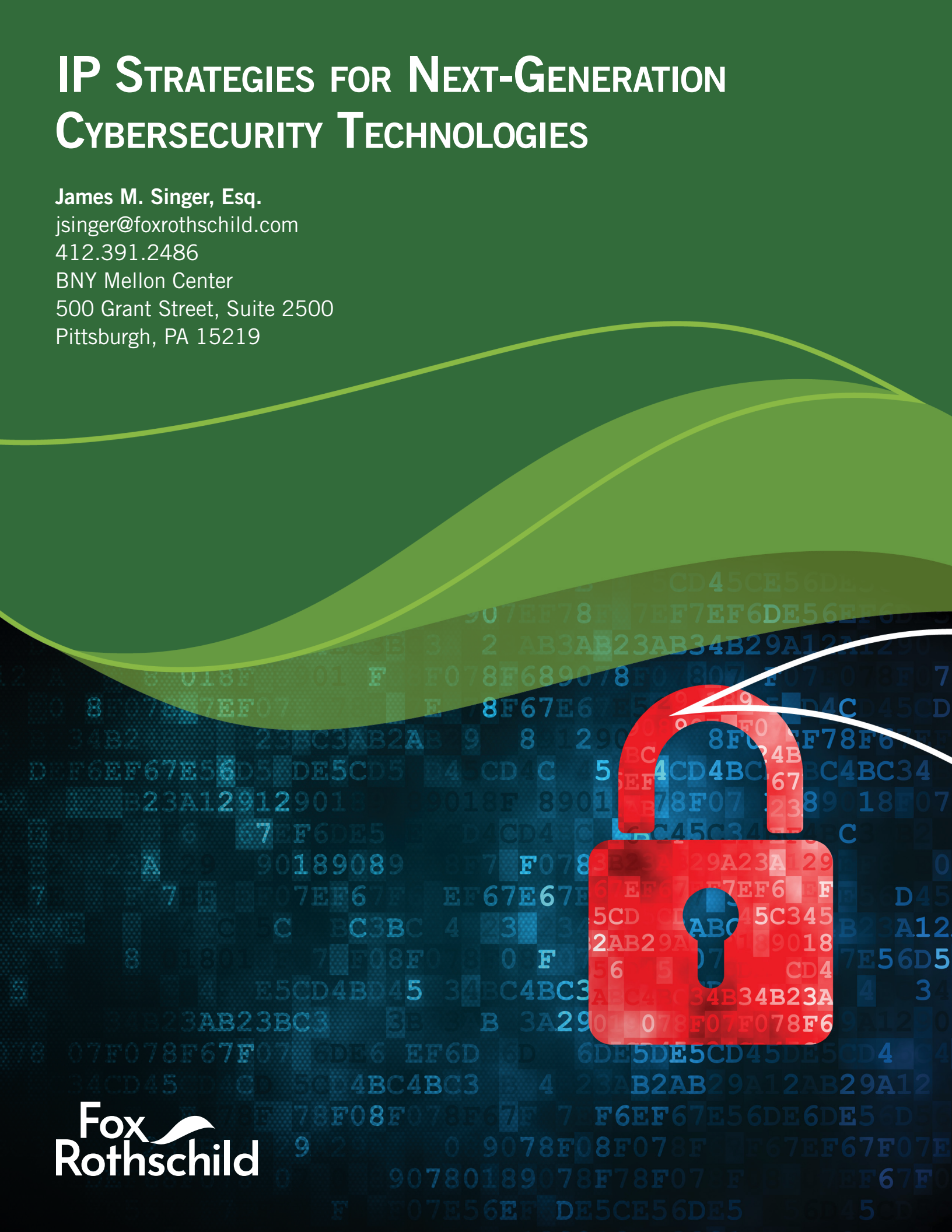
IP Strategies for Next-Generation Cybersecurity Technologies

James M. Singer, Esq.
jsinger@foxrothschild.com
412.391.2486
BNY Mellon Center
500 Grant Street, Suite 2500
Pittsburgh, PA 15219



Fox Rothschild

TABLE OF CONTENTS

Introduction

The growing cybersecurity technology industry has quickly become one of the most important industries in the world today. With products that are critical to businesses in countless fields, including finance, healthcare, transportation, public utilities, manufacturing, defense and government, experts have predicted that the global market for cybersecurity technologies will grow by 10% per year through 2020.[1]

Cybersecurity technologies are also one of the biggest drivers in corporate value today. 129-year-old Eastman Kodak Company recently saw the value of its stock jump by 200% after announcing a new service that will use blockchain technologies to help photographers get paid in a new cryptocurrency when others use their photos.[2] A New York-based beverage distributor experienced a 289% share price increase after it simply renamed itself from "Long Island Iced Tea Company" to "Long Blockchain Corp." and announced that it would start to offer blockchain technology solutions.[3]

Next-generation cybersecurity technologies include more than just blockchain-based payment systems. Distributed ledger technologies have applications in multiple fields, including document sharing, video and audio streaming, and biomedical applications. And although blockchain is all the rage at the moment, other cybersecurity technologies such as network attack simulations, network security awareness training through methods such as simulated phishing, and real-time analytics are equally important, if not more so.

[1] "Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020," *Forbes*, **Dec. 20, 2015.**

[2] **"Kodak CEO Plans to Seize Blockchain Moment and Win Over Skeptics," Bloomberg Technology, Jan. 12, 2018.**

[3] **"Long Island Iced Tea Soars After Changing Its Name to Long Blockchain," Bloomberg Technology, Dec. 21, 2017.**

Fox Rothschild

Intellectual Property Options

With this background in mind, what intellectual property protection options are available for next-generation cybersecurity technologies?

Patents

Patents cover novel processes and articles of manufacture. A patent, when granted by the applicable patent office, gives its owner the exclusive right to make, use, sell, import or export the invention.

Distributed ledger technologies such as blockchain are based on a decentralized management protocol in which all nodes of a system store copies of the complete ledger with a record of all transactions. Opportunities for patenting blockchain technologies may include:

- new applications of distributed ledger technologies;
- unique methods of creating a ledger, updating a ledger or distributing a ledger among multiple nodes; and
- unique methods for assessing integrity of one or more elements of a blockchain.

Most of the U.S. patents granted to date involving blockchain technologies cover new or improved aspects of the blockchain itself. For example, a unique way of creating and/or distributing a ledger in a cryptocurrency system may be patentable.

Only a small number of patents have granted to date for new applications of existing blockchain technologies. This may be because most companies that are using blockchain are not developing new technologies but rather are merely using existing technologies to implement different types of transactions. Innovators who want to patent new applications of blockchain technologies must focus on what new *technologies* they are bringing to the table, as patent applications seeking to merely cover new *business opportunities* with existing technologies are much less likely to succeed.

Businesses that develop other cybersecurity technologies such as network attack simulations, security awareness training, and real-time analytics also can build value with a strategic patent portfolio.

Copyrights

Copyrights cover original works of authorship, such as software code or database structures. The owner of a copyright has the exclusive right to reproduce, distribute, and create derivative works that are based on the copyrighted work.

Because distributed ledger technologies do not include centralized management, many blockchain technologies rely on an open source framework in which certain aspects of the code are open and freely available to all users. However, this does not mean that opportunities for building value through proprietary and copyrighted materials are not available. In open source platforms, many developers offer the basic elements of the platform for free to promote widespread adoption of the platform, but retain some proprietary code that the developer uses to offer value-added or premium services.

Companies that are developing cybersecurity software must ensure that all developers have signed agreements assigning all copyright in the code to the company. This is especially important if the company uses third party developers or independent contractors, as copyright is held by the author unless expressly assigned to the company.

In addition, it is important that companies who incorporate open source or third party scripts, libraries or other materials in their products obtain and retain all applicable license agreements. “Open source” typically means free, but it does not

mean "no strings attached." Most open source licenses require that users provide some type of attribution to the original author. Some open source licenses (such as the GPL and LGPL)[4] can require the user to make its proprietary code freely available to others, too. Failure to carefully review, understand, and comply with license requirements may result in copyright infringement, and it also may significantly devalue a company's code.

Trade Secrets

A trade secret is anything that provides an enterprise with value because it is secret. This can include a business process, software code that is not distributed to others, a data set or other confidential business information. Since blockchain and other distributed ledger technologies rely on an open, permissionless, public process and record, opportunities to assert trade secret protection over blockchain technologies can be limited.

However, other cybersecurity technologies can be ripe for trade secret protection. Real-time data analytics may use proprietary algorithms to yield a gold mine of data. The collector of the data may simply use that data for its own business advantage. In other situations, the data collector may license some or all of the data to others, optionally in combination with other data sets.

Before making a data set available to third parties, the data set owner must ensure that it has secured permission from all third party data suppliers to share the data. In addition, if the data set includes any personally identifiable information, financial information, or protected health information about individuals, the data set owner must comply with applicable privacy laws and regulations governing the use and disclosure of that data.

Trends in Patenting Blockchain Technologies

With the skyrocketing value of bitcoin, and the ever-increasing value created in initial currency offerings (ICOs), businesses around the world are rushing to build value with new blockchain technologies and applications. This presents many opportunities to patent innovative blockchain and other distributed ledger technologies.

This is a relatively recent trend. The first recorded appearance of the word "blockchain" in any U.S. patent or published patent application was in 2012, approximately three years after the launch of bitcoin. As of January 2018, United States Patent and Trademark Office (USPTO) records revealed:

- 25 granted patents with the term "blockchain" or "distributed ledger" in their title, abstract or claims; and
- at least 275 published patent applications include one or both of those terms in the title, abstract or claims.

When the data set is expanded to patents and applications that include the word "blockchain" *anywhere* in the text, the list grows to 56 granted patents and over 500 published applications.

Most of the granted patents cover new or improved aspects of the blockchain itself. Only a small number of U.S. patents have issued to date for new applications of existing blockchain technologies. This is likely because many companies are merely using existing blockchain technologies to implement different types of transactions.

Over half of the granted patents were examined within the USPTO's Technology Center 2400, which covers networking, multiplexing, cable and security technologies. TC 2400 includes over 200 examiners who focus on security technologies.

In each of the past three years examiners from TC 2400 have participated in a Cybersecurity Partnership meeting, in which the USPTO has interacted with stakeholders in the cybersecurity and network security sector to share ideas, experiences, and insights.[5] Information that the USPTO shared in these meetings includes:

[4] **"Licenses," GNU.org, https://www.gnu.org/licenses/licenses.html.**

[5] **"Cybersecurity Partnership Meeting," USPTO.gov, February 10, 2016, https://www.uspto.gov/about-us/events/cybersecurity-partnership-meeting.**

- The top 15 filers of patent applications for information security and cryptography technologies in each year during 2014-2016 included Amazon, Google, IBM, Intel, Microsoft, Qualcomm, Samsung, Symantec, and Tencent. Top filers in 2015 and 2016 also included Bank of America, Cisco, and EMC.
- While the vast majority of U.S. patent applications for information security and cryptography technologies have been filed by U.S. companies, the USPTO has also received a significant number of filings from companies that are based in Japan, China, Korea, Germany, France and Israel, among other countries.
- The average pendency (time between filing and either grant or abandonment) of patent applications for information security and cryptography technologies was approximately 27 months in 2016.

Globally, as of January 2018 World Intellectual Property Office (WIPO) records show 197 published Patent Cooperation (PCT) applications with the term "blockchain" or "distributed ledger" in their title, abstract or claims. However, relatively few of these PCT applications have reached the national stage. The European Patent Office database includes only 21 such patents and published applications. According to a recent report from Clarivate Analytics, in 2016 China experienced significant growth in new patent filings for blockchain technologies and is second only to the U.S. for new filings involving blockchain technologies.[6]

Defensive Patent Strategies for Blockchain and Distributed Ledger Technologies

The U.S. blockchain and distributed ledger technology patents that issued to date have been awarded to a variety of entities. Some of the patents were awarded to cryptocurrency startups that launched or are about to launch initial currency offerings (ICOs). Others were awarded to U.S. software and business services industry titans who already have large patent portfolios. Approximately one-third of the patents were awarded to businesses that appear – at least for now – to be non-practicing entities, which could signal a risk of patent litigation on the near horizon.

A strategically developed patent portfolio can have several benefits. In addition to increasing corporate value and providing a tool to prevent infringement, patents can serve as a defensive mechanism against high-stakes patent litigation. A competitor who holds patents may hesitate before filing a patent infringement suit against a company that owns a strong patent portfolio that it can assert in a counterclaim. Strong patent portfolios also can provide companies with the opportunity for favorable cross-licensing arrangements, with fewer royalties being paid and potentially more royalties coming in.

Patent applicants must consider how to draft effective patent applications. Tips for doing this include:

- Distributed ledger technologies typically require actions by multiple entities. However, it can be difficult to establish infringement of a patent claim unless all elements of the claim are used or performed by a single entity. Patent applications should draft claims with a single infringer in mind, rather than to a distributed system.
- The U.S. and many other countries around the world take a negative view of software patents that cover mere "abstract ideas" rather than innovations in technology. A new business application of an existing blockchain technology is unlikely to be patentable. Instead, patent applications should cover innovations that provide *a technical* solution to a *technical* problem.

[6] **Henry Chiu, "An Overview of the Blockchain Patent Landscape," Clarivate.com, https://clarivate.com/blog/overview-blockchain-patent-landscape/**

Patents strategies for distributed technologies also need to consider the tension between the limited monopoly that a patent provides and the open source platform that a distributed ledger necessarily requires.

For the last few years, several companies have openly discussed and favored the idea of a blockchain "patent pool" in which stakeholders share access to each others' blockchain-related patents. The Blockchain Patent Sharing Alliance (BPSA) is one such entity that is trying to gather a critical mass of stakeholders and companies.[7] In addition, in 2016, the Linux Foundation formed the Hyperledger Project, which seeks to create an open-source framework for distributed ledger technologies.[8]

Some stakeholders are taking matters into their own hands. In 2016 blockchain developer Blockstream publicly pledged that it will never use its blockchain patents as a weapon. Instead, Blockstream pledged that all of its blockchain software patents are available under the terms of a defensive patent license.[9] Under that license, Blockstream will only use its patents for "defensive purposes" against a party who brings or threatens a patent infringement claim against Blockstream or against a user of Blockstream's technologies.

Cybersecurity Patent Strategies vs. Growing Barriersto Software Patents

The USPTO's Technology Center 2400, which covers networking, multiplexing, cable and security technologies, includes over 200 Patent Examiners who focus on security technologies. TC 2400 issued over 33,000 patents in 2017. During this period, the USPTO's overall allowance rate was 59.4%.[10]

Despite this apparent boom, patent applications covering cybersecurity technologies have faced increasing scrutiny since the June 2014 U.S. Supreme Court decision in *Alice Corporation Pty Ltd. v. CLS Bank Int'l*.[11] In *Alice*, the Court found that a software implementation of an escrow arrangement was not eligible for patenting in the U.S. because it merely involved implementing an "abstract idea" on a computer. The Court did not define the term "abstract idea" other than to describe it as a building block of human ingenuity, or a fundamental concept, including concepts that involve a "fundamental economic practice."

Since then, the USPTO has issued several guidance documents, and lower courts have issued several opinions, describing when software is and (more often) is not eligible for patenting under Section 101 of the Patent Act. The USPTO typically denies, and courts often strike down, patent applications and patents covering methods of manipulating data, completing financial transactions, and algorithms that do not require any particular hardware other than a general-purpose computer. As of late 2017 over 90% of patent applications reviewed within the USPTO's business methods examining unit (which is within Technology Center 3600) received a Section 101 rejection on first action.[12] The allowance rate in TC 3600 remains far below that of the USPTO's overall statistics.

Claim Drafting Strategies

Despite the challenges that software patent applications currently face, the USPTO continues to grant, and courts continue to uphold, patents for innovations in cybersecurity technologies. To help improve a patent application's chances of success, both before a court and if challenged, patent applicants should consider some or all of the following:

[7] **Blockchain Patent Sharing Alliance,** http://www.bpsa.io/

[8] **Hyperledger Project,** http://hyperledger.org/

[9] **"Blockstream's Defensive Patent Strategy,"** https://blockstream.com/about/patent_pledge/

[10] **USPTO** *Performance and Accountability Report*, **FY2017.**

[11] **573 U.S. __, 134 S. Ct. 2347 (2014).**

[12] **Bilkisblog,** http://www.bilskiblog.com/blog/business-methods/#_edn6

- *Technical problem / technical solution*: The patent application's narrative should not focus on the business problem that the invention solves (such as allowing a financial transaction to be completed). Instead, the narrative should focus on the technical problem, as well as the technical solution that the problem solves. Examples of technical solutions include inventions that improve network security, that reduce bandwidth or data storage needs, that improve processing speed, or that help defend against cyberattacks, bots and other malicious systems.

- *Hardware:* Patent applications that claim unique hardware configurations, rather than a general purpose computer, may have a better chance of success.

- *Improvements to the underlying technology*: Patent applications may have a higher chance of success if they expressly claim features that could only happen with blockchain technologies or distributed networks, and which could not occur in the abstract or be implemented by humans alone. While this may end up with a narrower claim, the claim can be more likely to withstand challenges.

Procedural Strategies

A common feature of many of the patents granted on blockchain technologies is that the applicant sought expedited review under the USPTO's Track One prioritized examination program. Under this program, for an additional fee of $4000 (less for small entities), the USPTO will issue a final determination (allowance or final rejection) within twelve months. This typically means that the USPTO will issue a first action in less than four months. Although USPTO statistics indicate that the allowance rate is just under 50% for cases in Track One,[13] anecdotal evidence indicates that USPTO Examiners are often more willing to work with the applicant to find allowable subject matter early in prosecution.

[12] **Bilkisblog,** http://www.bilskiblog.com/blog/business-methods/#_edn6

[13] **"Data Visualization Center," USPTO.gov,** https://www.uspto.gov/corda/dashboards/patents/main.dashxml?CTNAVID=1007

Fox Rothschild

In addition, cases that are allowed under Track One receive an allowance within an average of six months after filing. An early allowance in the U.S. can help applicants implement a cost-effective global filing strategy in counties that offer a "Patent Prosecution Highway" (PPH) program with the U.S. A common feature of PPH programs is that if a patent application is allowed in one participating country, other countries' patent offices will more quickly review the application -- and often will allow it -- based on the allowance in one participating country. Using PPH treatment, cases allowed in the U.S. often can quickly receive allowance in other PPH-participating jurisdictions such as Australia, Israel, South Korea, China, and the United Kingdom.

Another strategy for getting early allowance of a patent application directed to cybersecurity technologies is to request an interview with the USPTO Examiner prior to first action. The USPTO's First Action Interview Pilot gives applicants a chance to discuss the patent application with the Examiner before the Examiner issues a first formal Office Action.[14] As of January 2018 USPTO statistics indicate that over 29% of cases in the First Action Interview Pilot had at least some claims allowed on first action, while only 13.4% of standard cases had claims allowed on first action.[15]

James M. Singer, Esq.
412.391.2486
jsinger@foxrothschild.com

[14] **"First Action Interview Pilot Program," USPTO.gov,**
https://www.uspto.gov/patents-application-process/applying-online/full-first-action-interview-pilot-program

[15] **"Data Visualization Center," USPTO.gov,**
https://www.uspto.gov/corda/dashboards/patents/main.dashxml?CTNAVID=1007

Fox Rothschild