Computer fraud and abuse act (cfaa) | analysis

The Computer Fraud and Abuse Act (CFAA) or 18 U. S. Code § 1030 is the primary federal law governing cybercrime in the United States today. It outlaw's activities that target computer systems. For the better, this act shields user connected to the Internet from possible threats, harm, spying, and any other activity that may corrupt systems as instruments of fraud.

Background information

Being around since the 1980s, The Computer Fraud and Abuse Act protects the U. S. government and other financial companies from threats stemming from computer systems. This act has been amended far beyond its original intent. Not only to meet new policy standards but also meet the scope of current day operations of society's ever-changing technological advances. More specifically, in 1986, The CFAA made it a federal offense to utilize protected information systems without proper authorization and authentication. This act goes far beyond simple specifications and blankets all computers hooked up to the Internet concerning unauthorized access (Thaw, 2013). Primarily, this act was intended to target hacking and decrease its occurrences. Over time, this act changed to allow individuals to sue on a local scale in regards to hacking (Wellington, 2014).

In the world, when a computer was the size of a room, access was already restricted. Today, CFAA is needed more than ever seeing that information systems are readily and easily available to the public (Lavin, H., & DiMichele, E., 2019). With the advances of today and the individual access to information systems and the Internet, it's entirely possible to access more than one computer at any single time.

By shopping with an online retailer such as Amazon, the host of the computer is accessing company servers and shopping within a public domain (Ziegler, 2012). One grouping that does not follow the ideologies of the CFAA and unauthorized access has to do with NORAD supercomputers (Oh, and Lee, 2014). Seeing that logging onto the Internet means touching and mostly accessing many other servers and computers, this brings the risk of unauthorized access up immensely.

Inadequacies of CFAA

The repercussions of specific actions under CFAA are out of touch with current day society. Stealing money online (3-5 years in prison) does not get the same punishment as bank robbery (7-10 years in jail). Online financial institutions are more at risk due to less penalty vs. “ in person” robbery. Non-US citizens (outside of the country) that commit crime through cyberspace are not pursued strong enough through the CFAA. There is not enough guidance or guidelines on effectively enforcing authorized access on individuals. Leaving much room for an innocent person to unknowingly access a system without permissions due to ignorance in which would result in felony charges.

Another issue lies with the power CFAA gives private organizations when it comes to what is considered criminal (Wellington, 2014). This act makes it hard to follow specific guidelines when it comes to abide within the constraints. Therefore, it is harder to explore and utilize the Internet and remain confident that no crime is being committed unintentionally. Essentially, CFAA puts a damper on innovative ideas and research. Accessing

specific data can be a violation of this act. Even though the CFAA intends to limit criminal activity, it also limits research and innovation. Private organizations are made to be more potent with stringent laws.

Adequacies of CFAA

The CFAA not only prosecutes minor actions but also covers more substantial cyber criminal conduct. 2014 had well over 150 federal criminal cases in which were pursued under the CFAA. Though the CFAA in many cases is a deterrent to cybercrime, it also can be used against more significant, more severe offenders when need be. Information systems and technology are taking over the world we live in today. It is nearly impossible to live in today's society and not take advantage of some form of information systems. Governments rely dramatically on this technology everyday for storage. With this fact, the increased use also brings a higher risk of criminal activity. Challenges that people, more specifically government agencies, would face would be the transmission of data to a far end. With this, the CFAA allows protection on criminal actions against and with that information. Seeing that the DoD is a highly critical, sensitive organization when it comes to national defense, it is at a higher risk of sabotage or criminal activity. The CFAA would allow for a barrier of protection if the information were put at risk in any way by hostile acts.

Another benefit of the CFAA is the fact that it replaced an existing law known as the Comprehensive Crime Control Act (CCCA). CCCA was not as developed. Though this act covered some of the wrongdoing when dealing with information systems, it had many holes and dealt profoundly with

malicious activity. When the world was seeing more technology and more sophisticated processes, the CFAA walked in to cover the gaps. Simply banning individuals from unauthorized use was a huge step forward when stopping criminal activity related to the information systems (Wellington, 2014). Though generic, the CFAA covered many security realms. One specific category that was specified was the malware and viruses topic. Once this area was known more by the world, the CFAA came up with a law that made it punishable for any virus to steal or delete data related to information systems.

Recommendation

Focus on extreme cases of cyber violations. Leave smaller infractions out of it to put the responsibility on local law enforcement agencies. Increasing punishments under CFAA will likely bring down cybercrime. Include law violations that cover intellectual property. Clearer guidelines on breaches and unauthorized access should be specified more thoroughly. Ensuring a companies terms of service follow these guidelines is crucial to ensuring ignorance cant be an excuse. Double punishment is unacceptable. By removing specific provisions, this will eradicate this issue.

Conclusion

Get the word out. Get political members involved to set up a plan going forward. A practical approach to necessary changes as needed is a must. A revamp on CFAA, and its scope will be required for ultimate protection with computers and to deter would-be cybercriminals on a more severe scale. In all, the act has many weaknesses that could be addressed and fixed with a

proper review. Though the CFAA does more good from existing than bad, there are still innocent people charged due to ignorance. Innovation is limited also. Vagueness is the problem, and interpretation is an opinion. The poor implementation of this act when compared to our advanced technological society gives room for innocent mistakes having huge impacts on the innocent. Whereas, repercussions of criminal activity are severe enough to the point that would prevent past criminals from becoming repeat offenders.

- Wellington, K. (2014). Cyber attacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions. Retrieved fromhttps://digitalcommons. law. scu. edu/chtlj/vol30/iss2/1/
- Lavin, H., & DiMichele, E. (2019). “ Questioning ‘ Authority’: Courts Split on What It Means to Access Computers ‘ Without Authorization’ Under the Computer Fraud and Abuse Act.” Retrieved fromhttps://www. stroock. com/publication/questioning-authority-courts-split-on-what-it-means-to-access-computers-without-authorization-under-the-computer-fraud-and-abuse-act/
- Ziegler, K. (2012). It’s Not Just Physical: Finding a Neutral Interpretation of Authorization Under the Computer Fraud and Abuse Act. *Jstor* . Retrieved fromhttps://www. jstor. org/stable/43489439? seq= 1#page_scan_tab_contents
- Oh, S., & Lee, K. (2014). The Need for Specific Penalties for Hacking in Criminal Law. *Hindawi* . Retrieved fromhttps://www. hindawi. com/journals/tswj/2014/736738/