution, in this case, the Court could then mandate extra years instead. Doing so would keep the wrongfulness proportionate to crimes in similar natures without pressing undue harm on individuals who did not deserve a harsher punishment. On the contrary, it would also prevent offenders from being punished too leniently since they are directly responsible for the damages and loss caused in capital. Although this is not a sureproof way of preventing inconsistencies, it could greatly aid in doing so and should be considered by the Court.

Most importantly, the CFAA should rewrite its statutes in clearly defined words and phrases. The CFAA currently uses words and phrases like "protected computer," "access," "unauthorized access," and "obtaining information--" all generalized and cloudy (*jfattah*, 2021). According to the CFAA, it is "a federal crime to access a computer without authorization or in a way that exceeds authorization" (*jfattah*, 2021). This authorization is not entailed or described in a way that would apply direct guidelines. We could easily say that Swartz exceeded his authorization by downloading those files. We could also say that he did not do so because he wasn't accessing a computer, he was accessing a network. We could say that the lack of physical

breaching would prove that he did nothing to infringe upon their computers or protected information. Username *jfattah,* with the *GW Law Review,* critiques of the CFAA related legislation and found that "minor offenses, which, at present, may receive the same punishment as computer terrorism for something as simple as violating a vendor's terms of agreement" (jfattah, 2021). These small discrepancies are causing years of additional prison time. The lack of clarity in the smallest of terms can lead to a higher or lower starting "base levels." If the judges are inconsistent in their sentencing, the changes in base levels could result in an unfair trial. This is the first and most practical step that cyber legislation needs to take in order to be consistent.

In conclusion, the war on cybercrime is an ever growing era. In order for the legislation to keep up, it needs to be reformed first to be proportionate now. Cyber sentencing is currently disproportionate and sentence lengths are inconsistent between similar crimes. In order to fix this, we can implement minimums alongside the already set maximums, replace a proportionate loss calculation with a standard minimum and maximum with restitution and forfeiture, and rewrite the current statutes to be clear and defined. These methods are sure to push cyber legislation a step in the right direction toward fair and reasonable punishments.

Annotated Bibliography:

Berris, P. (2020, September 21). Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress. *Congressional Research Service.* Retrieved from https://fas.org/sgp/crs/misc/R46536.pdf

This source helped me better understand the specifications of the CFAA and how it came to be from older legislation.

Fakhoury, H. (2013, April 10). *How the Sentencing Guidelines Work Against Defendants in CFAA Cases*. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2013/03/41-months-weev-understanding-how-sentencing-guidelines-work-cfaa-cases-0.

This source outlined the adjustments and base levels for crimes in specific cases. More specifically, it helped to outline Aaron Swartz's case and to compare his with others.

Graves, J., Acquisti, A., & Anderson, R. (2019). Perception Versus Punishment in Cybercrime. *Journal of Criminal Law and Criminology, 109*(4). https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7646&context=jclc

Perception Versus Punishment in Cybercrime provided relevant information on how computer crimes are currently being punished according to the policies placed by the CFAA. This article addressed the main concern that human perception of a crime greatly impacts the sentence length and argues that sentencing should have a standard for measuring the "weight" of a crime--and if influenced by perception--have a measurement to do so.

Infosecurity Group (2010, August 25). Do punishments fit the cybercrime? *Infosecurity Group.* https://www.infosecurity-magazine.com/magazine-features/do-punishments-fit-the-cybercrime/

Do punishments fit the cybercrime detailed the conviction of a large cyber criminal and addressed its role in the lack deterrence from former sentences and the current legislation.

Jfattah. (2021). *The Case to Update the Computer Fraud and Abuse Act*. CLB Criminal Law Brief. https://studentbriefs.law.gwu.edu/clb/2021/04/03/the-case-to-update-the-computer-fraud-and-abuse-act/.

This article gave me insight on the specific issues presented in the CFAA and some recommendations of what to do to fix them.

McConnell International LLC (2011). Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information. *McConnell International LLC.* http://www.iwar.org.uk/law/resources/cybercrime/mcconnell/CyberCrime.pdf

Cyber Crime and Punishment aided in proposing solutions to major flaws in cyber crime legislation and sentencing, focusing on the global impact cyber legislation in one country can have on many others that have yet to create laws for specific cybercrimes. This source also addressed the importance of responsibility of self when sentencing for crimes.

Oh, S., & Lee, K. (2014, June 16). The need for specific penalties for hacking in criminal law. Retrieved February 28, 2021, from https://www.hindawi.com/journals/tswj/2014/736738/

The need for specific penalties for hacking in criminal law compares cyber crime punishments from different countries and their models for how to punish those convicted.

Smith, Russell G. (2004). CYBER CRIME SENTENCING The Effectiveness of Criminal Justice Responses. *Australian Institute of Criminology*. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.586.3171&rep=rep1&type=pdf

Cyber Crime Sentencing - The Effectiveness of Criminal Justice Responses addresses concerns regarding restitution and deterrence within cybercrime sentencing and why it is difficult to be successful in both.

Tewksbury, R., Higgins, G., & Marcum, C. (2011). Doing Time for Cyber crime: An Examination of the Correlates of Sentence Length in the United States. *International Journal of Cyber Criminology, 5*(2). https://www.cybercrimejournal.com/marcumetal2011julyijcc.pdf

Doing Time for Cyber crime: An Examination of the Correlates of Sentence Length in the United States provided necessary results and reasonings from data collected from law enforcement in interested of sex and determinates for sentencing lengths. This information helped form evidence for the argument discussed in this paper that sentencing in cyber crime should include mandatory sentencing to prevent bias.

The World Bank (2017). Combatting Cybercrime. *United Nations and International Bank for Reconstitution and Development/The World Bank.* https://www.itu.int/en/ITU-D/Cybersecurity/Documents/worldbank-combating-cybercrime-toolkit.pdf

Combatting Cybercrime addresses cases and issues globally and proposed solutions on how to proceed for the betterment of society.

United Nations Conference on Trade and Development. (2015). Global mapping of cyberlaws reveals significant gaps despite progress. Retrieved from https://unctad.org/press-material/global-mapping-cyberlaws-reveals-significant-gaps-despite-progress

Global mapping of cyberlaws reveal significant gaps despite progress compares data about cyber laws around the world and analyzes their progress in successfully sentencing and deterring cyber crime.

Williams, K. (2016, February 04). Judges struggle with cyber crime punishment. Retrieved February 28, 2021, from https://thehill.com/policy/cybersecurity/265285-judges-struggle-with-cyber-crime-punishment?rl=1

Judges Struggle with Cyber Crime Punishment gives an overview of the issues revolving around cyber crime sentencing and professional quotes on the matter.