Northwestern Journal of Technology and Intellectual Property

Volume 19 | Issue 3 Article 2

4-2022

Beacons: A Viable Solution to the Ever-Evolving Problem of Corporate Data Breaches

Lauren Fiotakis

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

BEACONS: A VIABLE SOLUTION TO THE EVER-EVOLVING PROBLEM OF CORPORATE DATA BREACHES

Lauren Fiotakis

April 2022 VOL. 19, NO. 3

Volume 19, Number 3 (2022)
Northwestern Journal of Technology and Intellectual Property

BEACONS: A VIABLE SOLUTION TO THE EVER-EVOLVING PROBLEM OF CORPORATE DATA BREACHES

Lauren Fiotakis[*]

ABSTRACT—In an increasingly virtual world, data breaches continuously plague large corporations. These companies have few options to keep their data out of the hands of persistent hackers, who often discover ways around any safeguards that may be in place. It seems as though any measures companies are currently able to employ merely delay the inevitable breach that will bring with it the potential loss of both customers' data and their faith in the privacy and security of their information. These attacks can be debilitating to corporations; thus, it seems only fair to provide them the ability to take active measures to defend against cybercriminals.

Some have argued that allowing hacking victims to retaliate against their attackers could help reduce cybercrime. Others suggest that these counterstrikes may lead to an increased prevalence of attacks rather than deter initial attackers. This note will argue that the use of beacons—code hidden in a company's files that alerts the company of the files' theft—should be permitted as an effective and proportional cyber-self-defense measure.

[*] Northwestern University Pritzker School of Law, J.D., 2022.

INTRODUCTION

In an increasingly virtual world, data breaches continuously plague large corporations. These companies have few options to keep their data out of the hands of persistent hackers, who often discover ways around any safeguards that may be in place. It seems as though any measures companies are able to employ merely delay the inevitable breach that will bring with it the potential loss of both customers' data and their faith in the privacy and security of their information in the hands of the hacked institution.

The scale of this issue is only increasing; as of 2014, cybercrime cost the global economy more than $400 billion annually, with the United States' annual cost accounting for $100 billion of that figure.[1] To combat this, worldwide spending on information security products topped $70 billion in the same year.[2] However, these measures have not been as effective as their price tag may suggest. In 2013, Target suffered a significant security breach where customer payment records were stolen,[3] affecting as many as one in three Americans.[4] The well-publicized 2017 Equifax scandal, which saw the compromise of 143 million Americans' personal information,[5] cost the company's insurers alone at least $125 million.[6] According to the National Bureau of Economic Research, a company loses 1.1% of market capitalization and experiences a 3.2% drop in annual sales growth following a breach of customer data.[7] These attacks can be debilitating to corporations; thus, it seems only fair to provide them the ability to take active measures to defend against cybercriminals.

Some have argued that allowing hacking victims to retaliate against their attackers could help reduce such attacks.[8] Others suggest that these counterstrikes may lead to an increased prevalence of attacks rather than deterring initial attackers.[9] As it stands, federal cyber law does not permit

---

[1] Jay P. Kesan & Carol M. Hayes, Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities, 58 ARIZ. L. REV. 753, 755 (2016).

[2] Id. at 756.

[3] Id. at 763.

[4] Id.

[5] Seena Gressin, *The Equifax Data Breach: What to Do*, BLAKELY WATERS (Sept. 13, 2017), https://www.blakelywalters.com/blog/the-equifax-data-breach-what-to-do [https://perma.cc/P97C-EAYQ]. Hackers accessed Equifax's network from May through July, stealing names, Social Security numbers, birth dates, addresses, some customers' driver's license numbers, and other personal data. *See id.*

[6] Scott J. Shackelford et al., Rethinking Active Defense: A Comparative Analysis of Proactive Cybersecurity Policymaking, 41 U. PA. J. INT'L L. 377, 384 (2019).

[7] Id.

[8] Orin S. Kerr, Computer Crime Law 143 (4th ed. 2018).

[9] Id.

any unauthorized access of a network,[10] meaning these active defensive measures would not be permitted even if they were proportional to the initial attack—the usual standard for self-defense.

This note will argue that the use of beacons—code hidden in a company's files that alerts the company of the files' theft—should be permitted as a cyber-self-defense measure. Part I will examine the various dialogue around self-help in cyberspace, Part II will explore the relevant statute, Part III will discuss the need for proportionality in any response to crime, Part IV will illustrate different possible methods of cyber-self-defense, and Part V will present beacons as the most effective and proportional cyber defense mechanism given all other factors.

I. SELF-HELP IN CYBERSPACE

While the notion of self-help in cyberspace has never been litigated in federal court,[11] it has long been a topic of discussion among scholars. There are many arguments for and against its use; active defense and self-help tactics have the potential to aid companies who have been hacked but may also cause additional damage. While all forms of active defense carry with them some degree of risk, the benefits of proportional active defense measures likely outweigh the costs.[12]

Scholars in favor of active defense argue that there should be some acceptance of self-defense for cybercrimes, as it is a well-defined principle for other non-cybercrimes.[13] They argue that the threat of a counterattack could disincentivize potential hackers from committing these crimes, as perpetrators would come to expect some form of retaliation.[14] This would allow corporations to take a counteroffensive role in the protection of consumer data, rather than simply setting up firewalls in the hope that they will be sufficient to stop the ever-evolving hackers.[15]

One of the primary arguments in favor of cyber-self-defense is that there are many challenges in charging and prosecuting cybercriminals. First,

---

[10] Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

[11] KERR, *supra* note 8, at 141.

[12] *See* Michael Edmund O'Neill, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 GEO. MASON L. REV. 237, 265 (2000).

[13] *See id.*; Bruce P. Smith, *Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help*, 1 J.L. ECON. & POL'Y 171 (2005); *see also* discussion *infra* Part III.

[14] *See* O'Neill, *supra* note 12, at 279.

[15] *See* discussion *infra* Part IV.

hacking victims are often unwilling to come forward.[16] Reporting a breach to the authorities would necessitate revealing the breach to the public,[17] which often leads to bad publicity and a loss of consumer confidence. Additionally, law enforcement officers often struggle to determine the origin of a malicious code.[18] Sophisticated hackers take effort to cover their tracks by routing their attacks through many servers in myriad locations, increasing the difficulty of following an attacker's trail.[19] These servers may be located in different countries, and the lack of international cyber law combined with the difficulty of coordinating law enforcement efforts across borders reduces the chance that a hacker will ever be held accountable for the harm caused.[20] Additionally, many nations lack comprehensive cybercrime statutes and could potentially become safe havens for criminals.[21]

Computers have provided criminals with a tool that allows them to realize increased returns from their crimes. What used to take a team of in-person perpetrators and a complex plan can now be achieved by one offender writing a code far from the scene of the crime. The distance afforded by computer use also lowers the potential costs for these offenders, as they have a lower probability of detection and, therefore, conviction. To deter cybercrime, the government must raise the costs of these crimes, something it may not be well-positioned to accomplish.[22] Raising these costs could come through sentencing enhancements or by allowing for self-help by the victims of hacks.[23] While sentencing enhancements may be temporarily effective, they soon reach a point of diminishing marginal returns.[24] The government cannot increase sentences infinitely; they would soon become absurd when compared to sentences for non-computer-based crimes.[25] Additionally, the sentence would be long regardless of the severity of the crime.[26] This could actually increase the prevalence of more severe

[16] Smith, *supra* note 13, at 172–73. Many corporations worry that "negative publicity would hurt their organization's stock and/or image" and are concerned that competitors would take advantage of any information relayed to law enforcement. *Id.*

[17] *Security Breach Notification Laws*, NAT'L CONF. OF ST. LEGISLATURES (Jan. 17, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/XCF4-WY4Z]. Each state has different requirements for what constitutes a breach of personal information and who must be notified of such a breach. *Id.*

[18] Smith, *supra* note 13, at 173–74.

[19] *Id.* at 174.

[20] *Id.*

[21] *Id.*

[22] O'Neill, *supra* note 12, at 265.

[23] *Id.*

[24] *Id.* at 274.

[25] *See id.*

[26] *Id.*

cybercrimes, as criminals would have little reason to stop their illegal activities before causing significant damage.[27] The government's other option would be to create some allowance for cyber victims to deter criminals through self-defense. Rather than waiting for a trial and conviction, a victim could deliver a swift punishment immediately following a crime.[28]

The counterargument is that due to the difficulty in determining who exactly may have hacked a system, these hacking victims may consequentially launch an attack against an innocent third party.[29] That party then, having been attacked, would be within its rights to retaliate against the initial victim.[30] This has the potential to greatly increase unauthorized access and computer damage as a whole, effectively accomplishing what self-help techniques were meant to prevent.[31] Additionally, there is significant potential for collateral damage, as hackers often overtake others' computers and networks to launch attacks.[32] This both helps hackers to disguise their identities and could induce counterstrikes on these intermediary, or 'zombie,' computers.[33] Further, active defense has the potential to hinder law enforcement in its cyber investigations. A counterstrike or the reclaiming of stolen data could destroy evidence or compromise ongoing investigations, impeding authorities' ability to stop these already elusive criminals.[34]

Those in favor of active defense have relied on the doctrine of necessity to excuse the fact that the defender would have to access the attacker's network, or possibly that of a zombie.[35] Even if this doctrine were accepted in court, however, it could still expose defenders to significant civil liability.[36] Any harm caused while accessing someone else's computer or network would be recoverable as damages against the defender, consistent with typical treatment under the doctrine of necessity.[37] This may reduce the attractiveness of active defense, as any potential benefits achieved from the recovery of data could be offset by a significant damage award owed to the hackers or zombies.

---

[27] *Id.*

[28] *Id.* at 279.

[29] KERR, *supra* note 8, at 143.

[30] *Id.*

[31] *Id.*

[32] Smith, *supra* note 13, at 180.

[33] *Id.*

[34] C. Alden Pelker, *Permission to Come Aboard (an Adversary's Network)? Ensuring Legality of Enhanced Network Security Measures Through a Multilayer Permission Acquisition Scheme*, 53 AM. CRIM. L. REV. 437, 443 (2016).

[35] Smith, *supra* note 13, at 192; *see* discussion *infra* Part III b.

[36] Smith, *supra* note 13, at 192–93.

[37] *Id.*

Given the arguments for and against active defense, it is clear that an all-or-nothing approach to this issue would be less effective than a method that integrates these opposing concerns. While any type of active defense presents some risk, a complete prohibition of self-help in cyberspace is inevitably accompanied by a general lack of enforcement of cyber laws. An active defense method that is not meant to cause any damage could still accomplish the desired effects but may also avoid the negative repercussions associated with overly aggressive measures.

II. EXAMINATION OF THE CYBER FRAUD AND ABUSE ACT

Any type of active cyber defense measure would be governed by relevant unauthorized access statutes, as any activity that takes place outside of the defender's own network constitutes access to another network.[38] The federal government, as well as every state, has adopted an unauthorized access statute.[39] The primary federal statute governing unauthorized access to a computer or network is 18 U.S.C. § 1030, the Computer Fraud and Abuse Act ("CFAA").[40] The CFAA prohibits any kind of unauthorized access and there are no exclusions from this statute.[41] Therefore, even proportional self-defense measures are unavailable to victims of cyber-attacks.

One of the CFAA's most frequently utilized subsections is § 1030(a)(2), which prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access" of that computer to obtain information.[42] The section is limited to accessing the records of financial institutions, United States government agencies or departments, or protected computers.[43] While this appears to be narrow, a "protected computer" is defined under the statute as "a computer . . . which is used in or affecting interstate or foreign commerce or communication . . . ,"[44] covering effectively every computer with a network connection.

The CFAA does not define "access"; however, many states' unauthorized access statutes are similar to the federal statute, and therefore may be helpful in interpreting the CFAA. The State of California defines access as "to gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with . . . a computer, computer

[38] Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

[39] KERR, *supra* note 8, at 30.

[40] § 1030.

[41] *Id.*

[42] § 1030(a)(2).

[43] *Id.*

[44] § 1030(e)(2).

system, or computer network."[45] Under this definition, any time a hacker enters a network he does not own or is not authorized to enter, his actions would fall under the statute.[46] The phrase "exceeds authorized access" is defined by the CFAA and is described as "access[ing] a computer with authorization and . . . us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[47] In *United States v. Nosal*, the Ninth Circuit concluded that this provision relates to people with some limited authorization to access the network at issue,[48] who would be in violation if they accessed files or data that were beyond the scope of their authorization.[49] The purpose of the access is irrelevant; all that matters is whether the hacker was authorized to access the files in the first place.[50]

Additionally, § 1030(a)(5)(A) prohibits "intentionally caus[ing] damage without authorization, to a protected computer."[51] A hacker can only be charged under this subsection when the damage was caused intentionally; intentional unauthorized access is not sufficient here, as "without authorization" refers to the specific acts that caused the damage.[52] Additional subsections of § 1030(a)(5) only require intentional unauthorized access and have lower mens rea requirements for the act of causing the damage.[53]

Along with the CFAA's criminal components, § 1030(g) provides for civil relief from any "damage or loss by reason of a violation of this section. . . ."[54] This allows victims to receive some compensation for the extensive costs that come with being the target of a hack; however, this is not always practical, as law enforcement would have to identify and locate the hacker before a suit could be brought. While this section attempts to provide needed relief for hacking victims, it often falls short, seeing as hackers are notoriously difficult to track down.[55]

These provisions, along with the rest of the CFAA, create a framework in which there is no opportunity for reasonable exclusion from culpability; you have either accessed a computer in an unauthorized fashion or you have

---

[45] State v. Riley, 846 P.2d 1365, 1373 (Wash. 1993); CAL. PENAL CODE § 502(b)(1) (2020).

[46] *Riley*, 846 P.2d at 1373.

[47] § 1030(e)(6).

[48] 676 F.3d 854, 858 (9th Cir. 2012).

[49] *Id.*

[50] *Id.* at 858.

[51] § 1030(a)(5)(A).

[52] United States v. Thomas, 877 F.3d 591, 595 (5th Cir. 2017).

[53] § 1030(a)(5)(B)–(C).

[54] § 1030(g).

[55] *See* Smith, *supra* note 13, at 173–74; O'Neill, *supra* note 12, at 275.

not. While the statute provides provisions for sentencing enhancements,[56] there is no allowance for any type of self-defense, a divergence from the manner in which cybercrimes typically mirror more traditional crimes.[57] This makes the statute seem disproportionately harsh and skewed toward punishment, especially when compared with traditional crime statutes that include mitigating factors and affirmative defenses.

III. PROPORTIONALITY IN CYBER SELF-DEFENSE

Proponents for and against active defense measures often neglect the concept of proportionality. The most effective solution, however, is neither as drastic as those supporting active defense may suggest nor as restrictive as the current state of the CFAA mandates. Instead, active defense measures should be allowed only if they are proportional to the initial attack, as is commonly accepted in other criminal and tort settings.[58] If using this common standard, a violation under § 1030(a)(2), for example, could only be matched by a victim accessing the attacker's computer in an unauthorized manner to obtain specific and relevant information.

The concept of proportionality in self-defense is present in state criminal statutes and common law tort doctrine, evidencing its pervasiveness in the justice system.[59] Additionally, Congress recently proposed an amendment to the CFAA that would allow for proportional self-defense, further illustrating the importance of thoughtful and restrained countermeasures rather than aggressive and retaliatory strikes.[60]

A. Criminal Offenses

Self-defense is a commonly referred to doctrine used to justify criminal offenses. For the most part, criminal statutes and their associated self-defense provisions are written as state law, and therefore it can be difficult to gain a perspective that would be equivalent to the federal prohibition of active defense. The Model Penal Code, which has greatly influenced criminal law across the country, can be used as a proxy for nationwide criminal law. Model Penal Code § 3.04 outlines the provisions relating to the use of force in self-defense, stating generally that "the use of force upon or toward another person is justifiable when the actor believes that such force is

[56] *See* § 1030(c).

[57] *See* KERR, *supra* note 8, at 15–16 (explaining how unauthorized access statutes were built upon criminal theft statutes).

[58] *See* discussion *infra* Part III a–b.

[59] *See* discussion *infra* Part III a–b.

[60] *See* Active Cyber Defense Certainty Act, H.R. 3270, 116th Cong. (2019); *see also* discussion *infra* Part III c.

immediately necessary for the purpose of protecting himself against the use of unlawful force by such other person. . . ."[61] While proportionality is not explicitly mentioned, it can be inferred through the "immediately necessary" language, which implies that a defender is not authorized to use more force than would be sufficient to stop the attack.

Perhaps more applicable, the Model Penal Code also has a section detailing the circumstances under which force can be used to protect property.[62] Under § 3.06, force is justified when the defender believes that it is "immediately necessary . . . to prevent or terminate an unlawful entry or . . . a trespass against or the unlawful carrying away of tangible, movable property . . . in his possession. . . ."[63] While not an exact fit—due to the requirement that the property be tangible and moveable—this section could lay the framework for an equivalent section dealing with the protection of intangible and virtual data using reasonably necessary force.

Section 3.06 also creates an allowance for the use of a device to protect property, as long as the device is not meant to cause death or serious bodily injury, the use of the device is reasonable under the circumstances, and the device is one customarily used for such purpose or notice is given that the device will be used.[64] Using a computer as an active defense device would meet the requirements of this section. No active defense measure is likely to present a risk of death or bodily harm and therefore the first element would be met. Second, the use of the device is typically reasonable under the circumstances because it is logical for the defender to move beyond purely passive defenses once they have been bypassed and proven unsuccessful. Finally, active defense techniques meet the third element; whether employed by defenders or law enforcement, computers with specialized code are typically the tools used to locate attackers and reclaim stolen data. Alternatively, this element could be satisfied through a warning, putting intruders on notice that their network may subsequently be accessed to retrieve any stolen files or obtain attributional information.[65]

The Supreme Court has also acknowledged the proportionality requirement for acts of self-defense, despite the fact that such cases rarely make it to the highest court. In 1893, the Court stated:

> A man who is in the lawful pursuit of his business . . . and when in that condition he is attacked by another, under circumstances which denote an intention to take away his life or to do him some enormous bodily harm, he may lawfully kill the

[61] MODEL PENAL CODE § 3.04(a) (AM. L. INST. 1985).

[62] *Id.* § 3.06.

[63] *Id.* § 3.06(1)(a).

[64] *Id.* § 3.06(5).

[65] *See* discussion *infra* Part V.

> assailant. . . . The law of self-defense is a law of proportions as well as a law of necessity, and it is only danger that is deadly in its character that you can exercise a deadly act against.[66]

The criminal justice system is generally willing to recognize self-defense as a justification for committing a criminal act, but only if it was necessary under the circumstances and not more serious than the attack against which it was meant to defend. This principle must be taken into account when considering active defense in cyberspace; an extreme or retaliatory attack that is not meant to protect the network or reclaim stolen data will almost certainly be judged disproportionate, even if a court or legislature allowed for self-help in cyberspace.

B. Tort Principles

Self-defense is also seen in common law tort cases. The Restatement (Second) of Torts gives guidance that illustrates many instances where self-defense may be permitted, but only to the extent that it is reasonably necessary and proportional to the initial action. The Restatement first states that a defender may act in a manner that is not likely to cause death or serious bodily harm in effort to "prevent or terminate another's intrusion upon the actor's land or chattels. . . ."[67] Many proponents for active defense often equate computer crimes to trespass to chattels,[68] meaning that the Restatement illustrates a path for defenders to claim self-defense when using active defense measures. Death or serious bodily harm could be equated to disabling an attacker's network or destroying data, so it follows that any reasonable force less than that which would cause serious harm to the attacker's computer would be allowed. The Restatement also emphasizes proportionality in a section detailing the "[a]mount of [f]orce [p]ermissible."[69] It states that force "in excess of that which the actor correctly or reasonably believes to be necessary to prevent or terminate the other's intrusion" is prohibited.[70]

Additionally, the Restatement contemplates the use of a device to carry out self-defense measures, provided that the device does not threaten death or serious bodily harm.[71] Section 84 states that a defender can use a device to protect his chattels if

---

[66] Allen v. United States, 150 U.S. 551, 556–57 (1893) (internal quotations omitted).

[67] RESTATEMENT (SECOND) OF TORTS § 77 (AM. L. INST. 1965).

[68] Smith, *supra* note 13, at 189.

[69] RESTATEMENT (SECOND) OF TORTS § 81 (AM. L. INST. 1965).

[70] *Id.*

[71] *Id.* § 84.

> (a) the use of such a device is reasonably necessary to protect the . . . chattels from intrusion, and (b) the use of the particular device is reasonable under the circumstances, and (c) the device is one customarily used for such a purpose, or reasonable care is taken to make its use known to probable intruders.[72]

Similar to the analysis under MPC § 3.06,[73] this section could apply to active defense, with the defender's computer labeled as the device.

Many advocates for active defense in cyberspace cite the doctrine of necessity as justification for entering a network without authorization.[74] According to the Restatement, "[o]ne is privileged to enter . . . land in the possession of another if it is or reasonably appears to be necessary to prevent serious harm to . . . the actor, or his land or chattels. . . ."[75] Relying on this doctrine, and still assuming that data can be characterized as chattels, a defender would be able to access an attacker's network without authorization if such access were to reasonably appear necessary to stop an ongoing, or prevent a future, attack. A proportionality requirement can be inferred by the fact that only necessary actions are permitted.

Finally, some courts have recognized a privilege to enter someone else's land to reclaim stolen property.[76] This privilege is articulated in § 198 of the Restatement and, again, implies that proportionality is required.[77] Section 198 states that "[o]ne is privileged to enter land in the possession of another, at a reasonable time and in a reasonable manner, for the purpose of removing a chattel to the immediate possession of which the actor is entitled. . . ."[78] This section would also support the use of active cyber defense measures intended to reclaim stolen data.

C. Proposed Amendment to the CFAA

As noted above, the CFAA does not allow for any self-defense measures in cyberspace and so any active defense practices would almost certainly violate the statute. Former NSA General Counsel Stewart Baker, however, argued that if a thief steals data, the rightful owner should be given implied authorization to retrieve the stolen material, even if that involves accessing the thief's network.[79] While not a perfect analogy, the old English

---

[72] *Id.*

[73] *See* discussion *supra* Part III a.

[74] Pelker, *supra* note 34, at 438; Smith, *supra* note 13, at 192.

[75] RESTATEMENT (SECOND) OF TORTS § 197 (AM. L. INST. 1965).

[76] KERR, *supra* note 8, at 141.

[77] RESTATEMENT (SECOND) OF TORTS § 198 (AM. L. INST. 1965).

[78] *Id.*

[79] Brian Corcoran, *A Comparative Study of Domestic Laws Constraining Private Sector Active Defense Measures in Cyberspace*, 11 HARV. NAT'L. SEC. J. 1, 14 (2020).

'finders keepers' doctrine in property law states that someone who finds property has rights in that property against everyone except for the rightful owner; while others should be prohibited from further stealing the data, the thief cannot claim rights in the data superior to those of the rightful owner.[80] It seems counterintuitive that a company would be aware of a data breach and yet unable to reclaim its data due to the very law that prohibited the breach in the first place.

To address this incongruency, Congress recently proposed the Active Cyber Defense Certainty Act, an amendment to the CFAA effectively legalizing proportional self-defense in cyberspace.[81] In drafting the amendment, Congress acknowledged cybercrime's growing threat to national security and the associated economic implications.[82] It also referenced the difficulty of prosecuting cybercriminals and the resulting lack of deterrence.[83] Under the proposed amendment, a victim of "a persistent unauthorized intrusion of the individual entity's computer" could launch a counterattack against the alleged hacker.[84] The amendment provides for both an exclusion from the prohibitions under § 1030 and an affirmative defense.[85]

The proposed § 1030(k) creates an exception from the rest of § 1030 for the "use of attributional technology," such as beacons, which "return[] locational or attributional data in response to a cyber intrusion in order to identify the source of an intrusion."[86] This exception only applies if the defensive technology does not cause any destruction of data, impair the functionality of the attacker's computer, or make it easier for others to hack the attacker's network.[87]

In addition to excepting certain acts from § 1030, the amendment proposes § 1030(l), which creates an affirmative defense that may be used by a defender who has taken active defense measures against an attacker.[88] The amendment defines active cyber defense measures as "any measure . . . undertaken by, or at the direction of, a defender . . . consisting of accessing without authorization the computer of the attacker to the defender's own network to gather information in order to" perform a variety of objectives.[89] Under this provision, a defender could utilize the affirmative defense if its

[80] Armory v. Delamirie (1721) 93 Eng. Rep. 664 (K.B.).
[81] Active Cyber Defense Certainty Act, H.R. 3270, 116th Cong. (2019).
[82] *Id.* § 2.
[83] *Id.*
[84] *Id.* § 4.
[85] *Id.* §§ 3–4.
[86] *Id.* § 3.
[87] *Id.*
[88] *Id.* § 4.
[89] *Id.*

unauthorized access of the attacker's computer was to determine the attacker's identity, disrupt a continued attack, or monitor an attacker's behavior to prevent future attacks.[90] The proposed amendment does, however, contain carveouts excluding activity that intentionally destroys information on the attacker's computer not belonging to the victim or recklessly causes any physical or financial harm, along with other overly disruptive behavior, and thereby eliminates the availability of retaliatory strikes and other disproportional measures.[91]

The proposed amendment does not give defenders carte blanche to launch attacks against attackers, even if they do comply with the carveouts in § 1030(l), as defenders must also give adequate notice to the FBI.[92] This requirement mitigates some of the issues with active defense posed above, such as the attacking of intermediary zombie computers and the possible destruction of evidence necessary to charge the initial attacker.[93]

Finally, the amendment would only provide an exclusion from criminal liability; it does not excuse any civil liability that may arise under § 1030(g) due to defensive measures.[94] This further discourages overzealous counterstrikes, as intermediaries unintentionally targeted in an active defense operation could still claim compensatory damages or injunctive relief.[95] Further, the primary issue with § 1030(g)—the fact that perpetrators are difficult to locate—would be alleviated because the defender would have given notice to the FBI of its planned activities, thereby creating a clear trail back to it if something were to go awry.

Overall, the proposed Active Cyber Defense Certainty Act would transform the CFAA for the better—from a statute with little flexibility and no room for self-defense into one that more closely mirrors traditional crime statutes. The amendment would allow the benefits of proportional active defense to be captured, while also reducing the very real risk of unmitigated collateral damage to intermediary networks. The availability of civil remedies and the FBI notice requirement ensure that any resulting damage is duly rectified and overly aggressive active defense tactics would still not be available to defenders, further assuring those arguing against active defense that their fears about escalation and increased damage would not materialize.

---

[90] *Id.*

[91] *Id.*

[92] *Id.* § 5.

[93] *See* discussion *supra* Part I.

[94] H.R. 3270 § 4.

[95] *Id.*

IV. CYBER SELF-DEFENSE ALTERNATIVES

Although most scholars focus on the extreme example of causing destruction through retaliation,[96] there is a spectrum of cyber-self-defense measures that ranges from passive to aggressive.[97] Discussed in this Part are cyber hygiene measures, honeypots, sinkholes, beacons, and, at the aggressive end of the spectrum, hacking back. Some of the more passive measures may not be sufficient to repel an attack, while more aggressive measures would never be deemed proportional to the attack from which they would stem.

The most aggressive and well-known form of cyber-self-defense is hacking back. The goal of this retaliatory hacking could be to recover stolen data, to temporarily disrupt the adversary's network, or to damage the adversary's assets.[98] In 2012, one in every three attendees at Black Hat USA, a cybersecurity conference, reported that they had engaged in retaliatory hacking at least once, with 13% doing so frequently.[99] While this figure may not be perfectly representative of the actions of the broader corporate community,[100] it does illustrate that aggressive measures are not universally opposed and, accordingly, deserve to be analyzed. Conversely, many corporate executives and the Department of Justice have said that they do not support hacking back, as they believe the risks outweigh the benefits in many cases.[101] This further emphasizes the importance of proportionality in an analysis of active defense measures; defenders should only be permitted to carry out initiatives that remain effective while carrying little risk of collateral damage.

At the other end of the spectrum, the most passive forms of self-defense in cyberspace are labeled as cyber hygiene. These are measures taken within the defender's own network to deter and block hackers, such as the use of firewalls. These can work to prevent hackers from accessing the network but lose effectiveness once they are bypassed. Firewalls do not come into conflict with any cyber laws, as they do not involve accessing any networks other than that which they are meant to protect.[102]

---

[96] KERR, *supra* note 8, at 141.

[97] Shackelford, *supra* note 6, at 386.

[98] *Id.*

[99] Pelker, *supra* note 34, at 440.

[100] The company representatives that would choose to attend such a conference may be more inclined to engage in aggressive cyber defensive measures; however, the illegality of these tactics could also lead to underreporting in the survey.

[101] Smith, *supra* note 13, at 180.

[102] *See* Corcoran, *supra* note 79, at 2.

Honeypots are a more aggressive defensive measure, but still take place within the defender's own network. A defender can create fake files, file structures, or servers that appear to be real but are segmented from the rest of the defender's data.[103] Similar to Winnie the Pooh getting caught in a pot of honey, these files attract and isolate intruders so they are easily identifiable.[104] This tactic does not run afoul of statutes prohibiting access to other networks but could be considered a trap and trace device under the Pen Register/Trap and Trace statute.[105] While the Department of Justice has made no official statement determining whether honeypots should be considered trap and trace devices,[106] the fact that honeypots could allow companies to identify the source of hackers' electronic communications indicates that they would likely be included under this statute. If so, they could not be legally used absent a court order.[107]

Similar to honeypots, sinkholes redirect traffic as a domain name is translated to its corresponding IP address by replacing the target IP address with a sinkhole IP address.[108] This allows defenders to watch as potentially malicious traffic enters their local networks.[109] Sinkholes operate to capture incoming data and identify the source of an attack, and therefore may also be considered trap and trace devices.[110] Moreover, sinkholes require coordination with Internet Service Providers or Domain Name System registrars to operate, and these entities have little incentive to assist, even if the activity is deemed legal.[111]

Beacons are more aggressive than honeypots and sinkholes, as they do involve accessing the attacker's network, but still do not aim to cause damage. Further outlined in Part V, beacons can notify a defender when files are removed from its server and alert the defender as to the files' new location.[112] Because the beacons do access the attacker's network, however, they can violate statutes prohibiting unauthorized access.

---

[103] *Id.* at 10.

[104] *Id.*

[105] *Id.* at 11; 18 U.S.C. § 3127(4) ("The term 'trap and trace device' means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication. . . .").

[106] Corcoran, *supra* note 79, at 11.

[107] 18 U.S.C. § 3121(a) ("[N]o person may install or use a pen register or a trap and trace device without first obtaining a court order. . . .").

[108] Corcoran, *supra* note 79, at 12.

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] *See* discussion *infra* Part V.

V. BEACONS AS A PROPORTIONAL RESPONSE

To accomplish proportionality in cyber defense responses, companies should incorporate beacons into their most critical files as a part of their cybersecurity regimen. Beacons are small pieces of code embedded in files likely to be stolen that notify the owner when the files are removed from the owner's network.[113] They are also capable of sending information back to the files' owner, such as the thief's location and IP address.[114] Beacons are a tool commonly used for legitimate purposes by mainstream commercial websites to track activity and traffic.[115] Small, transparent images can be added to websites or emails, unbeknownst to the viewer.[116] When the page is accessed, the image reaches back out to the server on which it is hosted to load.[117] This communication can include information about the system on which the beacon now sits, helping the owner to learn about those accessing the website.[118] This innocuous technique can become a powerful defense tool when used to track cyber thieves.

Similar to the protection offered by a car alarm, embedding an alert into a computer's files that notifies the owner when they have been stolen would add another layer of protection for important data, as it would be easy to identify a breach. Further, similar to a stolen car's GPS tracker, the beacon could alert the victim as to where the data has been taken. This would alleviate any issues in determining who exactly perpetrated the attack. The company could then notify the relevant authorities, who could stop any persistent attacks and charge the hackers involved.

As shown above, an important consideration when dealing with self-defense is proportionality. The Model Penal Code dictates that force should only be used when it is reasonably necessary to protect either oneself or one's property from assailants or to reclaim stolen property[119]—requirements which beacons satisfy.[120] Causing no actual damage, beacons use precisely the amount of force that would be needed for a defender to determine the location of an attacker, allowing the defender to prevent further trespass against his property by notifying the relevant authorities of the attacker's information.

---

[113] Pelker, *supra* note 34, at 445.
[114] *Id.*
[115] *Id.*
[116] *Id.*
[117] *Id.*
[118] *Id.*
[119] *See* discussion *supra* Part III a.
[120] Pelker, *supra* note 34, at 445.

Further, both the Model Penal Code and the Restatement (Second) of Torts allow for self-defense using a device; both employ similar elements to determine if the device's use is proper.[121] A beacon is a useful tool because it satisfies Model Penal Code and Restatement elements.[122] First, a beacon is not meant to cause death or serious bodily harm—it is not intended to cause any damage whatsoever. Next, its use would be reasonable given the circumstances, as it is an effective way for defenders to discover that their data has been stolen and to determine its new whereabouts. Given the difficulty associated with finding and prosecuting hackers, this appears to be one of few viable options defenders may have to locate and eventually reclaim their stolen data. Finally, given that beacons' use as a self-defense tool currently violates the CFAA, the clearer method to satisfy the documents' third element would be to provide notice to assailants.

A company could use a terms of service or user agreement to give notice to anyone entering the company's system that beacons could be deployed.[123] Since intruders do not typically enter through normal channels, however, this notice would have to be apparent at many levels of access.[124] Scholars have suggested that the use of warning banners could alleviate this issue, ensuring that anyone entering the network from any point sees the warning at least once.[125] Courts typically view terms of service agreements as the parameter for authorization to access a network, and therefore as long as the defender does not exceed the access that it warned of, this action may be viewed as legal under the CFAA.[126]

While a beacon would typically constitute unauthorized access under § 1030(a)(2), as it would enter the hacker's computer without authorization and obtain information,[127] the violation would be at maximum proportional to the hacker's malfeasance. Because of this, the use of a beacon would be viewed as acceptable under both criminal and tort self-defense doctrines, should these doctrines be accepted in cyberspace as they are in the physical world.

CONCLUSION

Companies are facing an ever-growing silent threat in the form of hackers and data thieves. While it may seem prudent to allow law

[121] *See* discussion *supra* Part III a–b.

[122] *See id.*

[123] *See* Pelker, *supra* note 34, at 454.

[124] *Id.* at 468.

[125] *Id.*

[126] *Id.* at 454.

[127] Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2).

enforcement to track down and apprehend these criminals, the unfortunate truth is that law enforcement does not have the capacity or the means to tackle the well-hidden attackers who are regularly able to obtain consumer data. Companies must be given the opportunity to work alongside the authorities, using productive self-help measures, to protect their customers' information and their own reputations. Beacons, satisfying the traditional criteria of self-defense, would allow them to do just that. Additionally, allowing defenders to use this tool would decrease their desire to launch destructive counterattacks. Overall, the common use of beacons would increase costs and accountability for hackers and therefore discourage computer misuse crimes, improving the security of data stored in cyberspace while presenting little risk to unwitting third parties.