Record: 1

Title: ZERO-DAY RESPONSIBILITY: THE BENEFITS OF A SAFE HARBOR FOR CYBERSECURITY RESEARCH.

Authors: Emery, Alek Charles

Source: Jurimetrics: The Journal of Law, Science & Technology. Summer2017, Vol. 57 Issue 4, p483-503. 21p. 1 Diagram.

Document Type: Article

Subject Terms: *COMPUTER security
*INTERNET security
*SAFE harbor
*CYBERTERRORISM
*COUNTERTERRORISM
*CRIMINAL law
*COMPUTER security laws
*GOVERNMENT policy
UNITED States
COMPUTER Fraud & Abuse Act, 1984

NAICS/Industry Codes: 519130 Internet Publishing and Broadcasting and Web Search Portals
517110 Wired Telecommunications Carriers

Abstract: There currently exists a practically unregulated -- or under regulated -- market where the most powerful and potentially harmful computer exploits are routinely bought and sold. These cybersecurity commodities are known as "zero-day exploits" -- because there are zero days in which to prepare for the threat. Entities carrying out cyberattacks have used these types of exploits against nation states, like the Stuxnet attack against an Iranian nuclear facility, and against major corporations such as Sony. Although some zero-day exploits are sold to individuals seeking to employ them in cyberattacks, most are sold to United States intelligence agencies for domestic and international surveillance. Many have called for enhanced regulation of this market, but serious challenges remain in finding an effective means of controlling the market without relying on an overexpansion of the current criminal law framework regarding computer "hacking." Given the rapid evolution and complexity of the zero-day exploit market, tort law can provide a new, and more effective, regulatory model. Wherein administrative guidance works in conjunction with tort liability to create a more flexible, and easily administered, regulatory system ensuring that potentially harmful exploits enter the market in a responsible way. CITATION: Alek Charles Emery, Comment, Zero-Day Responsibility: Hie Benefits of a Safe Harbor for Cybersecurity Research, 57 Jurimetrics J. 483-503 (2017). [ABSTRACT FROM AUTHOR]

Full Text Word Count: 9952

ISSN: 0897-1277

Accession Number: 126542986

Database: Academic Search Complete

ZERO-DAY RESPONSIBILITY: THE BENEFITS OF A SAFE HARBOR FOR CYBERSECURITY RESEARCH

There currently exists a practically unregulated -- or under regulated -- market where the most powerful and potentially harmful computer exploits are routinely bought and sold. These cybersecurity commodities are known as "zero-day exploits" -- because there are zero days in which to prepare for the threat. Entities carrying out cyberattacks have used these types of exploits against nation states, like the Stuxnet attack against an Iranian nuclear facility, and against major corporations such as Sony. Although some zero-day exploits are sold to individuals seeking to employ them in cyberattacks, most are sold to United States intelligence agencies for domestic and international surveillance. Many have called for enhanced regulation of this market, but serious challenges remain in finding an effective means of controlling the market without relying on an overexpansion of the current criminal law framework regarding computer "hacking." Given the rapid evolution and complexity of the zero-day exploit market, tort law can provide a new, and more effective, regulatory model. Wherein administrative guidance works in conjunction with tort liability to create a more flexible, and easily administered, regulatory system ensuring that potentially harmful exploits enter the market in a responsible way.

CITATION: Alek Charles Emery, Comment, Zero-Day Responsibility: Hie Benefits of a Safe Harbor for Cybersecurity Research, 57 Jurimetrics J. 483-503 (2017).

Cybersecurity has become a popular issue -- as illustrated by the increasing media coverage of recent cyberattacks.[1] Reports covering attacks against large corporations, including, for example, Netflix and Sony[2] demonstrate the increasing public awareness of cyberattacks and the threats they pose. More recently, concerns over foreign influence on the 2016 U.S. elections via cyberattacks have made national headlines.[3] However, the majority of people who engage with the online environment do not consider, or adequately appreciate, the very real potential threats posed to them as individuals online.[4] Moreover, security vulnerabilities for which there are no existing defenses, so-called "zero-day" vulnerabilities,[5] pose risks to nation states,[6] corporations,[7] and individuals.[8] These vulnerabilities represent a tremendous and ever-present cyber-security threat, and have created a market where they are bought and sold by various actors[9] -- from individuals to national intelligence agencies.[10] Because this market exists within a rapidly evolving technological space,[11] it is difficult to predict what new trends might emerge within it -- making effective regulation difficult to implement.

Recognizing the threat zero-day vulnerabilities present, a growing number of regulatory and policy proposals that have attempted to address the complex issues presented by the market in which they operate.[12] This comment dismisses these proposals for various reasons and argues for a new regulatory model. Specifically, this comment sets forth a national regulatory framework fortius market based on ex post tort liability that is

augmented by an administrative agency, which provides guidelines for defining a liability-limiting safe harbor. This proposal shifts the cost-benefit calculus for actors within the market by creating an economic incentive for responsible actors, via a safe haibor. And, it also creates a corresponding disincentive for selling without sufficient due diligence. This shift encourages responsible selling and development of zero-day vulnerabilities, without some of the logistic difficulties of trying to enforce responsibility through criminal law or direct agency oversight.

I. BACKGROUND

A. A Primer on Computer Networks and Vulnerabilities

In the abstract, a computer network is a group of computers connected together that allows them to communicate.[13] The largest embodiment of this being the Internet, which is constructed as a massive interconnection of computer networks around the world.[14] Privacy regarding communications over remote networks has been an issue since the first wireless networks.[15] As the Internet is an essential part of most people's daily lives,[16] maintaining control over how information is stored and communicated between computers and devices connected to the Internet -- cybersecurity as it has come to be known -- has become an increasingly important and complex national and international issue.[17]

Defining what a computer or security vulnerability is can be complicated. Initially, it might be useful to think of a vulnerability as being any weakness in a computerized system's setup that allows for someone to gain unauthorized access to the system[18] Computer security weaknesses often result from, among other tilings, mistakes in software code, incorrect installation, or poor maintenance by network administrators.[19] For purposes of this comment, the Microsoft Security Response Center (MSRC) definition -- which defines a security vulnerability as "a weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of that product"[20] -- will be used. There is, by the nature of computer networks being designed to facilitate communication between computers, perhaps little that can be done to eliminate all security vulnerabilities.[21] Cybersecurity author Tyler Wrightson has suggested that no computer network is completely invulnerable.[22] For the purposes of this comment, a zero-day "exploit" will refer to a computer program designed to compromise a computerized system's security via a zero-day vulnerability.[23]

Having narrowed the issue to computer software vulnerabilities arising from weaknesses in the various programs on a system's code, it is important to understand the lifecycle of security vulnerabilities. As illustrated by Figure 1, generally, the "timeline" for a vulnerability begins when a software developer releases a product with an unknown weakness, which creates a vulnerability.[24] This vulnerability is then found by either a computer security professional looking to report the vulnerability or by an attacker looking to exploit that vulnerability.[25] Next, the vulnerability is either reported to the developer or used in an attack.[26] After becoming aware of the vulnerability the developers work to produce a security patch and release it to limit the potential damage caused by the vulnerability.[27]

B. Zero-Day Vulnerabilities and Exploits

A zero-day vulnerability is a vulnerability that is found before the software manufacturer has discovered it, or, if the manufacturer has discovered it, before the manufacturer can take action to correct it.[29] Designed to capitalize on this window of opportunity before a countermeasure can be put in place, exploiting a zero-day vulnerability facilitates attacks against targets that have no current means of specifically addressing the attack.[30] This is the power of a zero-day vulnerability; and, it creates both the increased value to attackers and the increased risk posed to those whom might become the targets of cyberattacks.[31] For simplicity, the phrase

"zero-day technologies" will be used hereafter to refer to a category of cybersecurity threats that encompasses both zero-day vulnerabilities and exploits.

Zero-day vulnerabilities are a form of "dual-use" technology, in that they pose both a risk to society based on their misuse, but they also offer a potential benefit to society when used to better prepare computer networks against attack.[32] Hie implications of which reach from protecting the national infra-stmcture down to protecting the individual consumer from identity theft.[33] Additionally, the potential beneficial uses of zero-day technologies by intelligence agencies who purchase them can be argued as a primary benefit of alio vying the private sector to continue to develop, and employ, these technologies.[34] Benefits being derived from both the potential offensive use of such vulnerabilities, as in the Stuxnet attack, and also from the increased awareness and opportunity it provides to our government to prepare for attacks against our infrastructure and citizens.[35] Granted, the dangers posed by these technologies when put into the wrong hands are very real, but it is important to recognize the potential benefit derived from research into this field.[36]

C. The Market for Zero-Day Exploits

Computer vulnerabilities have become increasingly valuable, and a market for selling the most valuable vulnerabilities -- zero-day vulnerabilities -- has emerged.[37] It is important to understand this market's terminology, which is used by both computer security professionals and hackers.[38] Experts looking to discover vulnerabilities while working for software vendors or providing vendors with free information to create more secure systems are referred to as "white hats," while security experts seeking to employ the same techniques for illegal or unauthorized use are known as "black hats."[38] Between the "white" and "black" positions are "gray hats" who seek to discover and sell security vulnerabilities to software vendors, government agencies, or third parties for a profit.[40]

The market for zero-day vulnerabilities and exploits can generally be described according to these classifications. White hats seek to discover and then privately disclose security vulnerabilities to software vendors because they are either contracted for such work or perform such work out of beneficence.[41] The "white hat market" represents the least threat for abuse, and offers some of the most direct benefits of research into zero-day vulnerabilities.[42] Bounty programs -- where software vendors offer rewards for information regarding security vulnerabilities -- like the Windows Bounty Program created by Microsoft, incentivize white hats by offering a legitimate financial reward for discovering vulnerabilities.[43] Gray hats sell vulnerabilities they discover to corporations or government agencies; attempting to make a profit on their work and obtain a greater financial return by selling to a legitimate agency on the open market.[44] Zero-day vulnerabilities can be extremely valuable -- with "zero-day brokers" (like Zerodium) who purchase zero-days to create cybersecurity and surveillance products, offering up to $US 1 million dollars for some zero-day vulnerabilities.[45] Black hat selling refers to the secretive selling of zero-day exploits to anonymous third parties by independent researchers or hackers over the dark web.[46] The motive is to sell to the highest bidder with as little evidence of the sale as possible.[47] The "black hat market" represents the greatest threat to national and public security, because in such a market, the buyer could be anyone; be it a government agency like the National Security Agency (NSA) or a terrorist organization like the Islamic State of Iraq and Syria (ISIS).[48]

II. CURRENT REGULATORY FRAMEWORK AND RECENT DEVELOPMENTS

Given the increased public and private attention towards cybersecurity over the last few years, it is unsurprising that there have been calls both domestically and internationally for regulation of the zero-day technologies market.[49] However, regulation of such a market has proven very difficult from both a policy and a practical perspective.[50] Calls for regulation have been met with industry scrutiny,[51] and there is concern

that government intrusion into the zero-day market will incentivize actors to engage in more anonymous selling as they attempt to avoid greater oversight.[52]

Proposals for regulation of the zero-day market generally tend to rely upon three different strategies of varying degrees of restrictiveness:

1. calling for application of criminal law to regulate the market[53]
2. proposing applying liability to software developers for releasing vulnerable software[54]
3. advocating for increased export control based on domestic and international law to regulate the trafficking of zero-day technologies internationally[55]

There is a tension between these different regulatory strategies regarding the extent to which they propose to restrict the zero-day market.[56] Generally, proposals put forward by governments tend to be the most restrictive, industry proposals appear to be the least restrictive, while those developed by academics, including Paul Stockton and Mchele Golabek-GoldmanorKelsey Annu-Essuman take a more moderate approach.[57] Importantly, however, proposals do not always fit neatly into this categorization or rely upon a single regulatory strategy; rather, many tend to include recommendations varying the degrees to which they apply multiple strategies -- but for each of these strategies remain challenges to effective and efficient regulation.[58]

A. Using Criminal Law to Regulate the Zero-Day Vulnerability Market

Criminal law is designed to carry "the condemnation of the community" for acts that it wants to deter.[59] Currently, the United States criminalizes computer "hacking" under the Computer Fraud and Abuse Act (CFAA).[6]'[1] Under the CFAA, a person who "knowingly causes the transmission of a program information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer" may face criminal penalties.[61] While the element of intent would arguably make the CFAA in its present form difficult to apply directly to those selling zero-day exploits,[62] the CFAA has already been interpreted expansively.[63] Charges under the CFAA have been brought against hackers outside the territorial boundaries of the United States, when the effects of their attacks were directed at U.S. corporations.[64] The CFAA has also been used in at least one criminal case where criminal liability for conspiracy to violate the CFAA was applied to someone operating a website that could serve as a marketplace for zero-day and other security vulnerabilities.[65]

Governments have been primarily concerned with cyberattacks against national infrastructure, like the power grid and traffic control systems, and have put forward restrictive regulatory proposals to combat this risk.[66] This risk is heightened when dealing with zero-day technologies, because of their unknown nature and potential use to target important systems like Industry Control Systems (ICS).[67] A number of governments, including the German government, have responded to this risk through expansion of criminal laws to cover activities outside of actually hacking a computer.[68] The German Parliament has passed legislation that makes it a crime to sell, supply, disseminate, or otherwise make available "software for the purposes of the commission of [gaining unauthorized access to another's data]."[69] Similarly, Stockton and Golabek-Goldman argue that within the United States, criminalization should be made to cover the selling of zero-day exploits that threaten critical U.S. infrastructure.[70] They argue that the serious threat to systems, like the U.S. power grid, warrant the imposition of severe criminal penalties to deter actors from engaging in sales of zero-day vulnerabilities and exploits to people who might use them against the United States.[71]

Criticisms regarding the expansion of the CFAA are powerfully made by several authors, including Oxford University Marshall Scholar Mailvn Fidler.[72] A central concern is the loss of potentially beneficial societal

gains, like the development of new cybersecurity tools, derived from zero-day vulnerability research.[73] Economic arguments regarding the benefits of allowing for "ethical hacking" or white-hat hacking suggest that controlling zero-day technologies through criminal law intervention might produce a negative overall effect.[74] Another issue facing criminalization is the ex ante application of the law towards researchers working for a beneficial purpose.[75] Researchers and security professionals often rely on the same techniques and tools employed by black-hat hackers[76] and developers of zero-day exploits.[77] To preserve the beneficial gains made by responsible research into zero-day vulnerabilities, researchers need to have some clarity in regards to what conduct they need to conform with.[78]

There are also issues surrounding the application of criminal law to zero-day vulnerability research because this conduct is outside its traditional scope. Fidler notes there are issues with defining both the scope of the expansion under the CFAA. according to the Stockton and Golabek-Goldman proposal, and that there remain issues of uncertainty in regards to the extraterritorial application of such an expansion.[79] While the CFAA has been used before to bring criminal charges for activities carried out beyond the territory of the United States, those activities demonstrated a clear intent to create harms within, and against, the United States.[80] Authors Preston and Lofton, in discussing the economics surrounding public disclosure of software vulnerabilities, also note that shifting liability onto researchers, both civil and criminal, can have a chilling effect on the creation of computer code -- which as a creative form of expression can arguably be construed as free speech.[81] The potential free-speech issues surrounding the criminalization of this research, especially if intended to be enforced extraterri-torially, presents an extremely difficult problem for any criminal law legislation.

Given the dual-use nature of zero-day technologies, the speed with which these technologies continue to evolve, and the practical difficulties of ex ante application, expansion of criminal law statutes to regulate the zero-day market is not an attractive option.

B. Applying Liability to Software Vendors

Regulatory actions taken to control the zero-day market should be tailored to produce the maximum benefit to security, both from a governmental standpoint as well as from a public perspective.[82] Given the practical difficulties in regulatingthe zero-day market through criminal penalties, some have suggested using tort law to implement regulation.[83] Professors Michael Rustad and Thomas Koenig suggest that the actors most effectively reached by regulation are the software vendors, and that tort liability should be placed on them for negligently releasing vulnerable software.[84] Rustad and Koenig argue that employing a tort liability framework for software vendors who release products with vulnerabilities will encourage the production of more secure programs and reduce cybercrime.[85] Additionally, they note that a tort of "negligent enablement of cybercrime" could be imposed on software vendors who fail to "incorporate reasonable security into their products and services."[86]

While this application of software vendor liability has some potential benefits, there are application issues for this type of liability -- specifically in regards to zero-day vulnerabilities.[87] Most notably, at least some zero-day vulnerabilities are likely to remain undiscovered even by the reasonable efforts of a software vendor because of their "unknown" or never-seen-before nature -- which is what makes these vulnerabilities valuable.[88] Some studies have suggested that a large percentage of security vulnerabilities remain unknown, and that zero-day vulnerabilities are less rare than commonly believed.[89] Hoping to curtail the release of software that contains zero-day vulnerabilities is not necessarily feasible,[90] and defining the "reasonable security measures" that would qualify under the negligent enablement of cybercrime tort, should it be implemented, may prove extremely difficult.[91] There also may be issues about imposing liability on foreign actors, though

such issues might be similar to imposing product liability on foreign manufacturers of other products.[92] Imputing liability to software developers might also come at the risk of stifling innovation.[93] While the use of tort law to regulate the zero-day market by imposing civil liability for negligently vulnerable software offers some attractiveness in light of the difficulties posed by using cri minal law. again the potential losses of such regulation miglit outweigh the benefits.

C. Regulation Through Export Control

One common theme regarding regulatory proposals for the zero-day market is that the international nature of the cybersecurity makes any type of regulation difficult. Extraterritorial application of criminal or civil laws can be problematic,[94] so calls for international law based regulations are common.[95] A discussion of the primary international treaty regulating export of zero-day-technologies to which the United States is a party is presented below, along with discussion about the limitations of such a regulatoiy approach.

The United States is a party to the Waasenaar Arrangements (WA) on export controls for conventional arms and dual-use goods and technologies.[96] With the goal of "promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies." the WA seeks to have states create their own national policies regarding the exports of dual-use technologies.[97] There are currently forty-one participating states to the WA.[98] Given the global nature of the Internet and cybersecurity, several authors have incorporated international law-based export controls into their regulatory proposals.[99] For example, the U.S. Bureau of Industry and Security (BIS) recently proposed regulations that attempt to regulate export of zero-day technologies under a licensing regime. Under the proposed BIS licensing regime, the export of such technologies could be restricted unless the exploit is approved by the government agency overseeing exports.[101]

Despite there being some agreement that export controls should be put in place to prevent zero -day exploits from ending up in the hands of terrorists, there has been serious criticism raised regarding the rules that BIS proposed.[102] hi particular, the requirement that the vulnerabilities be turned over to the federal agency for approval, and the likelihood of thembeing used by government agencies whose methods might be contrary to those of the seller's wishes[103] is likely to have a chilling effect on the beneficial research into such technologies. It is important that the United States create export controls under the WAto promote keeping zero-day vulnerabilities and exploits from being used by terrorist organizations, but such regulations should preserve the benefits derived from such dual-use technology.[104]

III. EX POST REGULATION BASED ON TORT LIABILITY AND FEDERAL AGENCY ADMINISTRATION

The proposals articulated above all address important regulatory considerations regarding how to oversee the zero-day market. However, individually they do not create a regulatory framework that does enough to retain the potential benefits of zero-day research. The application of ex post tort liability -- in conjunction with a liability safe harbor defined by regulatory guidelines promulgated by a federal agency regarding the due diligence required for sales of zero-day technologies -- offers a more satisfactory compromise in balancing attempts to control the zero-day market against retaining the benefits it currently provides. Such regulatory guidelines can serve to ineentivize responsible zero-day vulnerability research and impose controls on their sale and work in conjunction with export controls under the WA. Additionally, the current application of the CFAA to criminal use of zero-day technologies provides a sufficiently broad pronouncement to indicate what conduct regarding the use of zero-day technologies will be permitted and may work in concert with the proposed regulations. A discussion of this regulator}- scheme's components is presented below, along with a discussion of additional issues that will need to be addressed in implementing such a scheme.

A. The Proposed Regulatory Framework

Effective regulatory proposals should exert a normative influence on actors subject to the regulation by offering actors an incentive to comply with the regulations, and by discouraging them with punishment if they fail to conform[105] This "carrot vs. stick" determination is one of the starting points in creating a regulatory framework, because it can be determinative on whether to pursue a criminal or civil remedy to a problem[106] An ex post civil liability framework based in tort law to oversee actors, individuals or companies, who research or sell zero-day vulnerabilities and exploits used in conjunction with a liability safe harbor can strike the appropriate balance. While such regulations are domestic in nature, they will influence the market by shifting the cost-benefit considerations in working with zero-day technologies.[107] Because the market is global in nature, economic pressures on sellers in the market should have international effects -- which is especially true considering that the largest purchaser of zero-day technologies is the U.S. government.[108]

In general, a federal statute should be passed that clearly indicates when liability will attach, thus preempting inconsistency in the law among the states and preventing the ad hoc stretching of current tort and criminal laws to regulate the research and selling of zero-day technologies. Additionally, a federal agency -- perhaps as a division under the Department of Homeland Security like the United States Computer Emergency Readiness Team (US-CERT) -- should be tasked with promulgating a series of guidelines mandating the due diligence required before a sale of a zero-day vulnerability or exploit. These guidelines can serve as a basis for shielding an actor selling such a vulnerability or exploit from ex post liability if the actor conformed their acts within the guidelines. These guidelines can also be crafted to address issues surrounding international export of zero-day technologies to fulfill U.S. obligations under the WA. The specifics of the framework and the benefits of such a system over currently proposed systems are discussed below.

B. Statutory Civil Liability

A federal statute should be passed to create a national civil liability scheme to attach liability to sellers within the zero-day market who seek to sell, import, or export zero-day technologies. This statutory civil liability should be applied to the selling of zero-day technologies rather than expanding the current criminal law framework under the CFAA because such an expansion will likely come with detrimental effects, including a loss of potentially beneficial research.[109] Such a regulatory scheme can impose civil liability for damages resulting from negligent sales of zero-day technologies and influence the economics of the marketplace by shifting the potential risk involved in any sale.[110] While the regulations themselves are domestic, their effects, when used in conjunction with a liability safe harbor, may be used to influence the marketplace to global effect and serve to supplement current domestic criminal and international law.

One the primary benefits derived from research into zero-day vulnerabilities is the discovery and reporting of security flaws so that software patches can be released in a timely manner.[111] Therefore, any proposed regulations should seek to offer those who provide beneficial research certainty that they will not ran afoul of civil or criminal liability for their work, which as a necessity, will often involve exactly the same types of research and development as those who would use these zero-day vulnerabilities for harm.[112] The need to provide certainty to researchers suggests that an expansion of the current criminal law framework regarding computer hacking will too dramatically reduce the benefits derived from such work.[113] The CFAA is already expansively interpreted, often being stretched to cover essentially any unauthorized access to any computer -- due to the likelihood of that computer having participated in interstate commerce.[114] Researchers will be less likely to continue to work in the field if there is uncertainty that their work will result in them suffering criminal penalties.[115]

Additionally, those actors that are arguably the most dangerous -- individual black-liat actors seeking to sell zero-day vulnerabilities and exploits anonymously in private chatrooms and dark-web marketplaces -- will likely not be dissuaded from engaging in such behavior by the "stick" threatened by further criminal penalty. It is very difficult to catch, let alone prosecute, cybercriminals; it takes a tremendous amount of time and money to do so because it is possible to create nearly complete anonymity online.[116] These considerations demonstrate that the criminal law is poorly suited to deal with such dual-use technologies.

Moreover, the technologies being addressed are rapidly evolving.[117] Creating criminal statutes is a timely legislative process that is slow to adapt to an ever-changing environment of new cybertechnologies and vulnerabilities. Granted, some of the principles will remain the same. For example, a distributed denial of service (DDOS) attack will result in the same types of harm as before, but the means by which these attacks are carried out will likely evolve faster than the criminal law can adapt.[118] This rapid evolution in the way attacks are carried out will likely result in a demand to continuously expand the criminal law until it becomes such an impediment that it disproportionately hampers beneficial development or provides a degree of uncertainty in its scope that it will be unreasonably difficult to conform with.[119] Criminal law is designed to carry with it the weight of the public's condemnation of an act.[120] Expanding the criminal law to cover increasingly less offensive conduct in an effort to prevent a particular type of harmful conduct is not sound public policy.[121]

Therefore, regulation of a dual-use technology through ex post civil liability offers a more appealing compromise between maintaining the benefits of research into zero days and attempting to prevent their harmful use when used in conjunction with an appropriate incentive -- like a liability safe harbor.[122] The goal is to encourage people to continue to work in the field while making sure that their work is being used responsibly. Federal agency regulations can provide the needed certainty in the law to allow actors to responsibly research zero-day technologies. The potential to avoid civil liability by conforming with such guidelines is an incentive that will use market forces to increase compliance. Rather than push those seeking to sell such technologies further into the dark web, an opportunity to gain a more legitimate profit will encourage broader compliance and address many of the same harms. These regulations create a financial incentive to operate within the industry in a responsible manner, and the market influence created by such regulations may have global effect. Moreover, because the civil liability standard can be based on agency guidelines, rather than criminal statutes and the common-law process of developing potentially inconsistent case law, the civil system will be better suited to adapt to a rapidly evolving technology.

C. Federal Agency Regulations

The rise of U.S. federal agencies in regulating technologies, like the Federal Communications Commission (FCC) and Federal Trade Commission (FTC), can be tied in part to the increasingly technical nature of the technologies they oversee and the pace at which those technologies evolve.[123] Simply put, it is more effective to delegate authority to a federal agency tasked with regulating a rapidly evolving technology than it is to go through the legislative process and put proposed regulatory changes before Congress.[124] Agency regulations also provide a period for public comment, and agencies can work closely with industry experts to ensure that regulations are kept current and address emerging needs.[125] Therefore, it would be advantageous to create a civil liability scheme based on conformity with guidelines promulgated by an agency tasked with providing up-to-date and minimally intrusive due-diligence requirements.

The selected agency will create a set of rules and best-practice guidelines for actors intending to research, sell, or export zero-day vulnerabilities and exploits. Some proposed regulations have called for a licensing arrangement, wherein actors looking to sell can reveal who they are selling to and what they are selling to

obtain government approval.[126] This raises objections from those who may not want to turn over every vulnerability discovered to the government before it can be sold.[127] This is illustrative of the concern that an overly intrusive regulatory policy towards zero-day technologies and research will disproportionately diminish the beneficial research into zero-day vulnerabilities.[128]

A proper regulatory mechanism should take into account the benefits gained by the responsible discovery of zero-day vulnerabilities, and measures taken should be weighed against the potential benefits losl.[12]". lj-.v Technica editor Sebastian Anthony commented that "the threat of zero-days is largely driven by fear, uncertainty, and doubt."[130] Calls to entirely curtail the market for zero-day technologies fail to recognize two points: (1) the difficulties of achieving that type of control over an activity taking place in an environment like the Internet, especially those that largely exist and take place in the dark web,[131] and (2) the benefits available from encouraging responsible research, disclosure, and sale of these technologies.

Many zero-day vulnerabilities are bought by software developers, like Microsoft, through bounty programs.[132] Government agencies, like the CIA and NSA, are the single largest purchasers of zero-day technologies.[133] Regulations that go too far in prohibiting beneficial research might actually exacerbate any weakness faced by corporations or national infrastructure, as it may prevent the research and disclosure of such vulnerabilities so that security patches may be created before an attack occurs.[134] In fact, the driving forces behind the black market for exploits is the limited economic return available to researchers and the fear of liability for conducting and disclosing that research.[135] Moreover, because the largest buyers within the marketplace are U.S. based, U.S. domestic regulations within the United States can have expansive reach internationally -- a concept that has lead for some to call for regulation through the United States, "cornering" the market through increased purchase frequency.[136]

Guidelines should be created that require a seller to perform due diligence before the sale to help prevent the acquisition of zero-day technologies by known unethical buyers, criminal buyers, or those who camiot provide legitimate credentials for their purchase.[137] However, in contrast to the recommendations made by Stockton and Golabek-Goldman,[138] it can be argued that mandatory licensing for the sale of zero-day technologies should not be put in place for international sales. Moreover, the affirmative duty to perform reasonable due diligence for the sale of a zero-day exploit was proposed by Stockton and Golabek-Goldman in regards to an expansion of the CFAA to criminalize the sale of potentially dangerous zero-day exploits within the United States,[139] but this duty would be more advantageously applied within the context of civil law. The selected government agency should coordinate with the Department of Homeland Security to ensure that a database of known potential threats is made available to sellers, and to make clear to sellers that they face severe civil liability for any illegal damages caused by exploits sold to these actors.

The guidelines should provide clarity on what amount of research and due diligence must be performed by a seller towards a potential buyer, and what records must be maintained to avoid liability. Defining the amount of required due diligence before a sale will be a significant challenge, but it may be possible to look to regulatory systems put in place for other types of sales[140] or work with industry experts to determine what amount should be required.[141] Guidelines that provide a clear notice to researchers and potential sellers about what they must do to limit their civil liability will less dramatically diminish the beneficial research being done on zero-day vulnerabilities than further expanding the reach of the CFAA.

The appropriate balance between oversight and promoting beneficial use as well as determining the specific requirements of guidelines can be fine tuned incrementally in response to changing market conditions. Because the agency can go through the public comment process and make changes to the guidelines more

rapidly than can the legislative process, the guidelines can be kept up to date and revised as technological advances require. The agency may also work with the cybersecurity industry to determine the proper scope of the proposed guidelines. Additional study will also be required to fine tune the guidelines to strike the appropriate relationship between existing criminal and international laws regarding cybersecurity and to ensure that the gaps within those systems are addressed by the new regulatory scheme. The challenges facing such regulation make the process difficult -- but by working to promote beneficial use in a way that is minimally restrictive, hopefully the benefits will outweigh the administrative and judicial costs.[142]

Existing proposals for regulating the zero-dav market do not reach the most beneficial balance between maximizing safety and preserving the benefits of zero-day vulnerability research. The dual use of zero-day technologies underlies the need for regulation that preserves our ability to derive benefit from these technologies and the research that goes into them While zero-day exploits are rarely used in attacks on individual citizens, the effects of their attacks are felt by society. Preventing the harms caused by actors who sell these technologies irresponsibly can be more effectively done by imposing ex post liability on sellers who fail to perform a reasonable amount of due diligence prior to sale. The due diligence required can be specifically outlined and disseminated by a federal agency tasked with promulgating such guidelines and keeping them up to date. This provides a level of certainty for researchers to conform their conduct to the guidelines and continue to provide beneficial research, while a safe harbor for liability based on conformity with the guidelines creates a powerful incentive for sellers to conform rather than retreat further into the depths of the dark web. By manipulating the economic considerations within the market through civil-liability based regulation, there is the opportunity for increased responsibility within the marketplace without the additional costs of direct agency oversight. Likewise, this regulatory approach avoids the risks of continuing to expand the already broad application of the CFAA. Moreover, while such regulations are domestic in nature, they can influence economic considerations in the global marketplace, and hopefully reach actors who would otherwise fall beyond the reach of traditional regulatory methods.

Footnotes

1. See 'Internet of Things ' Hacking Attack Led to Widespread Outage of Popular Websites. NPR (Oct. 22. 2016. 8:10 AM), http://www.npr.org/2016/10/22/498954197/internet-outage-update-internet-of-things-hacking-attack-led-to-outage-of-popula (providing the transcript of an interview between Alina Selyukh and Scott Simon regarding recent Internet of Tilings (IoT) attacks and how it has made Dyn. an Internet company whose servers help connect users to many popular websites, go from essentially unknown to widely discussed).

2. See id.; see also Andrea Peterson. The Sony Pictures Hack, Explained. WASH. POST (Dec. 18. 2014). https://www.wasliingtonpost.com/news/the-switcli/wp/2014/12/18/the-sony-pictures-hack-explained/ (discussingthe cyberattack on Sony Pictures attributed by U.S. agencies to North Korea).

3. See, e.g., AdamEntous & Ellen Nakasliima. FBI in Agreement with CIA that Russia Aimed to Help Trump Win White House, WASH. POST (Dec. 16. 2016). https://www.Wasllingtonpost.com/ politics/clinton-blames-putiiis-personal-gnidge-agaiiist-her-for-election-interference/2016/12/16/12f3 6250-c3be-I le6-8422-eac61c0ef74d story.html.

4. See Emily Price, 5 Things You Do Everyday That Make You Vulnerable Online, ENTREPRENEUR (Sept. 14, 2015), https://www.entrepreneur.com/article/250405 (discussing popular activities online that increase vulnerability to cyberattacks for individuals); see also James Titcomb, Do YouHaveOm of the Most Common Passwords? They 're Ridiculously Easy to Guess, TELEGRAPH: TECH. (Mar. 23, 2016,1:35 PM), http://www.telegraph.co.uk/technology/2016/01/26/ most-common-passwords-revealed -- and-theyre-

ridiculously-easy-to/ (examining recent report of most commonly used passwords being too obvious to pose real security benefit).

5. For a definition and background information on what a zero-day exploit is and how they are deployed, see What Is a Zero-Day Exploit?, FIREEYE, https://www.fireeye.com/current-tlireats/ what-is-a-zero-day-exploit.html (last visited Sept. 17, 2017) ("It is an unknown exploit in the wild that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes some tiling is wrong.").

6. See Kim Zetter, An Unprecedented Look at Stuxnet, The World's First Digital Weapon, WIRED (Sept. 3, 2014, 6:30 AM), https://www.wired.com/2014/ll/countdown-to-zero-day-stuxnet/ (noting how the Stuxnet virus was spread throughout an Iranian uranium enrichment facility in part through a "print-spooler zero-day exploit").

7. See Arik Hesseldahl, Here's What Helped Sony's Hackers Break In: Zero-Day Vulnerability. RECODE (Jan. 20. 2015. 5:42 AM). http://www.recode.net/2015/l/20/11557888/heres-what-helped-sonys-hackers-break-in-zero-day-vuhierability (reporting that the worst corporate cy-berattack to date against Sony was facilitated by a zero-day exploit).

8. See Jessica Conditt. Apple Patches Three Zero-Day Exploits After Activist Is Hacked, ENGADGET (Aug. 25. 2016). https://www.engadget.coni/2016/08/25/apple-iphone-security-flaw-update-activist-hack/ (reporting on Apple's move to patch zero-day exploits after human-rights activist Ahmed Mansoor's iPhone 6 was hacked using zero-day exploits created by Israeli computer security company NSO Group).

9. SYMANTEC. INTERNET SECURITY THREAT REPORT 5 (2016). https://www.syniantec.coni/content/dani/syniaiitec/docs/reports/istr-21-2016-en.pdf ("[A] market has evolved to meet demand. In fact, at the rate that zero-day vulnerabilities are being discovered, they may become a commodity product.").

10. See Paul N. Stockton & Miehele Golabek-Goldman. Curbing the Market for Cyber Weapons. 32 YALE L. & POL'Y REV. 239. 248 (2013) (describing an "anarchic black market for [zero] day exploits where vulnerability researchers often sell exploits to criminal hackers, terrorist organizations, and rogue nations").

11. See, e.g., Brian Burrough, How a Grad Student Found Spyware That Could Control Anybody's iPhone from Anywhere in the World, VANITY FAIR (Nov. 28, 2016, 5:00 AM), http:// www.vanityfair.com/news/2016/11/how-bill-niarczak-spyware-can-control-the-iphone (discussing the emergence of the zero-day market within the context of a story about the discovery of a zero-day exploit).

12. See, e.g., Stockton & Golabek-Goldman. supra note 10. at 242-43.

13. Vangie Beal. Network, WEBOPEDIA http://www.webopedia.eom/TERM/N/network.html (last visited Sept. 17. 2017).

14. See Rus Shuler. How Does the Internet Work?, SHULERS (2002). http://www.theshulers.com/wliitepapers/internet%5Fwhitepaper/index.html (describing how the Internet is structured and providing an overview of the protocols computers use to communicate over the Internet).

15. See Amanda OftvS, A History of Hacking, IEEE: INST. (Mar. 6. 2015). http://theinstitute.ieee.org/technology-topics/cybersecurity/a-history-of-hacking (recounting the story of John Mas-kelyne's attack on Guglielmo Marconi's early 1900s wireless telegraph network).

16. See, e.g., OFCOM. ADULTS' MEDIA USE AND ATTITUDES 9 (2016). https://www.ofcom.org. uk/ data/assets/pdf%5Ffile/0026/80828/2016-adults-media-use-and-attitudes.pdf ("UK adults spend an average of 21.6 hours online each week □ .").

17. Seegenerally Nazli Choucri et al.. Institutions for Cyber Seairity: International Responses and Global Imperatives, 20 INFO. TECH. FOR DEV. 96 (2014) (describing international framework and national organizations created to address increasingly important and global cybersecurity issues).

18. See I ulnerabi/it)', TECHOPEDIA, https://www.techopedia.com/defmition/13484/vulnerability (last visited Sept. 17. 2017).

19. See Vulnerabilities. NORTON, https://us.norton.com/security%5Fresponse/wlnerabilities.jsp (last visited Sept. 17. 2017).

20. Definition of a Security Vulnerability. MICROSOFT DEVELOPER NETWORK. https://msdn. microsoft.com/en-us/library/cc751383.aspx (last visited Sept. 17. 2017).

21. See EDUARDO GELBSTEIN & AHMAD KAMAL. INFORMATION INSECURITY: A SURVIVAL GUIDE TO THE UNCHARTED TERRITORIES OF CYBER-THREATS & CYBER-SECURITY 1-3 (2d. ed. 2002).

22. See TYLER WEIGHT SON. ADVANCED PERSISTENT THREAT HACKING: THE ART AND SCIENCE OF HACKING ANY ORGANIZATION 26 (Brandi Shailer et al. eds.. 2015) ("We live in a world where an attacker can infiltrate any organization.").

23. See Margaret Rouse. Exploit. TECHTARGET. http://searclisecurity.techtarget.com/definition/ exploit (last updated Sept. 2005) ("In computing, an exploit is an attack on a computer system, especially one that takes advantage of a particular vulnerability that the system offers to intruders.").

24. What Is a Zero-Day Exploit?. supra note 5 (discussing the timeline of a security vulnerability in the context of a newly discovered, and potential zero-day vulnerability).

25. Id.

26. Id.

27. Id.

28. Adapted from Pierluigi Paganini, A World of Vulnerabilities, INFOSEC INST. (Nov. 28, 2012), http://resources.iiifosecinstitute.com/a-world-of-viilnerabilities/ (fig. 3). The figure draws inspiration from Paganini's representation of a visualization of the zero-day exploit life cycle. For clarity, the introduction of the vulnerable software has been omitted -- as the relevant period for this comment's regulatory proposal begins after a vulnerability has been discovered.

29. What Is a Zero-Day Exploit?, supra note 5.

30. Id.

31. See Sebastian Anthony, The First Rule of Zero-Days Is No One Talks About Zero-Days (So We ll Explain), ARS TECHNICA(Oct. 20,2015, 5:00 AM), http://arsteclinica.com/seeurity/2015/ 10/the-rise-of-the-zero-day-niarket/ (discussing how it is the unknown nature of a zero-day vulnerability that makes it valuable).

32. See Patrick Brannon, Regulating Zero-Day Exploits Is a Really Bad Idea, INT'L ASS'N PRIVACY PROFS. (Dec. 15, 2015), https://iapp.org/news/a/regulating-zero-day-exploits-is-a-really-bad-idea/ (discussing how zero-day vulnerability research can be beneficial to cybersecurity).

33. See supra notes 5-11 and accompanying text.

34. See Mailyn Fidler. Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis. 111/S: J.L. & POL'"Y FOR INFO. SOC'Y 405.448-49 (2015).

35. See id. at 476-78.

36. See Bramion. supra note 32 (discussing how zero-day vulnerability research can be beneficial to cybersecurity); see also Ethan Preston & John Lofton. Computer Security Publications: Information Economics. Shifting Liability and the First Amendment, 24 WHITTIER L. REV. 71. 129- 42 (2002) (commenting on the potential economic benefits gained from having some computer hacking).

37. See CHARLIE MILLER. THE LEGITIMATE VULNERABILITY MARKET: INSIDE THE SECRETIVE WORLD OF 0-DAY EXPLOIT SALES 2 (2007). http://www.econinfosec.org/arcliive/weis 2007/papers/29.pdf.

38. See PATRICK ENGEBRETSON. THE BASICS OF HACKING AND PENETRATION TESTING 2 (2d ed. 2013).

39. Id. at 3-4.

40. Trevor A. Thompson. Terrorizing the Technological Neighborhood: The Alienation and Deterrence of the "White Hats " Under the CFAA, 36 FLA. ST. U. L. REV. 537, 556 (2009) ("[SJince some activities do not necessarily lend themselves to a binary classification, mixed terms such as 'gray hat" have also been employed.").

41. See Stockton & Golabek-Goldman, supra note 10, at 247.

42. See id. at 247-18.

43. See KimZetter, Hacker Lexicon: What Are White Hat, Gray Hat. and Black Hat Hackers?, WIRED (Apr. 13, 2016, 5:03 PM), https://www.wired.com/2016/04/hacker-lexicon-white-hat-gray-hat-black-hat-hackers/ ("[WJliite hats can earn good money -- anywhere from $500 to more than $100,000 -- by selling information about a vulnerability to companies that have bug bounty programs."); see also MSRC Team, Announcing the Windows Bounty Program, MICROSOFT: TECHNET BLOG (July 26, 2017), https://blogs.teclinet.niicrosoft.coni/nisrc/2017/07/26/announcing-the-windows-bounty-prograni/.

44. See Stockton & Golabek-Goldman, supra note 10, at 247-248.

45. Anthony, supra note 31 ("Zerodium, which bills itself as a broker of 'premium zero-day vulnerabilities," said it would pay up to $1 million (£650,000) for an iOS 9 zero-day.").

46. See Stockton & Golabek-Goldman, supra note 10, at 248. For an interesting account of what the "dark web" is and what it is actually like, see Joseph Cox, The Dark Web as You Know It Is a Myth, WIRED (June 18, 2015, 7:00 AM), https://www.wired.com/2015/06/dark-web-know-niytli/.

47. See Anthony, supra note 31 (discussing how sales often take place on the "dark web" using Tor and Bitcointo increases anonymity).

48. See Stockton & Golabek-Goldman, supra note 10, at 248^19.

49. See. e.g., STRAFGESETZBUCH [STGB] [PENAL CODE] § 202(c), translation at https:// www.gesetze-ini-internet.de/englisch%5Fstgb/englisch%5Fstgb.html+754 (Ger.); James Ball, Secrecy Surrounding 'Zero-Day Exploits' Industry Spurs Calls for Government Oversight, WASH. POST (Sept. 1, 2012), https://www.wasliingtonpost.coni/world/national-security/secrecy-surrounding-zero-day-exploits-industry-spurs-calls-for-governnient-oversight/2012/09/0 l/46d664a6-edf7-l lel-afd6-f55f84bc0c41%5Fstory.html (describing calls for regulation of the market within the United States).

50. Compare Stockton & Golabek-Goldman, supra note 10, at 261 (arguing for an expansion of the CFAA to regulate the market for zero-day exploits through criminal law), with Fidler, supra note 34 (arguing against the Stockton and Golabek-Goldman proposal for expansion of the CFAA).

51. See Brannon, supra note 32.

52. See Stockton & Golabek-Goldman. supra note 10. at 241 (discussing how skeptics of calls for regulation have claimed that "[regulations may simply drive sellers onto the underground market").

53. See id. at 255-64 (arguing for expansion of criminal law and international export control through licensing).

54. See Preston & Lofton, supra note 36. at 131-41 (arguing for liability protection for those working in cybersecurity research); see. e.g., Michael L. Rustad & Thomas H. Koenig. The Tort of Negligent Enablement of Cybercrime, 20 BERKELEY TECH. L.J. 1553. 1557-58 (2005).

55. See Stockton & Golabek-Goldman, supra note 10, at 255; see also Fidler, supra note 34 (arguing against the Stockton and Golabek-Goldman proposal for expansion of the CFAA).

56. Stockton & Golabek-Goldman, supra note 10,at241-42. This tension results from not only different levels to which the proposals seek to regulate the market, but also from the extent to which the proposals rely on different regulatory strategies, like, for example, criminal law penalties. Id.

57. For discussion of a proposed federal regulation regarding zero-day research and the potential criminal law implications, see Andrea O'Sullivan, The Government's Latest Attempt to Stop Hackers Will Only Make Cybersecurity Worse, REASON.COM (July 28. 2015). http://reason.com/ archives/2015/07/28/gov-ploy-to-stop-hackers-will-backfire. Compare Zetter supra note 43 (discussing industry-based bounty programs), with Kelsey Annu-Essuman, An Analysis on the Regulation of Grey Market Cyber Materials, 8 CORNELL INT'L AFF. REV. 48 (2014) (discussing market based approaches like mandatory disclosure laws and "professionalization" of the grey zero-day market). See generally Stockton & Golabek-Goldman. supra note 10 (discussing various mechanisms for controlling the market, including criminal law).

58. See Stockton & Golabek-Goldman, supra note 10, at 251-64 (discussing regulations of the zero-day market through criminal law, financial incentives for companies to develop more secure software, and international trade restrictions).

59. JOSHUA DRESSLER, UNDERSTANDING CRIMINAL LAW 2 (7th ed. 2015).

60. See 18 I S C . § 1030 (2012).

61. 18 U.S.C. § 1030(a)(5)(A); see also 18 U.S.C. § 1030(c) (detailing the criminal penalties imposed under the CFAA which include incarceration for periods of up to 10 years for hacking offenses).

62. Stockton & Golabek-Goldman, supra note 10, at 261^62. The CFAA would criminalize the use of a zero-day exploit to gain unauthorized access to a computer network, but it may be difficult to apply to sellers of exploits as the marketplace is international in nature and transactions are likely to require extraterritorial application of the law and significant amounts of investigatory resources to police under a criminal law scheme. Id.

63. See Thompson, supra note 40, at 560-61 (noting that within the CFAA "the term 'protected computer" is broadly defined"' which results in "cyberspace-wide jurisdiction").

64. Press Release, Office of Pub. Affairs, Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-cliinese-niilitary-hackers-cyber-espionage-against-us-corporations-and-labor (detailing indictment brought against Chinese computer hackers in connection with cyberattacks carried out from China against LIS. corporations).

65. See United States v. Ulbricht, 31 F. Supp. 3d 540. 564-65 (S.D.N.Y. 2014) (finding sufficient evidence to support charges against man behind Silk Road dark-web market for conspiracy to commit computer hacking).

66. See Declan McC ulla gh, From "War Games' to Aaron Swart:: How U.S. Anti-Hacking Law Went Astray. CNET (Mar. 13. 2013. 4:00 AM), https://www.cnet.coni/news/froni-warganies-to-aaron-swartz-how-u-s-anti-hacking-law-went-astray/ (discussing how fears over hacking important national infrastructure and military operations, as seen in the movie War Games, has created an increasingly expansive anti-hacking criminal law since the 1980s with recent calls to further expand the reach of the CFAA); see also Statement. Office of the Press Secretary, FACT SHEET: Cybersecurity Legislative Proposal (May 12, 2011), https://obaniawhitehouse.archives.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal [https://perma.cc/ALI7H-225Y] (proposing new legislation to address concerns over attacks on "the electricity grid, financial sector, and transportation networks").

67. See: SYMANTEC, supra note 9, at 40. 47 (noting the increased frequency of zero-days aimed at ICS targets and that it should "give most people cause for concern").

68. See STGB § 202 (Ger.).

69. Id.

70. Stockton & Golabek-Goldman. supra note 10. at 243 ('The Computer Fraud and Abuse Act should be amended to impose an affirmative duty on sellers to conduct due diligence before selling [zero] day exploits that target U.S. critical infrastructure ICS and their applications layer software.").

See id. at 262.

72. See. e.g., Fidler. supra note 34. at 427-30 (arguing against the Stockton and Golabek-Goldman proposal for expansion of the CFAA).

73. See id. at 431-32.

74. See Preston & Lofton, supra note 36 (arguing that economic motives tend to drive the way that security vulnerabilities are disseminated, and that an expansion of the criminal law or civil penalties to prevent public disclosure of vulnerabilities might come at an economic cost that outweighs the benefits).

75. See. e.g., Brannon, supra note 32; Cassandra Kirsh, The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law, 41 N. KY. L. REV. 383 (2014) (proposing a "reporting" safe harbor to protect researchers from criminal liability).

76. ENGEBRETSON. supra note 38. at 2 ("It is important to note that ethical hackers complete many of the same activities with many of the same tools as malicious attackers.").

77. See Anthony, supra note 31 ("How do you craft a law that allows some research groups to keep on digging for vulnerabilities while at the same time blocking the black hats?").

78. See id. (quoting a cybersecurity professional who noted that there was a fear of disclosing discovered vulnerabilities to vendors as they frequently responded to the researcher with threats of liability under the DMCA),' see also Adam Segal. What to Do About Zero-Day Hacks? Try a Middle Road, DEF. ONE (Sept. 19. 2016). http://www.defenseone.coni/ideas/2016/09/what-do-about-zero-day-hacks-try-middle-road/131647/ ("The lack of clarity and the threat of severe punishment can prevent legitimate security research, as finding bugs often requires exceeding authorized access.").

79. See Fidler, supra note 34, at 427-29 (noting that definitional issues remain regarding what activity specifically will be criminalized under the Stockton and Golabek-Goldman proposal, and that extraterritorial application of the CFAA would be a serious issue to its implementation).

80. See. e.g.. Press Release. Office of Pub. Affairs, supra note 64 (noting that the criminal charges were brought against Chinese hackers for attacks on U.S. based companies).

81. See Preston & Lofton, supra note 36. at 96-118 (noting that liability threatens to be used as a threat by those capable of enduring the expense of litigation as a means of suppressing free speech. The author also provides a notable discussion of the history regarding computer code being regarded as protected speech.)

82. This is a position that would seem logical given the nature of the technology being regulated. Much of the literature about regulation of the zero-day market is focused on tailoring a solution that preserves at least some of the potential benefits gained from research into zero-day vulnerabilities. See. e.g., Segal, supra note 78. It would follow then that attempts at regulation should, as a general maxim, attempt to maximize the "cost/benefit" to both the governmental and societal interest.

83. See. e.g., Rustad & Koenig, supra note 54.

84. Id.

85. Id. at 1561.

86. Id. at 1557.

87. See Stockton & Golabek-Goldman, supra note 10, at 252-53 (discussing issues regarding the application of tort liability to software vendors, especially regarding the disincentive it provides to innovation).

88. See Anthony, supra note 31 ("A zero-day is a very specific tiling, and it likewise has a very specific purpose: gaining access to something without someone else finding out."); Paganini, supra note 28 ("The belief that zero-day vulnerabilities are rare is wrong. They are vulnerabilities exactly like any others with the fundamental difference that they are unknown.")

89. See Paganini, supra note 28.

90. See WRIGHTSON, supra note 22, at 12 (noting that security issues are likely to continue to develop, in part, because "[technology has developed too quickly without effective consideration for security").

91. Definitional issues present inthe application of criminal laws to regulate the zero-day market would be analogous to the difficulties in defining the standard of care for implementing civil liability based regulations. Fidler, supra note 34, at 427-29 (discussing definitional issues in use of criminal law-based regulation).

92. See Stockton & Golabek-Goldman, supra note 10, at 252 (discussing how tort liability for negligently insecure software might be similar to liability imposed on manufacturers in other industries).

93. Id. at 252 (discussing how the application of tort liability to software vendors might impede development, and recommending instead an alternative approach based on incentivizing greater investment in security for software vendors).

94. See supfa Sections II.A & II. B (discussing difficulties for imposing international regulations on zero-day market through domestic criminal or civil law).

95. Some of the most publicized calls have come from Marietje Schaake. a member of the European Parliament for the Dutch Democratic Party, who has campaigned for strict export controls and put forward a set of recommendations regarding the European Union's dual-use regulations. SeeMarietje Schaake Proposes 12 Actions to Remedy Human Rights Shortcomings in the EU's Dual Use Regulation. MARIETJE SCHAAKE (Oct. 15. 2015). https://marietjeschaake.eu/marietje-schaake-proposes-12-actions-to-remedy-human-riglits-shortcomings-in-the-eu-s-dual-use-re gulation?color= primary.

96. National Contacts, WASSENAAR ARRANGEMENT. http://www.wassenaar.org'participating-states/ (listing the participating states to the treaty) (last visited Sept. 17. 2017).

97. Home, WASSENAAR ARRANGEMENT, http://www.wassenaar.org/ (last visited Sept. 17. 2017).

98. See About Us, WASSENAAR ARRANGEMENT, http://www.wassenaar.org/about-us/ (last visited Aug. 9. 2017).

99. See, e.g., Stockton & Golabek-Goldman. supra note 10, at 243 ("Through the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, nations should develop criteria for which [zero-day] exploit sales should be authorized and which should be denied, focusing on the end-use and end-destination of such transactions.").

100. See Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items. 80 Fed. Reg. 28.853 (May 20. 2015) [hereinafter BIS Proposed Rule],

101. See Brannon. supra note 32 (noting that the BIS proposed rale "included provisions subjecting zero-day software exploits to license before they were to be exported. The proposed regulations were BIS's attempt to

implement the added provisions to the Wassenaar Arrangement (WA) in 2013").

102. See id.

103. See id. ("This process could be lengthy, and the NSA is open about its acquisition and use of zero-day exploits for its own surveillance capability.").

104. Id.'

105. See Victor Schwartz & Phil Goldberg, Carrots and Sticks: Placing Rewards as Well as Punishment in Regulatory and Tort Law, 51 HARV. J. LEGIS. 315,359 (2014) (discussing how states have enacted presumptions in some areas of tort law against liability when an actor complied with regulations as a "carrot" to incentivize compliance).

106. If the problem is one that can be regulated through civil remedies, then there is no need to rely on the more drastic criminal system. For a discussion of the potential influence regulations like civil penalties can have on a market, see generally Richard Posner, Regulation (Agencies) Versus Litigation (Courts): An Analytical Framework, in REGULATION VS. LITIGATION: PERSPECTIVES FROM ECONOMICS AND LAW 11-26 (Daniel P. Kessler ed., 2010).

107. Imposing civil liability, in an ex ante or ex post manner, can have regulatory effect on an industry based on the regulations effects on the economics within that industry. See id. (discussing liability as a regulatory tool through a law and economics perspective).

108. Stockton & Golabek-Goldman, supra note 10, at 249.

109. See Fidler, supra note 34, at 432 (discussing the issues surrounding expanding the reach of the CFAA); see also McCullagh, supra note 66.

110. See Posner, supra note 106 (discussing the interplay between regulation, litigation, and market forces on the effectiveness of regulation).

111. See Brannon, supra note 32 ("[SJoftware vendors -- so as to avoid a zero-day fueled, high-profile data breach -- rely on reports from security researchers as part of their vulnerability detection and remediation for their code.").

112. See ENGEBRETSON, supra note 38; see also Brannon, supra note 32 (highlighting the complications involved with dual-use tools like zero days).

113. Cf. Preston & Lofton, supra note 36, at 81 ("Computer security publications provide long-term benefits as vulnerabilities are corrected and better products reach the market.").

114. See Thompson, supra note 40, at 560-61.

115. See Brannon, supra note 32.

116. See Roger A. Grimes, Why It's So Hard to Prosecute Cyber Criminals, CSO (Dec. 6, 2016, 3:00 AM), http://wwwvcsoonline.com/article/3147398/data-protection/why-its-so-hard-to-prosecute-cyber-criminals.html [https ://perma. cc/LTZ4K"VVY7].

117. See SYMANTEC, supra note 9, at 5 (discussing how the rate at which new zero-day vulnerabilities are discovered has increased recently and that a growing market has emerged).

118. See 'Internet of Things' Hacking Attack Led to Widespread Outage of Popular Websites, supra note 1 (discussing the first large-scale IoT based DDOS attack carried out against Dyn in 2016).

119. See McCullagh. supra note 66.

120. DRESSLER. supra note 59. at 2.

121. This point was also persuasively argued within Fidler. supra note 34. at 431-32.

122. For a discussion of safe harbors as it relates to criminal law applications of the CFAA and gray-hat hacking, see Kirsh. supra note 75. at 400-07.

123. See KEITH WERHAN. PRINCIPLES OF ADMINISTRATIVE LAW 158-88 (2d ed. 2014) (discussing the process of rulemaking by federal administrative agencies).

124. Id.

125. See id. at 256-60. (discussing the public comment period and influence of interest groups on administrative law).

126. See, e.g.. BIS Proposed Rule, supra note 100.

127. See Brannon, supra note 32.

128. Id.

129. See Posner. supra note 106. at 22-24 (discussing the pros and cons of different regulatory schemes, and the nature of "hybrid" schemes that rely on a combination of regulations and litigation).

130. Anthony, supra note 31.

131. Because the Internet is so vast, with so many actors, and has such a potential for actors to obfuscate their activities (through various technical means) any regulation seeking to entirely eliminate certain types of transactions or behavior will likely be very difficult. A prime example of this being the rise of illegal drug sales online via dark-web marketplaces. Despite there already being a substantial infrastructure for policing illegal drag sales, the increased frequency of such sales online suggests that sellers are finding success in conducting their business online. For a discussion of this phenomenon, see Buying Drugs Online: Shedding Light on the Dark Web. ECONOMIST (July 16. 2016). http://www.economist, coni/news/international/21702176-drug-trade-moving-street-online-cryptomarkets-forced-compete [https://perma.cc/5T4M-TTVJ].

132. See Anthony, supra note 31 ("Katie Moussouris helped create Microsoft's security bounty programs and was pivotal in improving the company's approach to security research and vulnerability response.").

133. Stockton & Golabek-Goldman, supra note 10, at 249 ('The largest customers include the U.S. government and other nations" government agencies □ .").

134. See Brannon, supra note 32.

135. See Anthony, supra note 31.

136. See Segal, supra note 78 (describing calls for U.S. regulation through taking a larger portion of the market).

137. Stockton & Golabek-Goldman, supra note 10, at 257 ("Sellers with license exceptions would still be responsible for conducting due diligence and screening end-users. If they failed to do so, they would be subject to substantial administrative or criminal penalties."),

138. See id. at 256-57 (discussing licensing requirements for the international sale of zero-day technologies).

139. Id. at 262 ("[T]he CFAA should be amended to impose an affirmative duty on the seller to conduct due diligence when selling [zero] day exploits □ .").

140. See id. ("A similar affirmative duty to investigate buyers is placed on sellers in other weaponry contests, such as with handgun purchases from licensed firearm dealers.").

141. The selected agency might consider soliciting advice from industry experts during a public comment period before making changes to the guidelines. See WERHAN. supra note 123. at 256- 60.

142. See Posner. supra note 106 (discussing the burdens created by both regulation-based schemes and litigation-based schemes in regards to the pros and cons of different regulatory approaches).

DIAGRAM: Figure 1. Visualization of the Zero-Day Exploit Life Cycle[28]

~~~~~~~~

By Alek Charles Emery, J.D. Candidate. Sandra Day O'Connor College of Law at Arizona State University; B.S.. Physics. 2014. University of Utah. The author egresses his sincerest gratitude to Professor Diana Bowman and Alan Witt for all their extraordinary patience and encouragement. Also, thank you to all the authors whose work helped inspire my own.

~~~~~~~~