

2019

Cybersecurity and Patent Law - Let's Work Together

Vignesh Ramachandran

Follow this and additional works at: <https://digitalcommons.wcl.american.edu/ipbrief>



Part of the [Intellectual Property Law Commons](#), and the [Internet Law Commons](#)

Recommended Citation

Ramachandran, Vignesh (2019) "Cybersecurity and Patent Law - Let's Work Together," *Intellectual Property Brief*. Vol. 10 : Iss. 2 , Article 1.

Available at: <https://digitalcommons.wcl.american.edu/ipbrief/vol10/iss2/1>

This Article is brought to you for free and open access by the Washington College of Law Journals & Law Reviews at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in Intellectual Property Brief by an authorized editor of Digital Commons @ American University Washington College of Law. For more information, please contact kclay@wcl.american.edu.

Cybersecurity and Patent Law - Let's Work Together

CYBERSECURITY AND PATENT LAW – LET’S WORK TOGETHER

Vignesh Ramachandran*

ABSTRACT

Data has become currency. Personal data, behavioral data, financial data, location data, and more are being collected, using legal and illegal methods, and sold to the highest bidder. In some ways, we, as users, benefit: we get targeted ads, get local restaurants and points of interest suggestions. In other more significant and malicious ways, our data is being used to manipulate us or to threaten our core beliefs. The 2016 election showed Americans the extent that data collection can affect American ideologies. Irrespective of the result of the 2016 election, America now needs to evaluate how to defend itself and be proactive against a quickly developing method of disruption. To do so, America’s entrepreneurs, innovators, investors, scientists, engineers, and politicians must converge together with one goal: to become the leader in defensive cybertechnology. President Barack Obama perhaps said it best: “The Internet has brought incredible opportunity [and] incredible wealth. It gives us access to data and information that are enhancing our lives in all sorts of ways. It also means that more and more of our lives are being downloaded, being stored, and as a consequence are a lot more vulnerable. That is true for the private sector. That is true for individual Americans. That [sic] true for federal, state, and local governments. It’s true for our critical infrastructure.”¹

* Special thank you to Professor Chimène Keitner for helping develop this paper.

¹ Barack Obama, President, Remarks by the President on the Cybersecurity National Action Plan (Feb. 17, 2016) (transcript available in the National Archives and Records Administration).

Others have commented on the need to improve how our lives are being monitored and secured. Notably, in a speech at Fordham University in January 2018, Christopher Wray, the Director of the FBI said: “I’m convinced that the FBI—like a lot of other organizations—hasn’t fully gotten our arms around these new technologies and their implications for our national security and cyber security work.” He went on to discuss how cyber-attacks, like 9/11, will fundamentally transform the national security organization. A full transcript of his speech can be found here: <https://www.fbi.gov/news/speeches/raising-our-game-cyber-security-in-an-age-of-digital-transformation>.

TABLE OF CONTENTS

ABSTRACT.....	1
INTRODUCTION.....	3
I. Who is Currently Patenting Cybertechnology.....	5
II. The Problems with Getting a Cybertechnology Patent.....	6
A. Current State of Patent Law Regarding Cybertechnologies.....	6
B. The USPTO Backlog.....	8
III. Addressing the Issue.....	9
A. How to Determine if a Patent Application is Related to Cybertechnology. .	10
B. How to Implement Other Incentives.....	12
C. Sunset Clause.....	14
IV. Possible Critiques of the Proposed Solution.....	15
A. Domestic.....	15
B. International.....	16
V. Advantages of the Proposed Solution.....	17
A. Promotes Innovation.....	17
B. Pushes Innovators to Cybersecurity.....	18
C. Attributability.....	18
VI. Examples.....	19
A. Patent No. 9032521.....	19
B. Patent Application No. 15469985.....	20
C. Patent Application No. 12651649.....	20
D. Patent No. 9199242 – An Example from the GTPP.....	21
VII. Future of Cybertechnology.....	21
A. Facebook.....	22
B. Apple.....	22
C. Google.....	22
D. Microsoft.....	23
E. Amazon.....	23

F.	General Expected Cybersecurity Growth Areas.	23
VIII.	Other Possible Contributors to Incentivizing Cyber Innovation.	24
IX.	Summary of Proposal.	25
CONCLUSION.	26

INTRODUCTION

The global cybersecurity community has been on high alert over the last few years. Especially in America, where cyber-attacks have deeply impacted American beliefs in voting integrity, in the value of being “American,” and in being secure from global espionage. This heightened state of alert has prompted many actions such as the creation of a Cybersecurity National Action Plan by President Obama and the National Cyber Strategy Initiative by President Trump.²

Despite such progress, cyber-attacks continue to occur.³ Since 2014, hacking occurred at media providers such as Dailymotion, 8tracks Radio, Verizon, and Yahoo Inc.⁴ Organizations utilizing personal financial information such as Uber, PayPal, Equifax, and Dow Jones also experienced hacking.⁵ These are just a few examples of cyber-attacks that have had a large impact on the average American citizen. These attacks and several others combined cost Americans over \$1.3 billion in 2016 alone.⁶

Prevention or detection of incoming attacks such as these must be improved. However, several roadblocks stand in the way of swift innovation in the cyber-technology field. Chief among them is that innovation requires investment. Moreover, investment requires a projected profitable return on investment. Cyber technology companies have not attracted investment at the same rate as other technology companies because of the quick succession of new technologies by newer technologies and the lack of protected assets within a cyber-technology company. These characteristics, among others, are driving investors, and thereby, driving talent and brainpower away.

Thus, to hasten and incentivize innovation in technology capable of preventing, detecting, and mitigating cyber-attacks, this paper will propose new legislation. The new legislation will focus on using patent incentives to drive innovation in defensive cyber-technology.

First, this paper defines cyber-technology, cybersecurity-technology, and other synonyms as software functions and features to be provided in smart electronic devices

² Grant Schneider, *President Trump Unveils America's First Cybersecurity Strategy in 15 Years*, THE WHITE HOUSE (Sept. 20, 2018), <https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/>.

³ *See id.*

⁴ Riley Walters, *Private Sector Cyber Incidents in 2017*, Heritage Foundation Issue Brief No. 4803, 1, 4 (2018), <https://www.heritage.org/sites/default/files/2018-01/IB4803.pdf>.

In 2018, the list of victims to cyber-attacks has grown. It now includes Facebook, Panera, Sacramento Bee, Under Armour, Marriott Hotels, Orbitz, and etc. Several blogs and news outlets have been accumulating a list of attacks. An example of one can be found here:

<https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-september-2018-925633824-records-leaked>.

⁵ Walters, *supra* note 5, at 3-4.

⁶ *Id.* at 1.

(“SEDs”) to accommodate cybersecurity programs, which secure the access, operation, configuration, firmware revision, and data retrieval from a SED. External devices connected to a SED may also be a part of this ecosystem.⁷

Second, this paper defines a cyber-attack, cyber-warfare, and other synonyms as software attacks, which disrupt the manufacturer-designed functionality of the SEDs.

Third, this paper will address how patent law can provide incentives to hasten defensive cyber-technology development. This paper will build on existing patent law programs such as the Patent Prosecution Highway (“PPH”), and the Green Technology Pilot Program (“GTPP”). These existing programs provide a framework for the legislation that this paper proposes.

This paper will discuss the current state of cyber-technology; then, it will address the roadblocks confronting cyber-technology related patents. Moreover, it will address steps the United States Patent and Trademark Office (“USPTO”) has taken to clarify the current status of patent law regarding this subject. Next, it will draw parallels to GTPP and comment on how a similar program can spur innovation in cyber-technology. In the next section, this paper will address the logistics of such a program, such as identification of cyber-technology patents and providing incentives within the patent prosecution process. Lastly, this paper will address non-patent methods to incentivize innovators and how certain departments in the government can play a role.

I. WHO IS CURRENTLY PATENTING CYBERTECHNOLOGY

Five companies have become a major part of our lives over the past few years: Facebook, Amazon, Microsoft, Google, and Apple.⁸ These companies are dominant in the data collection industry. They collect data related to our daily routines, search habits, and much more making them attractive targets to hackers evidenced by the recent Facebook hack that led to the compromise of up to 90 million Facebook log-on credentials.⁹ These companies have begun filing patents in data security to combat risks. From 2013 to 2017, Microsoft has filed 170 patents, Facebook has filed 58, Google has filed 111, Apple has filed 91, and Amazon has filed 100.¹⁰

⁷ *IEEE 1686-2013 - IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities*, IEEE STANDARD ASSOCIATION, <https://standards.ieee.org/standard/1686-2013.html> (last visited Sept. 6, 2018).

IEEE is the Institute of Electrical and Electronics Engineers. Its core purpose is “to foster technological innovation and excellence for the benefit of humanity.” There are several organizations such as this. For example, ETSI — the European Telecommunications Standards Institute.

⁸ *See What Big Tech’s Patents Tell Us About The Future of Data Security*, CB INSIGHTS (Oct. 2, 2018), <https://www.cbinsights.com/research/famga-patent-data-security-innovation/>.

⁹ *Id.*

¹⁰ *Id.*

However, this illuminates one of the problems that the proposed solution is to solve: easier entry into the cybertechnology field.¹¹ It is not a surprise that the wealthiest and most successful companies can invest in research and development and have enough resources to continue through the long patent prosecution process. Smaller, yet relevant, companies such as in the financial industry (e.g., PayPal, Square, Dow Jones, etc.) or the medical industry (e.g., Affinity Health Plan, Anthem Inc., etc.) have not been able to invest drastically in patents.

II. THE PROBLEMS WITH GETTING A CYBERTECHNOLOGY PATENT

A. *Current State of Patent Law Regarding Cybertechnologies*

As an initial matter, this paper focuses on *software* cybertechnologies. This distinction is crucial to keep in mind as the case law focuses on software implementation.¹² Cybertechnology patent applications have faced increased scrutiny since the U.S. Supreme Court's decision in *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*.¹³ In

¹¹ Commentators have seen a different barrier to entry from the antitrust perspective. On the other hand, some also see this as an opportunity to grow in unison. Notably, Renata B Hesse, the Deputy Assistant Attorney General for Criminal and Civil Operations: Antitrust Division, made remarks for the Conference on Competition and IP Policy in High-Technology Industries. The goal was to merge technology with the antitrust laws that are aimed at ensuring commercial outcomes are decided in free and open markets, on the basis of superior innovation, quality, and price. The full report can be found here: <https://www.justice.gov/atr/file/517776/download>.

Others have mentioned that antitrust laws can encourage information sharing when done under the protection of antitrust laws, in accordance with recent DOJ and FTC guidance. The full report can be found here: <https://www.crowell.com/files/Industry-Collaborations-on-Cybersecurity.pdf>.

¹² Patenting software has become a challenge for many in the industry. Primarily because of the difficulty of distinguishing software from its end result and the logic used within it. For example, in a software program coded to do basic addition, assuming it is novel, is the invention the logic behind the code, the result of added numbers, or the physical lines of code? This difficulty skyrockets with complex inventions, such as cyber security — is the invention a safe digital ecosystem, the concept of privacy which is logically imputed by code, or the code itself?

Patent experts have toiled with the dilemma for years. Reputed patent blogs such as ipwatchdog have several articles regarding this dilemma. See, e.g., *Software Patents*, IPWATCHDOG (Feb. 17, 2018), <http://www.ipwatchdog.com/software-patents/>. The World Intellectual Property Organization, WIPO, has attempted to delineate considerations before filing for software patent. See Patenting Software, WORLD INTELLECTUAL PROPERTY ORGANIZATION, https://www.wipo.int/sme/en/documents/software_patents_fulltext.html (last visited Apr. 27, 2019).

Others, noting the difficulty in getting software patents, have written about how to protect your software inventions. See, e.g., Stephen Key, *How to Protect Your Software Innovation with Patents*, FORBES (June 6, 2018), <https://www.forbes.com/sites/stephenkey/2018/06/28/how-to-protect-your-software-innovation-with-patents/#184f634d4195>. Similarly, experts have provided tips for start-ups to get software patents. See, e.g., Stephen Key, *Software Startups: This is how You Craft a Patent Strategy*, FORBES (June 27, 2018), <https://www.forbes.com/sites/stephenkey/2018/06/27/software-startups-this-is-how-you-craft-a-patent-strategy/#6d7f7a3f1fee>.

¹³ See Jim Singer, *Cybersecurity Patent Strategies vs. the Growing Barriers to Software Patents*, IP SPOTLIGHT (Feb. 1, 2018), <https://ipspotlight.com/tag/cybersecurity-patents/>.

Alice, the Court stated that an “abstract idea” is not patent eligible merely by being implemented on a computer. Unfortunately, the Court did not define “abstract idea.”¹⁴ Before and since the *Alice* decision, there have been several other cases that illuminate the Court’s directionality regarding software patents.

In *Alice*, the technology was a management system for financial obligations implemented on a computer.¹⁵ To deduce whether this technology was patentable, the Court implemented a two-step inquiry process: (1) Does the subject matter of the patent fall into patent ineligible criteria (law of nature, abstract idea, and natural phenomenon); and (2) if so, is there an inventive concept sufficient to ensure that the patent, in practice, amounts to significantly more than a patent upon a patent-ineligible concept?¹⁶

The “two-step” test has become the threshold inquiry in many software-related patents and the barrier to many cyber technology patents. The Federal Circuit has incorporated this test in software patent cases since *Alice*. A few of the crucial cases are described, summarily, below.

In *Enfish, LLC v. Microsoft Corp.*, the Federal Circuit deemed the invention to be patent eligible after putting the technology through the rigors of the two-step inquiry.¹⁷ The invention was a self-referential database.¹⁸ The court justified its decision by saying that not all computer improvements are abstract ideas; the analysis must center around whether the focus of the claims is on the specific asserted improvement in computer capabilities or on a process that qualifies as an “abstract idea” for which computers are merely a tool.¹⁹

In *McRO, Inc. v. Bandai Namco Games America Inc.*, the Federal Circuit again decided that the patent application was patent eligible.²⁰ The invention was a method for synchronizing speech and facial expression of 3D animal characters through a computer program.²¹ The court justified its decision by saying that this invention was directed towards an improvement, not the entire abstract idea.²²

Although *Enfish* and *McRO* are examples where the invention was patent eligible, a significant amount of applications are rejected or face a long prosecution timeline.²³ In either case, the current system has disincentivized innovation in the area. As an

¹⁴ *Id.*; see also *Ass’n for Molecular Pathology v. Myriad*, 569 U.S. 576 (2013) (The invention had two parts: synthetic DNA and the discovery of DNA that caused breast cancer; the court permitted patenting of the synthetic DNA but not the naturally occurring DNA).

¹⁵ *Alice Corp. Pty. Ltd. v. CLS Bank Int’l*, 573 U.S. 208.

¹⁶ *Id.* at 218, 221.

¹⁷ 822 F.3d 1327, 1334, 1336 (Fed. Cir. 2016).

¹⁸ *Id.* at 1330.

¹⁹ *Id.* at 1335-36.

²⁰ 837 F.3d 1299, 1316 (Fed. Cir. 2016).

²¹ *Id.* at 1307.

²² *Id.* at 1313.

²³ See Singer, *supra* note 14.

anecdote, in the e-commerce and business method patent group (group #3600), the rejection rate has doubled from pre- to post-Alice.²⁴

To remedy the situation and perhaps shed light on patent eligibility, the USPTO released the *Berkheimer* memo as guidance on April 19, 2018.²⁵ In summary, the memo makes two crucial points: (1) a patent examiner can only conclude that an element or a combination of elements of the invention is well-understood, routine, or conventional activity when the examiner, based upon a factual determination and relying on his or her expertise in the art, can readily conclude that the elements do not amount to significantly more; and (2) an element or combination of elements is not well-understood, routine, or conventional unless the examiner finds, and expressly supports, a rejection in writing with certain evidence.²⁶

This is a departure from the status quo of examination because, according to the Manual of Patent Examiner Procedure (“MPEP”), the examiner was previously not required to make a factual or evidentiary based determination of whether an element or combination of elements were well-understood, routine, or conventional.²⁷ Therefore, this memo provides more light on how an invention can be rejected under the current status of patent law.

B. The USPTO Backlog

Another issue that all patent applicants must face is the backlog of the USPTO. Currently, there is a backlog of over 700,000 applications.²⁸ This means that an examiner does not look at an application until approximately two or three years after the filing date. In turn, a patent could be in pendency for approximately three to four years.²⁹ This prolonged process frustrates the goal of the patent system. More inventors are driven to keeping their inventions as trade secrets.³⁰ Or worse, they are not able to receive funding to continue innovation or are phased out by an upcoming technology before they are able to get patent protection.³¹

²⁴ *Id.*

²⁵ Memorandum from the U.S. Patent and Trademark Office & Robert W. Bahr on Changes in Examination Procedure Pertaining to Subject Matter Eligibility, Recent Subject Matter Eligibility Decision (*Berkheimer v. HP, Inc.*) (Apr. 19, 2018), <https://www.uspto.gov/sites/default/files/documents/memo-berkheimer-20180419.PDF>. Prior to this memo, an examiner could reject a patent based on invalid subject matter (a 101 rejection) without any support. In return, the applicant would have no argument to refute, and thus would struggle to explain away or to amend any issues.

²⁶ *See id.*

²⁷ *See id.*

²⁸ *See* Lily J. Ackerman, *Prioritization: Addressing the Patent Application Backlog at the United States Patent and Trademark Office*, 26 BERKELEY TECH. L.J. 67 (2011).

²⁹ *Id.*

³⁰ *Id.* at 68–69.

³¹ *Id.* at 69.

Due to these issues and several others, the USPTO has put in place programs such as the Petition to Make Special, Accelerated Examination, GTPP, and PPH.³²

The Petition to Make Special advances an application out of turn if the application falls into one of nine categories, such as: if the patent is related to environment quality, energy conservation, cancer or HIV/AIDS, countering terrorism, and a few others.³³ The Accelerated Examination procedure can only be used if the applicant helps the examiners by having fewer claims, claiming a single invention, interviewing with the examiner, doing a pre-examination search for prior-art, and providing a document with related prior-art.³⁴

The PPH is a partner program with several other countries that allows for sharing of prior art searches to reduce pendency and application backlog.³⁵ The results have been that examiners see the applications within two to three months of filing, and the allowance rate has been near ninety percent (non-PPH applications have approximately a fifty percent allowance rate).³⁶

The GTPP, to which this paper intends to draw a parallel, requires that an application be based on several categories such as environmental quality, energy conservation, and reduction of greenhouse gases.³⁷ As a result of this program, an application that falls into the listed categories sees a first response from the examiner within fifty days of filing.³⁸

Therefore, currently, cyber-technology related patents face two major hurdles: (1) the current status of patent law under the *Alice* regime; and (2) the backlog of the USPTO.

III. ADDRESSING THE ISSUE

The basics of the proposed solution is to have a streamlined process for patent applications that are related to cyber-technology. More specifically, the applications that are cyber-technology related could have fewer fees, more chances to interview the examiner, and more opportunities to amend.

However, complicated questions immediately arise such as (1) how does the USPTO determine if a patent application is related to cyber-technology, (2) how are the incentives going to be implemented, and (3) how long will the program run?

³² *Id.* at 71.

³³ *Id.* at 72.

³⁴ *Id.* at 73.

³⁵ *Id.* at 75.

³⁶ *Id.*

³⁷ *Id.* at 74.

³⁸ *Id.* at 74–75.

A. How to Determine If a Patent Application is Related to Cybertechnology

Under the GTPP, the applicant had to file a Petition to Make Special which forced the applicant to ensure that the application complied with the requirements and definitions of an applicable invention. If during the initial screening, the applicant was missing a requirement, the Petition to Make Special was denied.³⁹ Other procedures, such as the PPH, have similar methods to ensure compliance.

However, the proposal for a cyber-technology initiative is more complicated because, in theory, many inventions may be applicable. As mentioned before, this paper defines cyber-technology, cybersecurity technology, and other synonyms as software functions and features to be provided in SEDs to accommodate cybersecurity programs which secure the access, operation, configuration, firmware revision, and data retrieval from a SED.⁴⁰ External devices connected to a SED may also be a part of this ecosystem.⁴¹ This paper defines a cyber-attack, cyber-warfare, and other synonyms as software attacks which disrupt the manufacturer-designed functionality of the SEDs.

In order to funnel the applications, this paper proposes using definitions from Standard Setting Organizations (“SSOs”). A SSO is an entity that develops and adopts an industry standard such as a performance standard, a technical standard, or an interoperability standard.⁴² Examples of SSOs are the Institute of Electrical and Electronics Engineers (“IEEE”) and the European Telecommunications Standards Institute (“ETSI”).⁴³

The definitions provided by SSOs can serve as the criterion for a patent application to be a part of the cyber-technology initiative. For example, ETSI Standard TR 103 306 defines cybersecurity as the following: “Collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.”⁴⁴

³⁹ See Sarah M. Wong, *Environmental Initiative and the Role of the USPTO'S Green Technology Pilot Program*, 16 MARQ. INTELL. PROP. L. REV. 233, 246 (2012).

⁴⁰ See 1686-2013 – IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities, *supra* note 7, at 1.

⁴¹ *Id.* at 3–4. External devices can be any electronic device that connects to a SED via a port on the SED. For example, a memory device connected via a universal serial bus (USB) on a SED will become a part of the ecosystem.

⁴² *Standard-Setting Organization (SSO)*, THOMSON REUTERS: PRACTICAL LAW, [https://uk.practicallaw.thomsonreuters.com/9-557-1858?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&comp=pluk&bhcp=1&OWSessionId=ea195ab7b5df44b7848ea1df6667807c&skipAnonymous=true](https://uk.practicallaw.thomsonreuters.com/9-557-1858?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1&OWSessionId=ea195ab7b5df44b7848ea1df6667807c&skipAnonymous=true) (last visited Nov 11, 2018).

⁴³ *Standard Setting Organizations and Standards List*, CONSORTIUMINFO.ORG, <https://www.consortiuminfo.org/links/#.XK0ssyhKhhF> (last visited Apr 9, 2019).

⁴⁴ ETSI TECH. REPORT 103 306 V1.3.1 7 (2018), https://www.etsi.org/deliver/etsi_tr/103300_103399/103306/01.03.01_60/tr_103306v010301p.pdf.

For a step-by-step definition, TR 103 306 details cybersecurity as a continuing cycle of structured action to: (1) identify risks to systems, assets, data, and capabilities, (2) implement the appropriate safeguards, (3) implement the ability to identify a cyber-security event, (4) take action following a cyber-security event, and (5) restore impaired capabilities.⁴⁵

Another option is a compilation of SSO definitions. For example, IEEE standard 692-2013 defines the criteria for security systems for nuclear power generation stations.⁴⁶ IEEE Standard 1711-2010 defines the criteria for cryptographic protocol for cyber-security of substation serial links.⁴⁷ There are several other IEEE standards, or standards by other SSOs that may be used to form a compilation of applicable definitions.

As another example, the USPTO has classifications that categorize incoming inventions.⁴⁸ Class 726 is labeled “Information Security”.⁴⁹ Under class 726, there are several sub-classifications such as access control or authentication, protection of hardware, monitoring or scanning of software or data, prevention of unauthorized use of data, and several others.⁵⁰ These classifications by the USPTO may also be useful definitions.

However, it must be understood that these exemplary definitions are based on the current status of cyberattacks and cyber technology. As the field progresses, the definitions are liable to and should be changed to encompass applicable technologies. Logically, the burden to redefine and keep up-to-date must be placed on someone. Here, it makes most sense to leave this task up to the SSOs. This is for one major reason: uber-focused technology groups are perhaps the most motivated to and knowledgeable enough to make continuous updates.⁵¹

⁴⁵ *Id.* at 5.

⁴⁶ IEEE-SA Standards Board, IEEE Std 692-2013: IEEE Standard for Criteria for Security Systems for Nuclear Power Generating Stations (Aug. 23, 2013), <https://ieeexplore.ieee.org/servlet/opac?punumber=6613500> (last visited Nov 11, 2018).

⁴⁷ *Id.*

⁴⁸ U.S. Pat. and Trademark Office, *Patent Classification* (Apr. 2019), <https://www.uspto.gov/patents-application-process/patent-search/classification-standards-and-development>.

⁴⁹ U.S. Pat. and Trademark Office, *Class 726: Information Security* (Apr. 2019), <https://www.uspto.gov/web/patents/classification/uspc726/sched726.htm> (noting that “Classes” are different from “Standards,” standards are established by standard setting organizations who are attempting to set a standard so that there is interoperability within products; a class is a distinction made by the Patent Office to separate patent applications; this allows this patent office to send applications to the examiners that know that “Class” of technology well).

⁵⁰ *Id.*

⁵¹ See Adam Segal, *Rebuilding Trust Between Silicon Valley and Washington* 4 (Council on Foreign Relations, Council Special Rep. No. 78, Jan. 2017), https://cfrd8-files.cfr.org/sites/default/files/pdf/2017/01/CSR78_Segal_Silicon_Valley.pdf (noting the growing gap between Silicon Valley and Washington DC; the gap was perhaps publicly most evident at the Mark Zuckerberg’s trial in front a committee of senators; the full transcript can be found here:

GTPP faced a similar dilemma — whether to strictly define the field or leave it up to interpretation.⁵² Initially, GTPP defined the eligible patent applications as only those that fell into the technology class or subclass of “green technology.”⁵³ However, since numerous applications were rejected, the USPTO changed its classification to four general areas: renewable energy, technology to improve environment quality, energy conservation, or gas reduction.⁵⁴ While there are several methods to arrive at a definition, it seems clear that one definite articulation of cyber technology or cyberattack is likely not sufficient. A compilation of sub-categories will likely serve the purpose better and encompass a larger field of technologies.

B. How to Implement Other Incentives

Once a patent application qualifies for the proposed initiative, other incentives will begin to take effect. There are three categories of possible further incentives: (1) monetary, (2) time, and (3) quality of the patent.

As a monetary incentive, a qualified applicant may pay lower filing fees, processing fees, and fees to extend prosecution after a final rejection. This is similar to the GTPP and other programs. However, an added incentive could be lower fees for any related application that stems from the parent application.⁵⁵

Under the current USPTO fee schedule there are multiple categories for which the fees vary: regular, small entity, and micro entity.⁵⁶ Regular sized entities have the highest fees and micro entities have the lowest fees.⁵⁷ A regular patent application fee is broken down by its stage in the prosecution process — application, search, examination, post-allowance, extension of time, maintenance, miscellaneous, post issuance, trial and appeal, petition, and service.⁵⁸ In general, a patent applicant, from start to finish, will likely pay between \$5,000 and \$16,000 in fees to the USPTO.⁵⁹ The

https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?hpid=hp_hp-top-table-main-apple-privacy%3Ahomepage%2Fstory&hpid=hp_hp-top-table-main-apple-privacy%3Ahomepage%2Fstory&hpid=hp_hp-top-table-main-apple-privacy%3Ahomepage%2Fstory&utm_term=.9a96bfae27dc.

⁵² See Wong, *supra* note 39, at 246.

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ See MPEP § 306 (9th ed. Rev. 08.2017, Jan. 2018) (noting that every patent application, while it is still in pendency, can stem “family members” as long as the technology is initially encompassed in the parent application; for example, the first patent application filed will become the parent; a continuation, or “child” can be filed as long as the invention disclosed in the continuation is also disclosed in the parent; there are other types of dependent applications such as continuations in part, divisional, etc.).

⁵⁶ U.S. Pat. and Trademark Office, *Fee Schedule* (Mar. 21, 2019), <https://www.uspto.gov/learning-and-resources/fees-and-payment/uspto-fee-schedule>.

⁵⁷ *Id.*

⁵⁸ *Id.*

⁵⁹ *Id.* (This fee calculation may include, among others, the filing of a provisional application, a non-provisional application, search fees, and post-allowance fees).

range is large because of the various types of inventions (e.g., software, hardware, mechanical, etc.) and their varying complexities.⁶⁰ The range above excludes attorney fees, which could range between \$5,000 and \$20,000; again depending on the complexity of the invention.⁶¹

Therefore, to lower this hurdle, the proposed legislation will decrease a number of fees: the basic filing fee, fees for each independent claim beyond twenty, translation fee, search fee, and others. Another option is to match the “micro-entity” fees for applications that meet the defined criteria. In general, the reduction in fees should attract innovators that would not have been able to file a patent otherwise.

Next, a qualified application can side step the usual USPTO backlog and be placed above any other non-special track applications. Similar to the PPH and GTPP, this ensures that an application is reviewed by an examiner within 3 months of the filing date.

Lastly, the proposed initiative should allow for interviews between the applicant and examiner during the prosecution and after every rejection. Currently, an applicant is allowed an interview after the first rejection by the USPTO and by examiner discretion after a final rejection.⁶² The limited opportunities to interview the examiner takes away from the applicant’s opportunity to explain away any clarifications, ambiguities, or discrepancies. As the USPTO says, “discussion between an applicant and an examiner are often indispensable to advance the prosecution of a patent application...properly conducted, an interview can bridge the gap between an examiner and an applicant with regard to the substantive matter at issue in an application.”⁶³

By doing more interviews, the applicant can be satisfied that (1) the examiner understands the extent and limitations of the invention, (2) he or she understands the examiner’s rejection, and (3) that the patent at the end of the prosecution covers the intended scope. Therefore, applicants under this special criteria can have carte blanche for interviewing the examiner. At a minimum, the applicant and examiner must have mandatory interviews after filing and after every rejection. At a maximum, the interviews can occur whenever either party can articulate a reasonable reason to have an interview.

The USPTO is, understandably, not going to absorb the cost of providing monetary incentives to cyber-technology applicants. Therefore, there must be government intervention, as there was with the GTPP. GTPP was likely a result of President Obama’s stimulus plan that provided funding for green technology research and

⁶⁰ *Id.*; see also, Singer, *supra* note 13 (Longer prosecution times for complex patents likely leads to extension fees, trial fees, and others).

⁶¹ *How Much Does a Patent Cost: Everything You Need to Know*, UpCounsel, <https://www.upcounsel.com/how-much-does-a-patent-cost> (last visited Apr 10, 2019).

⁶² MPEP § 713 (9th ed. Rev. 08. 2017, Jan. 2018).

⁶³ *Id.*

development.⁶⁴ This was done in 2009 when the economy was still in the midst of the recession and fears of environmental decay was peaking.⁶⁵

Currently, we are in a similar situation with global tension between major world superpowers. President Trump and President Obama have addressed the seriousness of cybersecurity.⁶⁶ President Trump has enacted the National Cyber Security Strategy in 2018, one of the first fully articulated cyber strategies in the U.S. since 2003.⁶⁷ Prior to President Trump, President Obama also prioritized cybersecurity by enacting the Cybersecurity National Action Plan in 2016.⁶⁸

While it may not be as directly needed as the stimulus package was in 2009, the current state of protection is clearly a high priority amongst American citizens and the government. Therefore, in order for the USPTO to provide monetary incentive to cyber technology inventors, the federal government will have to provide more funding to the USPTO.

C. Sunset Clause

The GTPP was originally designed to run either for twelve months or until 3,000 grantable petitions were received.⁶⁹ The program would be sunset even if fewer than 3,000 grantable petitions were received after twelve months.⁷⁰ 3,000 applications was seen as a feasible amount to garner enough attention from examiners, while also serving the purpose of promoting innovation in green technology.⁷¹

For the proposed solution, a similar sunset clause can be used. Additionally, due to the transitory nature of cyber-technology, a push for immediacy should be a goal. Therefore, the applications filed earlier should receive more incentives than those filed later. For example, if the legislation is due to sunset within two years, the grantable applications filed in the first year may receive a complete reduction of fees to file, while those filed in the second year only get a partial reduction.

Another factor to consider is the maximum number of grantable applications to be accepted. The GTPP chose 3,000.⁷² In this case, the number should be based on the current backlog of the examiners in the art unit, the number of current applications that the art unit receives yearly, and how many applications an examiner reviews per day. Moreover, the number should only count the initial application, not any of the applications that derive from the original application.

⁶⁴ See Wong, *supra* note 39, at 245.

⁶⁵ *Id.*

⁶⁶ See Schneider, *supra* note 2.

⁶⁷ See *id.*

⁶⁸ Remarks by the President on the Cybersecurity National Action Plan, *supra* note 1.

⁶⁹ See Wong, *supra* note 39, at 245.

⁷⁰ *Id.*

⁷¹ *Id.* at 245–46.

⁷² *Id.* at 245.

Therefore, similar to the GTPP, a limitation of time, number, or both should be used for the proposed solution.

IV. Possible Critiques of the Proposed Solution

A. Domestic

Government action, especially monetary action, have seen vehement opposition within the U.S.⁷³ In this case, opposers may have two concrete claims: (1) monetary incentives should go directly to funding research and development; and (2) that patents on cyber security would commercialize a matter of national security.

Those that say monetary incentives should go directly to research and development may lean on existing programs such as the National Science Foundation. In 1950, President Truman created the NSF to fund basic research by U.S. colleges and universities.⁷⁴ Again, in 2009, President Obama's stimulus package provided \$2.5 billion to NSF for basic science research.⁷⁵ The purpose of NSF funding is to promote the progress of science and to advance the national health, prosperity, and welfare by supporting research and education in all fields of science and engineering.⁷⁶

Although this will address the issue at hand of developing cybersecurity, NSF targets a wide array of technologies and research organizations.⁷⁷ Companies and individual innovators, who focus on cybersecurity, need their own commercial incentives to be able to invest in and develop their technology. Patents are one way to have a profitable return on investment.

Thus, this paper argues that government funding to programs such as NSF will help mitigate the issue, but incentives such as the proposed legislation also need to be put forth. By doing so, students, employees, and companies have a reason to focus on cyber security development.

The Bayh-Doyle Act of 1980 supports this notion of government funding with commercialization in mind.⁷⁸ Under the Act, federal research grant recipients are allowed to apply for patents.⁷⁹ This was justified because, while universities and colleges are not necessarily motivated by patent monetization, a private entity requires monetary incentives to bring technology to the general public.⁸⁰ A private entity

⁷³ *Id.* at 237.

⁷⁴ *Id.* at 240.

⁷⁵ *Id.*

⁷⁶ *Building the Future: Investing in Discovery and Innovation*, NATIONAL SCIENCE FOUNDATION (2018), https://www.nsf.gov/about/performance/strategic_plan.jsp.

⁷⁷ *Id.*

⁷⁸ Wong, *supra* note 39, at 241.

⁷⁹ *Id.*

⁸⁰ See *id.*

requires a projection of a profitable return on investment to attract sufficient capital or investment to convert its research into commercially available products.⁸¹ In other words, private entities require monetary incentives. Therefore, while government funding is sufficient for some organizations, patent incentivization is one way to indicate to private entities that cybertechnology is a good investment.

The second argument against the proposed solution is intricately tied to the first. Commercialization of a matter of national security likely does not benefit the general public.⁸² Basically, are there safe guards to stop a developer of cyber security from selling to the highest bidder, irrespective of their intent? First, as discussed earlier, commercialization is a necessary risk to foster development. Second, a patent has a safeguard in place for not releasing inventions regarding national security. The USPTO, in concert with a defense agency (i.e., Department of Defense), can place a secrecy order on a patent.⁸³ Under current patent law, when notified by a defense agency that the publication or disclosure of the invention in a patent would be detrimental to national security, an order that the invention be kept secret will be issued by the Commissioner for Patents.⁸⁴ Therefore, a concern regarding disclosure to malicious actors, or a sale to the highest bidder mentality, is a necessary risk and is somewhat mitigated by existing patent law.

B. International

Within the international cyber community, issues may arise such as: (1) allies may not want to work with the U.S. against malicious actors if knowledge is not shared; and (2) allies may be concerned that they may be blocked from using patented innovations.

Currently, the U.S. is working with other countries to stem attacks from malicious actors.⁸⁵ For example, in the past five years, NATO has launched the Strategic Communications Center of Excellence and the Cooperative Cyber Defense Center of Excellence. In 2017, Finland launched the Europeans Center of Excellence for Countering Hybrid Threats.⁸⁶ With U.S. participation in such group efforts, obtaining patent protection may dissuade other countries due to the lack of openness.

This is a concern because the goal of patent law is to allow the inventor to exclude others from making, using or selling his or her invention in the granting country during

⁸¹ *Id.*

⁸² See *id.* at 242.

⁸³ 37 C.F.R. § 5.2(a) (2018); MPEP § 120 (9th ed. Rev. 08.2017, Jan. 2018) .

⁸⁴ 37 C.F.R. § 5.2(a) (2018); U.S. PATENT & TRADEMARK OFFICE, U.S. DEP'T OF COMMERCE, MANUAL OF PATENT EXAMINATION PROCEDURE § 120 (7th ed. Oct. 2015).

⁸⁵ *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, S. REP. NO. 115-21, at 4 (2018), <https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf> (last visited Nov 7, 2018).

⁸⁶ *Id.* at 68, 110–11.

the life of the patent.⁸⁷ However, as with any other property, the owner has the right to license, share, and disclose their own invention with anybody. Therefore, a contractual agreement, for example, is sufficient to protect the patent owner and to continue participation in-group efforts.

Next, a group effort would not be effective for other members if they have to pay royalty fees every time they would like to use technology that has been patented. Fortunately, as described above, a patent owner may license, share, or disclose the patent invention in any way that they see fit. Therefore, the patent owner can contractually allow another to use the patented technology under agreeable terms.

There are likely more concerns from participants in international cybersecurity efforts. However, obtaining a patent is a part of many countries' legal systems, and patented technology has continued to spread across the world. Therefore, cyber security innovations should not be different.

V. Advantages of the Proposed Solution

A. Promotes Innovation

Innovation means doing something new to improve a product, process, or service.⁸⁸ An innovation can likely be protected through patents.⁸⁹ Patents protect the interests of inventors whose technologies are truly groundbreaking and commercially successful, by ensuring that an inventor can control the commercial use of his or her invention.⁹⁰ In other words, a key advantage of patenting is a monetary return on investment to the inventor and anybody that the inventor chooses to share the patent rights with.

A patent is arguably most valuable to those companies or individuals that are seeking money, such as start-ups. One of the many hurdles a start-up has is getting its first round of funding.⁹¹ A venture capitalist assesses many factors such as where the invention fits in the marketplace, if the invention offers an advantage over current technology, if there is evidence that a business built around the technology would

⁸⁷ Joseph G. Hadzima, Jr., *The Importance of Patents: It Pays to Know Patent Rules*, BOSTON BUSINESS JOURNAL, <http://web.mit.edu/e-club/hadzima/the-importance-of-patents.html> (last visited Nov 11, 2018).

⁸⁸ *Reasons for Patenting Your Inventions*, WORLD INTELLECTUAL PROPERTY ORGANIZATION, https://www.wipo.int/sme/en/ip_business/importance/reasons.htm (last visited Nov 11, 2018).

⁸⁹ *Id.*

⁹⁰ *Id.*

⁹¹ Mario W. Cardullo, *Intellectual Property – The Basis for Venture Capital Investments*, WORLD INTELLECTUAL PROPERTY ORGANIZATION, https://www.wipo.int/sme/en/documents/venture_capital_investments_fulltext.html (last visited Nov 11, 2018).

succeed, what the possible returns might be, and so on.⁹² In general, a venture capitalist needs to be assured that the technology has a secured place within its target market.⁹³ One convincing indicator of that is strong intellectual property rights.⁹⁴ To prove this, the inventors need to show a strong patent position in terms of threats of litigation from competitors and time to market.⁹⁵ Therefore, under the proposed solution, an inventor could be fast-tracked to receiving a patent, making his or her endeavor more appealing to an investor, which in turn makes it more probable to result in further innovation and success.

Another factor that is also relevant is the right to license. A licensing agreement is a business relationship between a patent holder and another who is given authority to use the patent rights in exchange for a royalty payment.⁹⁶ This ability provides an additional source of income, increases the value of one's venture during a possible merger or acquisition, and allows an inventor to expand their business as they see fit.⁹⁷

B. Pushes Innovators to Cybersecurity

Similar to the ways that patent law incentivizes corporations, it can also be a crucial factor when innovators are deciding their next challenge. In general, an individual with patent rights has exclusive rights to the invention, a strong market position, the possibility of higher returns on investments, and the opportunity to license or sell the invention, and an increase in negotiating power.⁹⁸

Under the proposed solution, an innovator would be facing a shorter pendency window, have more access to the examiner and reduced fees. Therefore, it would make cybersecurity a promising enterprise.

C. Attributability

Under the Manual of Patent Examining Procedure ("MPEP") 605, a patent for an invention must have the inventor, members of a joint venture, assignee, or a person with sufficient proprietary interest listed in the application for the patent.⁹⁹ From an incentivization perspective, this gives credit to the inventor and allows him or her to be the face of a large accomplishment. Moreover, it allows others to know who the point

⁹² *Id.*

⁹³ *Id.*

⁹⁴ *Id.*

⁹⁵ *Id.*

⁹⁶ *Licensing of Intellectual Property Rights; a Vital Component of the Business Strategy of Your SME*, WORLD INTELLECTUAL PROPERTY ORGANIZATION, https://www.wipo.int/sme/en/ip_business/licensing/licensing.htm (last visited Nov 11, 2018).

⁹⁷ *Id.*

⁹⁸ *See id.*

⁹⁹ MPEP § 605.01 (9th ed. Jan. 2018).

of contact is if they are interested in acquiring, licensing, hiring the inventor, or just learning more about the invention. This is important to cyber technology because it promotes ease of access to the best minds in the field. A corporation or government agency that is reeling from the latest form of cyberattack may be hunting for solutions and people to help them. One way to speed up the process is to contact the prolific inventors in the field.

VI. Examples

The following are examples of how the proposed legislation could alter the current state of patent prosecution for cyber technology patents. In general, the proposed solution will lower fees, shorten pendency times, and allow for more interaction with the examiner.

A. *Patent No. 9032521*

The first example is a granted patent, which is assigned to International Business Machines (“IBM”).¹⁰⁰ This patent is titled “Adaptive cyber-security analytics” and is meant to perform adaptive cyber-security analytics including a computer-implemented method that receives a report on a network’s activity.¹⁰¹ The patent was filed on October 13th, 2010 and was granted on May 12th, 2015.¹⁰² During that period, the patent was rejected by the examiner three times, there was one interview, one extension of examination requested, an advisory action was filed, one disclosure statement, and several other document exchanges.¹⁰³

This patent shows three important factors that the proposed solution intends to remedy: (1) the delay between the filing date and the first response from the USPTO; (2) the lack of interviews between the examiner and applicant; and (3) the fee schedule.

For this application, the applicant was permitted only one interview during the pendency period.¹⁰⁴ The interview was held on December 17, 2014, after the 3rd rejection.¹⁰⁵ Notably, less than a month after the interview, on January 6th, 2015, the notice of allowance (preliminary allowance) was mailed.¹⁰⁶ This shows the positive impact an interview can have during the prosecution process.

¹⁰⁰ U.S. Patent No. 9,032,521 (filed Oct. 13, 2010).

¹⁰¹ *Id.*

¹⁰² *Id.*

¹⁰³ *Id.*

¹⁰⁴ *Id.*

¹⁰⁵ *Id.*

¹⁰⁶ U.S. Patent No. 9,032,521 (filed Oct. 13, 2010).

The first response from the USPTO was received more than a year and a half after the filing date.¹⁰⁷ This delayed pendency period highlights the impact of the USPTO backlog and lack of avenues for expedited examination. Lastly, for all the interactions with the USPTO, excluding attorney fees, the inventor must have paid the regular fees.¹⁰⁸

Under the proposed legislation, the applicant would be granted more opportunities to interview the examiner. In this case, an interview after the 1st or 2nd rejection could have expedited allowance. Next, similar to the GTPP, the target would be to get an examiner response within three months of the filing date of a grantable application. Lastly, the fee structure would be reduced as to make the fee a negligible issue for applicants of all financial statuses.

B. Patent Application No. 15469985

This is a pending patent application assigned to IBM.¹⁰⁹ It was filed on March 27, 2017.¹¹⁰ This application is titled “Unauthorized data access detection based on cyber security images.”¹¹¹ It is attempting to patent a system which detects a suspicious operation to be executed by the system.¹¹²

Unfortunately, the USPTO has yet to send its first response to the applicant (as of November 2018).¹¹³ This delay illuminates, perhaps better than the previous example, the impact of the USPTO backlog. In this case, as of the end of 2018, over a year and a half has passed since the filing date.¹¹⁴ Fortunately, IBM is a large company and likely does not feel the impact of this delay. However, a company seeking funding, such as a start-up, would be deeply impacted by this delay. The “what-ifs” are numerous, but it is clear that the delay between exchanges with the USPTO is causing more harm than good.

The proposed solution, as mentioned before, would target less than a 3-month delay between filing of a grantable application and the first response.

¹⁰⁷ *Id.*

¹⁰⁸ *Id.*

¹⁰⁹ U.S. Patent Application No. 15,469,985 (filed March 27, 2017).

¹¹⁰ *Id.*

¹¹¹ *Id.*

¹¹² *Id.*

¹¹³ U.S. Patent No. 15,469,985 (filed March 27, 2017).

¹¹⁴ *Id.*

C. Patent Application No. 12651649

This is an abandoned patent application assigned to Bank of America; it is titled “Designing Security into Software during the Development Lifecycle.”¹¹⁵ The invention is meant to provide a system that addresses all of the concerns and vulnerabilities present at the design and production levels associated with software.¹¹⁶

This application was rejected six times before it was abandoned, and the applicant had no interviews with the examiner.¹¹⁷ Nevertheless, the applicant paid to go through approximately eight years of prosecution to get a granted patent.¹¹⁸ Again, this highlights the importance of ample opportunities for interviews and for reduced fees to accommodate for prolonged prosecution.

D. Patent No. 9199242 – An Example from the GTPP

This is an example of how the GTPP impacted the prosecution of a patent. This patent is titled “Hazardous Waste Sanitation and Removal Device, Method of Use and Application Thereof.”¹¹⁹ The invention is meant to be a water treatment system.¹²⁰ This application had less than a four-year pendency period; even though it was rejected six times, there were four interviews, the first response (a Notice of Missing Parts) was filed within six days of filing, and the first rejection was issued within a year of filing of a grantable application.¹²¹ The delay between the initial filing date and the receipt of the first rejection was due to a petition and resubmission process that took six months.¹²²

This example highlights the positives of utilizing a program like the GTPP. Although there were reasons to reject this invention six times, there was continuous communication between the examiner and applicant, shorter delays, and reduced fees.¹²³ More importantly, the exchange led to an allowance.¹²⁴ Therefore, by mirroring the GTPP, the proposed solution will likely have the same positive effects on the patent prosecution process.

¹¹⁵ U.S. Patent Application Serial No. 12/651,649 (filed Jan. 4, 2010).

¹¹⁶ *Id.*

¹¹⁷ *Id.*

¹¹⁸ *Id.*

¹¹⁹ U.S. Patent No. 9,199,242 (filed Jan. 6, 2011).

¹²⁰ *Id.*

¹²¹ *Id.* Important to note here that a grantable application is one that has all the required parts. An Examiner will not review a patent application unless all parts are submitted.

¹²² *Id.*

¹²³ *Id.*

¹²⁴ Compare ‘242 Patent with ‘649 Patent Application. ‘242 is a patent using GTPP; ‘649 is a patent application that did not.

VII. Future of Cyber-Technology

The following are a few examples of what the major-impact companies are patenting in the cyber security realm. The purpose of these examples is to show that the proposed solution has an abundant market and that it will have positive impacts on the future of cyber-technology. More importantly, down the line, it will help strengthen America's cybersecurity infrastructure.

Currently, the major-impact companies are focused on filing patents related to the following areas: (1) security to share data with advertisers, (2) securing data in use, and (3) data security in the cloud.¹²⁵

A. Facebook

Facebook submitted an application in January 2018 titled, "Anonymizing User Identifiable Information."¹²⁶ This invention is meant to scramble personally identifiable information in raw datasets, which in turn would shield users from identification by third parties.¹²⁷ The goal is to no longer tie any personally identifiable information on the Facebook servers to a person's real identity, thereby making raw data obsolete.¹²⁸ By doing this, Facebook can share all their information with advertisers while being compliant with new privacy laws (i.e., GDPR).¹²⁹

B. Apple

Apple is known as the privacy leader in the industry.¹³⁰ Nevertheless, it has recently decided to delve into advertising, while keeping protection of the privacy of its user base as its highest priority.¹³¹ To do so, it has begun filing patents in the cybersecurity field.¹³² As an example, a patent titled "Repackage Media Content Data with Anonymous Identifiers" was filed in December 2017.¹³³ The goal of this invention is to allow Apple to share information with third parties without exposing identities.¹³⁴

¹²⁵ What Big Tech's Patents Tell Us About the Future of Data Security, CBINSIGHTS (Oct. 2, 2018), <https://app.cbinsights.com/research/famga-patent-data-security-innovation>.

¹²⁶ *Id.*

¹²⁷ *Id.*

¹²⁸ *Id.*

¹²⁹ *Id.*

¹³⁰ *Id.* GDPR is the General Data Protection Regulation enacted on May 25, 2018. It was enacted by the European Union.

¹³¹ *Id.*

¹³² *Id.*

¹³³ *See id.*

¹³⁴ *Id.*

C. Google

Google, a known distributor of user-information, filed a patent in May 2018 titled, “Access Control for User Related Data.”¹³⁵ This invention permits Google to exchange user-information with a third party through a secure and encrypted data exchange.¹³⁶ In general, Google is continuing to develop technology that can prove data integrity, where user data originated and can restrict who has access to the data.¹³⁷

D. Microsoft

Microsoft is seen as the leader in technology that is capable of operating on and securing data that is currently in use by another.¹³⁸ In theory, the purpose is to be able to prevent data molestation while a malicious actor is modifying, stealing, or otherwise tampering with user data.¹³⁹ Microsoft has filed patents in this field from early 2013 and has continued to do so in 2018.¹⁴⁰

Moreover, Microsoft has been patenting technology that can utilize user-specific data such as voice, handwriting, iris scans, and others without compromising security.¹⁴¹

E. Amazon

Amazon is unique because of its Amazon Web Services (“AWS”) business. Numerous third parties have entrusted Amazon with keeping their data safe. Recently, data exposure to Accenture, WWE, and others have happened on AWS servers.¹⁴² Therefore, Amazon has filed patents that allow it to offer encryption as a service to its customers.¹⁴³

¹³⁵ *Id.*

¹³⁶ *Id.*

¹³⁷ *Id.*

¹³⁸ *Id.*; Accord Kenneth Colbin, *Microsoft CEO Takes a Collaborative Approach to Cybersecurity*, CIO, <https://www.cio.com/article/3007746/cyber-attacks-espionage/microsoft-ceo-takes-a-collaborative-approach-to-cybersecurity.html> (last visited Mar. 26, 2019) (noting that Microsoft has been on the forefront of pushing collaborative cyber-defense strategies, and Microsoft CEO, Satya Nadella, has stressed that cyber-defense is best approached in an “eco-system” manner and that partnerships are critical to battling security threats).

¹³⁹ *What Big Tech’s Patents Tell Us About the Future of Data Security*, CBINSIGHTS (Oct. 2, 2018), <https://app.cbinsights.com/research/famga-patent-data-security-innovation>.

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

¹⁴² *Id.*

¹⁴³ *Id.*

F. General Expected Cybersecurity Growth Areas

Two overarching areas that are expected to grow in the cyber-attack and malware fields are software-defined security functionality and artificial intelligence (“AI”).¹⁴⁴ A software-run world requires options that can be deployed, configured, and scaled to secure data depending on the attack.¹⁴⁵ AI can increase detection and prevention efficacy, provide granular risk monitoring, and instantaneous and fine-tuned decision-making.¹⁴⁶

VIII. Other Possible Contributors to Incentivizing Cyber Innovation

While the proposed solution will likely be a factor in future cyber innovation, it cannot be the sole factor. This is a lesson to be learned from the GTPP. In the first six months of the GTPP, there were not many applications being submitted.¹⁴⁷ Even after a change in the applicability criteria, applications were not being submitted at the expected pace.¹⁴⁸ After 11 months, the program was well short of the 3,000 application limit.¹⁴⁹ Nevertheless, Congress and the USPTO felt strongly about the efficacy of and the need for the program and extended the program another year.¹⁵⁰ However, to avoid similar setbacks, there must be other factors that innovators will weigh before entering or delving further into the cyber technology industry.

Currently, commentators have had several ideas such as adding a Department of Cybersecurity.¹⁵¹ This would allow the American government to assemble the country’s best talent and resources, operate under a single agenda, develop a coherent policy, have training programs, share knowledge, and in general, act as Homeland Security does under physical attacks.¹⁵²

Another method is to increase National Science Foundation (“NSF”) funding for cybertechnology, as briefly discussed before. NSF has three goals: to expand knowledge in science, engineering and learning, to advance the capability of the nation to meet current and future goals, and to enhance NSF’s performance of its mission.¹⁵³ Allocating funds to cybertechnology would address all three goals and continue to push

¹⁴⁴ Jon Oltsik, *3 Advanced Prevention Technologies Expected To Grow In 2018*, CSO ONLINE (Dec. 08, 2017), <https://www.csoonline.com/article/3241123/security/more-on-advanced-prevention-in-2018.html>.

¹⁴⁵ *Id.*

¹⁴⁶ *Id.*

¹⁴⁷ Wong, *supra* note 39, at 246.

¹⁴⁸ *Id.* at 246, 247.

¹⁴⁹ *Id.* at 247.

¹⁵⁰ *Id.*

¹⁵¹ Ted Schlein, *The United States Needs a Department of Cybersecurity*, TECHCRUNCH (Apr. 16, 2018), <https://techcrunch.com/2018/04/16/the-united-states-needs-a-department-of-cybersecurity/>.

¹⁵² *Id.*

¹⁵³ *Building the Future: Investing in Discovery and Innovation*, *supra* note 76.

young innovators to the field. One of the key ways that NSF meets these goals is by providing funding at the collegiate level in the form of research grants.¹⁵⁴ In addition to their current methods, NSF could begin hosting cyber technology conferences for students. This would expose them to the field and show that they could contribute greatly to a growing industry.

Another factor could be the Department of Defense's ("DoD") involvement in patenting cyber technology. As briefly mentioned before, a patent may require the DoD's involvement when the technology is regarding national defense.¹⁵⁵ It even goes as far as to allow the DoD to place secrecy orders on patents.¹⁵⁶ Additionally, intellectual property rights development, acquisition, and access have each played a substantial role in allowing the DoD to use and deploy cutting edge, high-technology machines such as ships, aircraft, weaponry, and software used in America's defense.¹⁵⁷ In general, intellectual property rights have been a key resource that have provided enhanced capabilities to the DoD.¹⁵⁸ The DoD is in a unique position regarding this technology: it has unparalleled information about the level of acumen of malicious actors and the current state of America's cyber defense capabilities. Due to the DoD's history and comfort with patent rights and unique knowledge, the DoD could get more involved by recruiting interns, engineers, and other innovators for the specific task of developing patentable cyber technology in a particular niche and vulnerable area.

Therefore, while the proposed solution will improve the current status of cybertechnology, it will not do so alone. Other incentivizing factors must exist to have a meaningful impact.

IX. Summary of Proposal

The proposed solution is one factor an innovator may assess when deciding which technological field to enter. Understandably, there are many factors to balance in this decision such as money, time to research and develop, size of market, and so on. Nevertheless, ease of patenting can be a heavy factor during the balancing process. A patent offers protection against litigation, protection against copycats, increased chances of receiving funding, and increased chances of monetization. Therefore, the proposed solution intends to use patent law as an incentive to innovators to enter the cyber technology industry.

¹⁵⁴ *Id.*

¹⁵⁵ See 37 C.F.R. § 5.2(a) and MPEP § 120.

¹⁵⁶ *MPEP115-REVIEW OF APPLICATIONS FOR NATIONAL SECURITY AND PROPERTY RIGHTS ISSUES*, UNITED STATES PATENT & TRADEMARK OFFICE, <https://www.uspto.gov/web/offices/pac/mpep/s115.html> (last visited Apr 10, 2019).

¹⁵⁷ Michael Kenneth Greene, *Patent Law in Government Contracts: Does It Best Serve the Department of Defense's Mission*, 36 Pub. Cont. L.J. 331, 332 (2007).

¹⁵⁸ *Id.*

The key factors of the proposed solution are:

1. Monetary: Reduce fees such as the filing and extension fees during the patent prosecution process. It will also reduce fees for any patent that is derived from the original or parent patent.
2. Time: Speed up pendency rates by having an examiner respond within 3 months of the filing date of a grantable application. In many cases, this date is not the date that the application is submitted but the date after compliance with a notice of missing parts, submission of a disclosure statement, or remediation of other errors.
3. Quality of the Patent: Interviews between the examiner and applicant help clarify any ambiguity in the language of the patent. This allows for more of the original words of the patent to stay and not be removed due to unfounded or easily explainable rejections.
4. Period of Applicability: The proposed solution can run until one of the following occurs: a set date passes or a maximum number of grantable applications have been submitted. However, with the goal of attracting innovators now, the incentives should diminish over time or as more grantable applications are submitted.
5. Feasibility: Ideally, grantable applications come pouring into the USPTO with the start of this program. If this occurs, the examiners at the USPTO must be able to manage their increasing docket, while still responding within three months of the filing date. To do so, setting a cap on the maximum number of applications to be submitted to this program or a last date to apply allows the examiners to not be overwhelmed. Next, the USPTO will need to receive funding from the federal government to subsidize this program. Considering the status of cyber security and the vulnerability of personal data, funding is a requirement and should happen quickly.
6. Other factors: The proposed solution cannot be the only incentive in place. For example, increased education at the collegiate level through the National Science Foundation or a government push for a Department of Cyber Security would show innovators that they will receive support and resources from the government.

CONCLUSION

Cyber warfare has quickly become a threat to the privacy of our data, the integrity of American politics, the belief in what it means to be “American,” and much more. A

concerted and cohesive effort must be made to develop America's and its citizens' awareness of how cyber warfare has impacted their lives. To do so, incentives, such as ease of patenting, must be put in place to attract the best and brightest minds.