In the lectures we have touched on the narrow and broad approaches to interpreting the terms “exceeds authorized access” and “authorization.” How have changes in the use of technology affected the application of these approaches to modern cybersecurity needs and challenges? Which approach do you ultimately agree with, and why?

Congress passed the Computer Fraud and Abuse Act (CFAA) due to a growing concern about more computers becoming networked and subject to unauthorized access, which can compromise sensitive data. The CFAA is the primary U.S federal statute that prohibits and criminalizes certain activities taken by an individual that lacks authorization or exceeds authorized access. To make the execution possible, the law criminalizes seven different categories of behavior, each outlined in sections (a)(1) through (a)(7) of the CFAA. Some of these sections only apply if the individual didn’t have authorization while the others apply if the person didn’t have authorization or exceeded authorized access. However, the statue doesn’t provide a clear and specific definition of the term “authorization” or “exceeds authorized access” (Kosseff, 2017). This issue has been resulting in a continuous dispute between the plaintiff and the defendant in terms of what category the incident falls under. It has also given rise to the narrow and broad interpretation of the words “without authorization” or “exceeds authorized access” by courts (Kosseff, 2017).

A narrow view of the statute would lead to the conclusion that an individual violates the CFAA if he or she commits a code-based violation. This violation involves the defendant circumventing computer software code to access a computer without authorization or in excess of authorized access. On the other hand, a broader view of the statute would allow prosecutors to bring up cases arising from code-based, contract-based, norms-based violations. That is, a contract-based violation occurs when an individual’s access violates any agreement, policy, or terms of service; while a norms-based violation occurs when an individual’s access is in contrary to societal expectations. I believe that the middle ground between these two interpretations is a more viable application of the CFAA. Unfortunately, unless the supreme court eventually resolves this issue, federal courts will continue to apply definitions of the terms “without authorization” and “exceeds authorized access”. Nevertheless, I am currently more inclined to the broad interpretation of the terms. This is because modern violations are increasingly complex. It is very hard to categorize a violation incident as merely code based or contract based. For example, in the case of EF Cultural BV v. Explorica, employees of Explorica used a program to scrape pricing information from EF Cultural’s publicly accessible website. These employees had previously worked for EF Cultural and breached their confidentiality agreement with the organization. The contract required them to not disclose or use any information for a third party’s benefit or against the EF Cultural (Kosseff, 2017).

The changes in the use of technology certainly bring modern cybersecurity needs and challenges. More devices are connected to the internet today, and employees are leveraging different types of access to get tasks accomplished. Additionally, employees work from home and bring their devices to work. This situation poses more risks for misuse of data and violations that arise from improper handling of it. Hence, the application of the two CFAA approaches can give rise to incidents that are considered as severe CFAA violations. Both organizations and employees have to do their part in reducing the occurrence of these violations and the consequences it can bring.

References

Kosseff, J. (2017). Cybersecurity Law. Hoboken, N.J: John Wiley & Sons, Inc.