John Sikes
9/3/2020

The Legality of Cyber Stings

Since the advent of the internet and the world-wide web's adoption into our daily lives there have been, and will continue to be, many that would seek to use humanity's most powerful tool in history to further their own means at the cost of other's privacy, safety, and income. To catch these hackers, predators, and other dangerous entities before harm can be done, law enforcement and private citizens alike have constantly developed more advanced and intricate ways of catching these people in the act. However, the legality of these actions are much more complex than one may initially assume. To this extent, clarification of laws regarding entrapment and enticement are necessary in order to set up a cyber sting operation, so as to avoid breaking the law oneself in an attempt to catch another.

Cyber stings (or "honeypots", as many know them as) are a form of enticement by officials and citizens alike to capture would-be predators in the act before any harm is caused. However, these are meticulously regulated by existing legal statutes regarding setting up an opportunity for a criminal to commit a crime (enticement) and convincing a perpetrator into committing a crime they otherwise would not have committed (entrapment). These legalities become even more nefariously intertwined and difficult to decipher between when applied to honeypots that deter hackers or collect information on them, as the latter in particular are highly illegal on their own. To work around these legislations, sting operators have found that to avoid indictments they need to gauge the level of the operation as compared to the level of crime the perpetrator has been likely to commit, such that the sting will serve to indicate enticement to commit a similar, if not identical, crime to those performed in the past, rather than reaching out of their range and serve as a basis of an entrapment argument by a competent defense team.

In a similar manner, sting operations that function in a purely technical manner (i.e. data breaches) to catch a repeat offender red-handed are the trickiest of stings to avoid technicalities as a result of the potential data collection setup on the sting operator's end. Technicalities arise in this manner due to operators setting up honeypots to collect tracking information on those that breach it, as well as presenting itself as a real entity rather than a fictitious one. These could then be used by a defense team to not only shoot down the prosecution, but also turn the tables and potentially file lawsuits against the honeypot operators due to breaching of federal anti-hacking laws.

While the internet perpetually evolves, so too must defense and threat analysis. To keep up with the evolving network of criminals and perpetrators, active defense through the use of honeypots and enticement in general is a proven method to catch predators in the act and bring them to justice. However, those operating in the right must be careful so as not to become the criminals themselves as a result of the setup and the corresponding anti-hacking, privacy protection, and security statutes.

Works Cited

Marshall, David S. “Internet Sting Operations.” *The Marshall Defense Firm*, www.marshalldefense.com/services/internet-sting-operations/.

Hanson, Jarrod S. "Entrapment in Cyberspace: A Renewed Call for Reasonable Suspicion," *University of Chicago Legal Forum*: Vol.1996: Iss. 1, Article 17

Luck, Morgan. “Entrapment behind the Firewall: the Ethics of Internal Cyber-Stings.” *Australasian Journal of Information Systems*, vol. 23, 2019, doi:10.3127/ajis.v23i0.1886.

Overly, Michael R. “Avoiding the Pitfalls of Operating a Honeypot.” *CSO Online*, CSO, 25 Nov. 2019, www.csoonline.com/article/3455187/avoiding-the-pitfalls-of-operating-a-honeypot.html.