IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

WETRO LAN, LLC,

Plaintiff,

vs.

EMERSON ELECTRIC CO.,

Defendant.

Case No: 2:15-CV-414-RWS-RSP

JURY TRIAL DEMAND

DEFENDANT'S COMBINED MOTION AND MEMORANDUM TO DISMISS PURSUANT TO RULE 12(b)(6) DUE TO INVALIDITY BECAUSE THE '918 PATENT CLAIMS INELIGIBLE SUBJECT MATTER IN VIOLATION OF TITLE 35 U.S.C. §101

Respectfully submitted,

Michael Smith

By: ______________________________
Michael C. Smith
State Bar Card No. 18650410
Siebman, Burg, Phillips & Smith LLP
113 East Austin Street
Marshall, TX 75670
903.938.8900
Email: michaelsmith@siebman.com

and

Rudolph A. Telscher, Jr.*
Email: rtelscher@hdp.com
Steven E. Holtshouser*
Email: sholtshouser@hdp.com
HARNESS, DICKEY & PIERCE, P.L.C.
7700 Bonhomme, Suite 400
St. Louis, MO 63105
Telephone: 314-726-7500
Facsimile: 314-726-7501
**Pro Hac Vice Pending*

Attorneys for Defendant Emerson Electric Co.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INDEX OF EXHIBITS

A. U.S. Patent No. 6,795,918

B. Newsweek cover, “Cyberpower: The Russian Hackers Are Coming”, May 15, 2015, *http://www.newsweek.com/2015/05/15/issue.html*

C. Assignment of ‘918 Patent to Wetro Lan recorded January 22, 2015

D. Assignment agreement re ‘918 Patent signed January 10, 2015

E. Dkt. 12-2, Declaration Of Anthony Wang Re: Wetro Lan LLC’s Response To TP-Link USA Corporation’s Motion To Transfer Venue Pursuant To 28 USC § 1404(a), *Wetro Lan LLC v. TP-Link USA Corp.*, No. 2:15-cv-105 (W.D. Tex. Apr. 20 2015)

F. History of Keys and Locks

G. Historical Locks – Definition of Keys

H. Historical Locks – Padlocks

I. Wikipedia – Pin tumbler locks

J. Historical Locks – Other locks

K. History of Safes and Bank Vaults

L. History of Padlocks – Who invented padlocks?

M. History of Locks – Who invented locks?

N. History of Keys – Who Invented Keys?

O. Cipher Machines: The History and Technology of the Enigma Cipher Machine

P. Excerpt from “Solving The Enigma: History of the Cryptanalytic Bombe”, by Jennifer Wilcox, Center for Cryptoanalytic History, National Security Agency (2006)

Q. “Password Security: A Case History”, by R. Morris and K. Thompson, Bell Laboratories (1979)

R. “A History and Survey of Network Firewalls”, by K. Ingham and S. Forrest, University of New Mexico Computer Science Department Technical Report (2002)

S. Speakeasy Cards: A Prohibition-Era Ticket to Drink

T. Speakeasy

U. Prohibition and Speakeasies

V. “Firewalls”, by Dr. Talal Alkharobi, 5-29-07

W. “Packet filtering”, California State University, Dominguez Hills, http://www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=2&ved=0CCYQFjAB&url=http%3A%2F%2Fwww.csudh.edu%2Feyadat%2Fclasses%2FCIS478%2Fhandouts%2FFall08%2FPacket%2520Filtering.ppt&ei=INRXVZLNL4nHsAWVwYGoBg&usg=AFQjCNGLlHFLc8iUNvfL57h1RSRrgu5QHQ&sig2=kKgMRug_rB8MV-fV0By3TA&bvm=bv.93564037,d.b2w

X. Wikipedia – Proxy Server

Y. Wikipedia – Personal Firewall

Z. Wikipedia – Application Firewall

AA. Wikipedia – Router (computing)

BB. Wikipedia – Firewall (computing)

CC. U.S. Patent No. 5,802,320

DD. Building Internet Firewalls Chapter 6: Packet Filtering

EE. Open BSD – PF:Packet Filtering

FF. *THE AMERICAN HERITAGE COLLEGE DICTIONARY* (3d ed. 1997), definitions of “firewall” and “sentry”

STATEMENT OF THE ISSUES

1. Whether the complaint in this case fails to state a claim on which relief can be granted, because the asserted '918 patent is invalid as a matter of law under Title 35, United States Code, Section 101, as interpreted by the Supreme Court in, for example, *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014)?

   a. Whether the '918 patent is directed to the abstract idea of securing communication access to a computer network?

   b. Whether the elements of the '918 patent provide an "inventive concept" that is "significantly more" than the foregoing abstract idea where the recited steps are merely directed to generic computer hardware and software and offer no technological advance?

I. INTRODUCTION

The asserted patent claims are patent-ineligible as a matter of law under 35 U.S.C. § 101 of the Patent Act. The Supreme Court's decision in *Alice Corp. Pty. Ltd. v. CLS Bank Int'l* controls here. 134 S. Ct. 2347 (2014).

U.S. Patent No. 6,795,918 ("the '918 Patent") is directed to computer security - authorizing or denying access to senders of communications from a public network, such as the Internet, to a private network, such as that used with home and small business computers. *See*, Ex. A ('918 Patent). Security has been a fundamental human need since the dawn of civilization and the realization that some humans are bent on doing evil. Methods to prevent unauthorized entry into any secured space are equally ubiquitous. While no one foresaw "hackers" when the Internet became a reality, it was not long before the identical need for security of communications was well known in the computer realm.

The '918 patent on its face is directed to nothing more than the abstract concept of securing a home or small business computer network from unauthorized access. Ex. A., Col. 1, ll. 28-29, Col. 2, ll. 25-26, 51-52, 60-62, Col. 3, ll. 6-8. Yet, Wetro sued fifty-five defendants and products not directed to this market, based on the vague and abstract nature of the patent. The '918 patent claims a combination of generically recited computer hardware and software to apply undisclosed but pre-set rules (a "decision block" or "look-up table") for access to information contained in incoming communications. Without contributing an inventive concept or an improvement to computer technology, the '918 patent amounts to little more than a directive to secure access by using generic computer technology to perform the most basic function–

comparing addressing/protocol data to a look-up table/rules to see if a communication should or should not be allowed.

Historical examples of the fundamental nature of securing access in human activities include the use of sentries by the Roman Legions, castles and moats, the Great Wall of China, physical locks, passwords, coded military communications, Personal Identification Numbers, and bank safes. Human-implemented and mechanized methods date back thousands of years. Similarly, the application of the fundamental idea of securing access has been vigorously applied to the field of computers for decades, because hackers pose a serious threat.

Steven Trolan, the inventor on the ‘918 patent, did not invent: a computer for preventing cyber-attacks; more secure data packets; more secure Internet communications; specific rules for more effectively filtering data packets; or improved firewalls which apply rules to filter data packets. The patent and asserted claims are not directed to any improved method, improved hardware or improved software for securing a computer from unauthorized access. Instead, the abandoned and now expired ‘918 patent claims only the most basic, general steps of securing access: (1) receive and extract data coming into a computer, specifically source, destination and protocol data; (2) comparing said data against pre-set rules for granting/denying access; and (3) granting or denying access based on the outcome of the comparison. The ‘918 patent claims these basic, abstract steps and implements them with **any** generic computer and ***any*** generic software to detect ***any*** authorized or unauthorized access requests to the computer.

The invention had so little value that Mr. Trolan abandoned the patent in 2012 by intentionally not paying his renewal maintenance fee. Wetro, nonetheless, purchased the patent to sue and did sue companies like defendant for nuisance value sums for the years 2010 (the statutory time limit on past damages) to 2012 (the year of abandonment), knowing very well that what's at stake pales in comparison to the cost to defend. Worse yet, the simple '918 patent firewall technology that might be suitable for the home or small business user to which the patent is directed, would never be used to secure sophisticated industrial control networks from intrusion. Moreover, the accused product is an added feature to a sophisticated, unrelated product, and is used only to protect an inner layer of a network rather than the layer exposed to a public network.

Alice and Section 101 are themselves a filtering mechanism for bad patents and lawsuits relying on bad patents. They empower this Court to act as a gatekeeper, just like *Daubert*, to secure the public and litigants, like Emerson and the other fifty-four defendants, from having to pay the cost of defending against patents that attempt to foreclose broad areas of technology by advancing non-specific, abstract concepts. Rule 12(b)(6) is the device that empowers this Court to block access to the courts for such patent suits.

If these claims are allowed to stand, an actual innovator, such as Emerson, developing real improvements in this area, would be foreclosed from developing practically any computer firewall, router hardware or software securing access by means of data packet filtering. The risk of disproportionate preemption here is intolerable, especially at time[1] when cyber-security is a critical mission for every entity. The volume and diversity of defendants and products in the cases filed by Wetro, all purportedly

[1] The May 15, 2015 cover of Newsweek Magazine proclaimed: "Cyberpower: The Russian Hackers Are Coming!", http://www.newsweek.com/2015/05/15/issue.html. *See*, Ex. B.

covered by the ‘918 patent, is clear evidence of the disproportionate preemptive power of permitting enforcement of the ‘918 patent. The Supreme Court noted this very dynamic in holding that patents directed to broadly-worded, theoretical, speculative, abstract concepts are not patentable without significantly advancing technological progress. *Alice*, 134 S. Ct. at 2354-55 (allowing patent protection for broad, abstract concepts risks disproportionately tying up the use of the underlying ideas).

Since the *Alice* decision, many courts have followed the Supreme Court’s directive to invalidate abstract patents that do not **proportionately** advance the technological arts. Such patents serve only to provide material roadblocks to the companies that are truly developing specific, usable technology in the area. Defendant’s post-*Alice* review indicates that the Federal Circuit has affirmed invalidity findings in all but one decision. District Court challenges produce a similarly high rate of invalidity. By now, the application of *Alice* and the abstract idea exception to patentability under §101 has become routine for patents of this nature. A finding of unpatentability in this case is not a close question and Emerson is entitled to dismissal under Rule 12(b)(6) based on this threshold inquiry.

II. FACTS

A. Introduction

Although not necessary to resolution of the motion, the background facts of the dispute are set forth for context. The Court need only apply the Supreme Court’s jurisprudence, especially *Alice,* to claims of the ‘918 patent. This legal inquiry is so non-fact dependent that many district courts have invalidated abstract patents at the pleading stage. *See, e.g., Tuxis Techs., LLC v. Amazon.com, Inc.*, No. 13-1771-RGA, 2015 WL 1387815 (D. Del. March 25, 2015) (Rule 12(b)(6) motion to dismiss granted under

Section 101 for patent claiming upselling in electronic remote commerce systems); *Clear with Computers, LLC* v. *Altec Inds., Inc.*, No. 6:14-cv-79, 2015 WL 993392 (E.D. Tex. March 3, 2015) (same for patent claiming computer-implemented customized sales presentation); *Cogent Med., Inc. v. Elsevier Inc.*, No. C-13-4479-RMW, 2014 WL 4966326 (N.D. Cal. Sept. 30, 2014) (same for patent claiming maintenance and searching of medical updates database).

B. Background Facts

Plaintiff Wetro, Inc. ("Wetro") is the owner of U.S. Patent No. 6,795,918 ("the '918 Patent"). Wetro makes and sells nothing. Its owner claims to be an "internet marketer", but Emerson was unable to locate a website for "Wetro Lan", "Wetro Lan LLC", or "Wetro". *See,* Ex. E (Dkt. 12-2, Declaration Of Anthony Wang Re: Wetro Lan LLC's Response To TP-Link USA Corporation's Motion To Transfer Venue Pursuant To 28 USC § 1404(a), *Wetro Lan LLC v. TP-Link USA Corp.*, No. 2:15-cv-105 (W.D. Tex. Apr. 20 2015). Wetro did not exist before December, 2014 and did not own the expired patent until January 10, 2015. *See*, Ex. C (Assignment of '918 Patent to Wetro Lan recorded January 22, 2015); and D (Assignment agreement re '918 Patent signed January 10, 2015).

Emerson[2], on the other hand, was founded in 1890 and sits at the head of a global industrial enterprise whose divisions and subsidiaries collectively design, manufacture

[2] Emerson is a Missouri corporation with its headquarters in St. Louis, Missouri, and does not even make or sell the accused product in this case. Emerson is a distinct legal entity, several entities and subsidiaries removed, from the actual entity which sells the accused product. That entity is a Delaware limited liability limited partnership, Emerson Process Management, LLLP, ("Emerson Process"), with its principal place of business in Round Rock, Texas in the Austin Division of the Western District of Texas. To have found the accused product on the Internet, plaintiff Wetro's counsel had to have also found that the source of the accused product was Emerson Process, in Round Rock, Texas and not

and distribute innovative solutions to technical problems in a wide variety of fields. A distant subsidiary of Emerson, Emerson Process Management, LLLP ("Emerson Process"), located in Round Rock, Texas, markets a successful computer hardware and software system, the DeltaV, for monitoring and controlling various types of industrial processes, particularly liquid or chemical processes. Emerson Process, and the business unit of which it is a part, for decades has been a market leader for such products. Wetro accuses a small part of the DeltaV system, the "Controller Firewall", of infringing its recently acquired and expired '918 patent. The DeltaV product line was introduced in 1995 as a replacement for its prior PROVOX product, which had been on the market since the 1980s.

C. The '918 Patent

The '918 Patent covers "Service Level Computer Security" and has an issue date of September 21, 2004. *See* Ex. A. The Abstract of the patent describes "[n]ovel apparatus and methods for filtering data packets by providing non-user configurable authorization data. The invention provides an efficient, quick, secure, and simple to implement technique for computer communication security, in part, by utilizing service level filtering of data packets." Ex. A., Abstract. The "Background of the Invention" ties the invention to the broad concept of securing a computer connected to a network from unauthorized access. *Id*. at Col. 1, ll. 15-18. *See also, id*. at Col. 1, ll. 22 ("access"), 25

Emerson Electric Co. in St. Louis, Missouri. Emerson Process, has filed a claim in the Western District of Texas, Austin Division, seeking declaratory judgment that Emerson Process M's DeltaV Controller Firewall does not infringe any valid claim of the '918 patent. Regardless, Emerson Electric Co., the defendant in the case at bar, seeks dismissal of this case under Rule 12(b)(6), because the '918 patent claims unpatentable subject matter as a matter of law.

(“access”). *See also, id*. at Col. 6, l. 9 (“authorized to pass through”); Col. 7, l. 61 (“allowed to pass through”).

The Background further identifies the focus of the patent to be preventing so-called “hackers” from “breaking into home and small office computers” connected to a network such as the Internet. Ex. A., Col. 1, ll. 14-17, 29. Notably, the accused product, which is configurable, sits *behind* a highly configurable and robust firewall, called the Smart Firewall, and could not function as a first-line firewall for the industrial networking control it protects. Thus, very few accused products have been sold to date.

The patent itself noted that firewalls used by industry and large companies were “impractical and too complex”, expensive, excessive, imperfect and not suitable for home or small business users. The Background concludes that “what is needed is a simple to implement, inexpensive, relatively fast, efficient, and non-user configurable solution for a computer user at home, on the road, or in a small office, to be able to protect itself from computer hackers. Col. 3, ll. 4-8.

Independent Claim 1 is representative[3] of the claims of the ‘918 patent and it states, *in toto*:

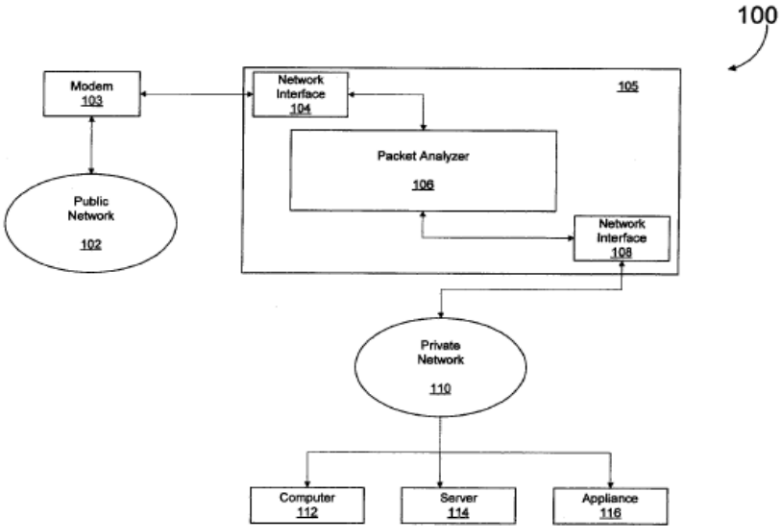
> A method for filtering a plurality of data packets, the method comprising:
>
> receiving a data packet from the plurality of the data packets, the received data packet having source, destination, and protocol information;
>
> extracting the source, destination, and protocol information

[3] The Federal Circuit has approved analysis of Section 101 issues by evaluation of a representative claim. A claim is considered representative of all claims if “all the claims are substantially similar and linked to the same abstract idea.” *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat’l Ass’n,* 776 F.3d 1343, 1348 (Fed. Cir. 2014) (internal citations omitted). *See also, Alice Corp.*, 134 S.Ct. at 2359 (“representative claim”); *Hewlett Packard Co. v. ServiceNow, Inc.*, No. 14-cv-00570-BLF, 2015 WL 1133244, at *3 & App. A, n.5 (N.D. Cal. March 10, 2015) (same).

> from the received data packet;
> providing the extracted information to a non-user configurable decision block, the decision block including information on which services are authorized depending on the extracted information, the non-configurable decision block being substantially free from user adjustment;
> dropping the received data packet if the extracted information indicates a request for access to an unauthorized service; and
> permitting the received data packet to go through if the extracted information indicates a request for access to as authorized service,
> wherein the protocol information includes information about transport types.

Other claims, including independent claims 10, 21, 25 and 26, describe the invention in other combinations of patent-ese, but generally describe the same invention as that described in Claim 1. The common methodology is analysis of data packets coming into a computer for three categories of specific content: 1) source; 2) destination; and 3) protocol information. The extracted information is then compared to non-configurable authorized combinations of said information in either a "decision block" or a "lookup table." If the data packet content of the incoming communication is among authorized combinations, the communication is granted access; if not, it is dropped or prevented from gaining access to the secured computer.

The elements of the claims, which relate to any computer on any network receiving any communications from any other network connected by almost any means, are generically described at the highest level of generality. *See*, Ex. A, Description of the Specific Embodiments. *See also*, Ex. A, Col. 7, ll. 51-52 ("protocol, source port, and destination port information"), Col. 3, ll. 28 and 50 ("decision block" and "lookup table”). For example, Figure 1 illustrates the components of the computer security system claimed by the ‘918 patent, as follows:



The ‘918 patent does not claim any new or improved hardware or software or provide any specific content of any non-configurable “decision blocks” or “lookup table[s]”.

III. LEGAL PRINCIPLES

A. Motion to Dismiss For Failure to State a Claim

The legal principles applicable to a motion brought under Rule 12(b)(6) of the Federal Rules of Civil Procedure were recently set forth by Judge Gilstrap of this District in *Clear with Computers*, 2015 WL 993392, at *3. In *Clear with Computers,* Judge Gilstrap granted a Rule 12(b)(6) motion asserting invalidity of the asserted patent under Section 101. Judge Gilstrap concluded that such an issue was properly resolved **at the pleading stage**, because “patentable subject matter presents a question of law” and the Federal Circuit’s leading post-*Alice* decision was itself an appeal from a dismissal under Rule 12(b)(6) that found that the patent claimed ineligible subject matter. *Id*. (citing *Ultramercial, Inc. v. Hulu, LLC,* 772 F.3d 709, 717 (Fed. Cir. 2014)).

Judge Gilstrap recognized the policy behind handling Section 101 issues at the outset, when he stated: “Furthermore, the Court sees no reason to delay its §101 ruling while the parties continue to expend significant resources which will not impact or aid the Court in reaching this decision.” *Clear with Computers*, 2015 WL 993392, at *3. This rationale is particularly important in this case where the patent was long ago abandoned and the potential damages are extremely low.

The Supreme Court and the Federal Circuit strongly support resolution of Section 101 issues at the outset of a case. *Alice* itself was an appeal from a dismissal under Rule 12(b)(6). *See also, Ultramercial,* 772 F.3d at 717 (Section 101 is a “threshold question, one that must be addressed at the outset of litigation”, Mayer, C.J., concurring). Resolution of Section 101 issues prior to filing an answer or conducting claim construction is also supported by an overwhelming majority of district courts facing such issues in cases filed since *Alice* was decided. *See, e.g., In re TLI Commc’ns, LLC*, No. 1:14md2534, 2015 WL 627858, at *1 (E.D. Va. Feb. 6, 2015); *Tuxis Techs.,* 2015 WL 1387815, at *1; *Money Suite Co. v. 21st Century Ins. and Fin. Servs., Inc.,* No. 13-984-GMS, 2015 WL 436160, at *1 (D. Del. Jan. 27, 2015); *Morales v. Square, Inc.,* No. 5:13-cv-1092-DAE, 2014 WL 7396568, at *1 (W.D. Tex. Dec. 30, 2014).[4]

[4] A more narrow view of this principle is stated in *Certified Measurement, LLC v. CenterPoint Energy Houston Electric LLC*, No. 2:14-cv0627-RSP, 2015 WL 1432324, at *2 (E.D. Tex. Mar. 30, 2015), where U.S. Magistrate Judge Payne opined that Section 101 issues should only be addressed in the Rule 12(b)(6) context, and before claim construction, in narrow circumstances. The court did not provide clarity about what circumstances do and do not qualify, and this position is contrary to the great weight of authority and the clear preference for resolution of Section 101 issues “at the outset.” A litigant should not have to undergo the time and expense of unnecessary claim construction and corresponding expensive discovery where, as here, the patent is invalid on its face as a matter of law.

B. <u>Section 101 Patent Eligible Subject Matter</u>

Section 101 of Title 35, United States Code, broadly defines patentable inventions: "new and useful *process*, machine, manufacture, or composition of matter, or any new and useful improvement thereof . . ." Supreme Court precedent recognizes three exceptions to the scope of Section 101: "laws of nature, physical phenomena, and *abstract ideas*." *Bilski v. Kappos*, 561 U.S. 593, 601 (2010) (emphasis added); *see also Ass'n for Molecular Pathology v. Myriad Genetics, Inc.*, 133 S. Ct. 2107, 2116 (2013); *O'Reilly v. Morse*, 56 U.S. 62, 112-20 (1853); *Le Roy v. Tatham*, 55 U.S. 156, 174-75 (1852).

The exceptions to eligibility are rooted in the Patent Clause of the Constitution and its primary objective of promoting innovation, while holding in the public domain "the basic tools of scientific and technological work." *Myriad*, 132 S.Ct. at 2116. The purpose of the Patent Clause would be frustrated "by improperly tying up the future use of" such basic tools. *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 132 S. Ct. 1289, 1301 (2012). Because "all inventions . . . embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas," only *new and inventive applications* of these "basic tools" are patent eligible. *Id*. at 1293; *Gottschalk v. Benson*, 409 U.S. 63, 67 (1972).

Patent eligibility of the implementation of the "basic tools" by computers presents a specific application of the issue. The Supreme Court addressed this issue in *Alice:*

> [I]n applying the §101 exception, we must distinguish between patents that claim the 'buildin[g] block[s]' of human ingenuity and *those that integrate the building blocks into something more*, thereby 'transform[ing]' them into a patent-eligible invention. The former 'would risk disproportionately tying up the use of the underlying' ideas, and are therefore ineligible for patent protection. The latter pose no comparable risk of pre-emption, and therefore remain eligible for the monopoly granted under our patent laws.

Alice, 134 S. Ct. at 2354-55 (emphasis added). The patent at issue in *Alice* claimed a method for mitigating settlement risks in financial transactions by using a computer system as a third-party intermediary. The Supreme Court held that the patent claimed ineligible subject matter, because it claimed the abstract idea of intermediate settlement. Requiring the use of generic computer hardware and software did not transform it into a patent-eligible invention. *Id.* at 2355.

The *Alice* Court's analysis applied the two-step inquiry articulated in *Mayo*, 132 S. Ct. at 1289: first, "we [must] determine whether the claims at issue are directed to one of those patent-ineligible concepts"; and second, if so, whether the claims include "an element or combination of elements that is 'sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.'" *Alice*, 134 S. Ct. at 2355; *see also Ultramercial*, 772 F.3d at 714 (using advertising as medium of currency for access to copyrighted material on the Internet is ineligible). At both steps of the inquiry, the focus is on "the claims at issue." *Alice*, 134 S. Ct. at 2355 (emphasis added); *see also Accenture Global Servs., GmbH v Guidewire Software, Inc.*, 728 F.3d 1336, 1345 (Fed. Cir. 2013).

With regard to the first step, determining whether the patent is drawn to an abstract idea, the *Alice* Court concluded the patent was "drawn to the concept of intermediate settlement," which the Court characterized as "'a fundamental economic practice long prevalent in our system of commerce."' *Alice*, 134 S. Ct. at 2356 (quoting *Bilski*, 561 U.S. at 611). Similarly, the patent in *Bilski* claimed the concept of hedging risk; the claims consisted of nothing more than step-by-step instructions on how to hedge risk. *Bilski*, 561 U.S. at 599.

Subsequent decisions of lower courts make clear that to be an abstract idea, and hence ineligible for a grant of a patent monopoly, the idea need not necessarily be old or have a long history. Abstract *new* ideas are still abstract ideas that *cannot* be patented simply by instructing to perform them on a computer. *Alice*, 134 S. Ct. at 2357-58. Post-*Alice*, courts often perform the first step by focusing on the *purpose* of the claim or the outcome that the patent tries to achieve. The purpose in *Bilski* was to hedge risk, the purpose in *Mayo* was to apply a natural law and the purpose in *Alice* was to mitigate settlement risk through an intermediary. In determining whether a computer-implemented process is abstract, the computer portion must be disregarded–it is the process apart from the computer which must be judged. *Alice,* 134 S. Ct. at 2358 (disregarding presence of computer given "ubiquity of computers"); *see also, McRo, Inc. v. Sony Computer Entm't Am., LLC*, No. CV14-383-GW, 2014 WL 5419425, at *10 (C.D. Cal. Sept. 22, 2014) (same).

Step two of the *Mayo/Alice* analysis asks "what else is there in the claims before us?" *Alice*, 134 S. Ct. at 2355 (quoting *Mayo,* 132 S. Ct. at 1297). The inquiry considers "the elements of each claim both individually and as an ordered combination to determine whether the additional elements transform the nature of the claim into a patent-eligible application" of the concept. *Id*. (quotations omitted). Ultimately, this is a search for an "inventive concept", such that the "'patent in practice amounts to *significantly more* than a patent upon the [ineligible concept] itself.'" *Id*. (quoting *Mayo*, 132 S. Ct. at 1294 (emphasis added). Without such an inventive concept, the risk is too great that the patent will disproportionately tie up one of the basic building blocks of human progress.

In addition, the *Diehr* Court read *Flook* as holding that an abstract idea does not become patentable merely because it is limited "to a particular technological environment" or because the claim recites "insignificant post-solution activity." *Diamond v. Diehr*, 450 U.S. 175, 191-92 n.14 (1981). *See also, Alice*, 134 S.Ct. at 2358 (citing *Bilski*, 561 U.S. at 610–11). The Federal Circuit has reiterated this principle on numerous occasions. *See.e.g., Ultramercial,* 772 F.3d at 716; *Content Extraction,* 776 F.3d at 1348; and *buySAFE, Inc. v. Google, Inc*., 765 F.3d 1350, 1355 (Fed. Cir. 2014).

1. Step One: The Asserted Claims Of the'918 Patent Are Directed To The Abstract Idea Of Securing Access

Courts considering §101 eligibility questions readily accept the probative value of historical proof of time-honored concepts. *See, e.g., Alice*, 134 S.Ct. at 2352. Securing a place, device or form of communication from unauthorized access and intrusion is without question a historic, longstanding and well-known abstract idea. Keys, locks and padlocks date back several thousand years. The Egyptians mastered a technique of "falling pins to control the movement of [a] security bolt." The Romans improved on the concept and through the development of advanced materials, by the 19th Century it was routine to lock homes, safes and anything of value. Keyless padlocks were developed between the 16th and 19th centuries and relied on a combination of letters, numbers and words to gain access. *See generally,* Exs. F-O. Thus, the abstract idea of security and preventing unauthorized access is a longstanding building block in mankind's progress. Walls were used to keep out intruders and block unauthorized entry dating back thousands of years. *See*, Ex. R. ("A History and Survey of Network Firewalls", by K. Ingham and S. Forrest, University of New Mexico Computer Science Department Technical Report (2002)). The Great Wall of China is one of the most prominent examples, but medieval castles protected by moats and walls embodied the same basic building block of human progress. Steam engines on trains had walls between the boiler car and the engine car and passenger cars to protect the fire beneath the steam engine's boiler from spreading to the passenger cars. The modern use of the term "firewall" is derived from historical origins: a "fireproof wall used as a barrier to prevent the spread of fire." *THE AMERICAN HERITAGE COLLEGE DICTIONARY*, 513 (3d ed. 1997), Ex. GG.

Access could also be secured by **humans**, not just mechanisms and hardware, through the use of passwords. The Roman Legions used guards to prevent unauthorized passage. The term "sentry" dates back to the 1600's and is defined as" "[a] guard, esp. a soldier posted at a given spot to prevent the passage of unauthorized persons." *THE AMERICAN HERITAGE COLLEGE DICTIONARY*, 1242 (3d ed. 1997), Ex. GG. During the early 20th century "speakeasy" rooms, where liquor could be acquired during Prohibition or other illegal activities could be enjoyed, were accessed by a combination of human recognition and a password. *See*, Ex. S ("Speakeasy Cards: A Prohibition-Era Ticket to Drink"), T ("Speakeasy"), and U ("Prohibition and Speakeasies").

The idea of securing **communications** from unauthorized access also is a long-standing concept. The Enigma Cipher machines developed in Germany for use by the Nazi military to communicate and maintain daily command and control is but one example. The Enigma machines of World War II relied on a key made up of daily discrete settings or points of information that permitted each character of a message to be enciphered 7-9 times. *See*, Exs. O ("Cipher Machines: The History and Technology of the Enigma Cipher Machine"), P ("Solving The Enigma: History of the Cryptanalytic Bombe"), Q ("Password Security: A Case History"). Passwords of the day used by military, addresses for mail communication, phone numbers for telephonic communication, and IP addresses for computer communication are also examples of applying the fundamental concept of securing access to communication. Passwords have a rich history and a paper describing the use of passwords to gain access in the field of computers is dated as early as 1979 and describes passwords being used in connection with computers as early as the 1960's.

The idea of securing communications between computers, whether originating from humans or not, is likewise a well-established, routine and long-standing concept. The term firewall was borrowed from fire prevention to describe the practice in computer communications of placing a "wall" between the outside world and the contents of the computer to serve as a boundary between networks. All firewalls have a mechanism or set of rules for determining which computer communications pass while blocking others. In the area of computer security, most early firewalls employed some form of data packet filtering to protect networks, directly or through proxies. Ex. BB. ("Firewall (computing)"). Data packets are the basic unit of communication over a digital network. Firewalls inspect the contents of data packets for information such as source address, destination address, port, and compare that information to an established set of rules to decide whether or not to forward the packet. Ex. R at 13. *See generally*, Exs. V-AA, DD, EE.

The first paper describing the use of filtering data packets for user authentication criteria was published by Jeffrey Mogul in 1989. He described the monitoring of "protocol, source and destination addresses and ports to decide which packets were allowed to continue." Ex. R at 9-13. He also described a system of *preconfigured* routing of traffic, just as the '918 patent does. *Id*. Indeed, another history of computer firewalls described data packet filtering of incoming computer communications, developed in the 1980’s at AT&T Bell Labs, as merely the “first generation” of firewalls. Second and third generation firewalls were all developed long prior to the application date of the ‘918 patent. Ex. V. In 2002, one author wrote that “[t]he need for firewalls has led to their ubiquity.” Ex. R at 31.

The ‘918 patent is directed to nothing more than the ubiquitous and abstract concept of securing access against unwanted and harmful intrusion to a computer on a communication network. The underlying idea is basic and fundamental to human and industrial activities. The ‘918 patent secures access using another generic computer, device or software to perform conventional and routine functions with conventional and routine technology in conventional and routine ways. Therefore, the ‘918 patent is ineligible for monopoly protection under the first step of the *Mayo/Alice* analysis. Plaintiff can wrap this patent in as much contrived complexity and verbiage as it wants, but at the end of the day the ‘918 patent claims nothing more complicated than the concept of a bouncer at a nightclub with a list of authorized attendees – you get in if your name is on the list, you don’t get in if it is not. It is that simple. The patent simply claims the abstract concept and applies it to the realm of computer communications.

Like hedging risk in *Bilski* and using a computer as a third-party intermediary to mitigate settlement risk in *Alice*, securing access is a long-standing method of human activity. The combination of information that must match to access the protected computer is not significantly different than a combination to a bank vault’s lock. Indeed, securing access is an abstract idea that is fundamental to almost every human endeavor. Like data collection and storage in *Content Extraction*, “humans have always performed” access authorization as a means of protection. 776 F.3d at 1347. Performing it *with a computer* does not make it any less abstract. Claiming the basic ideas of securing access when implemented by generic computer technology is a patent-drafting attempt to monopolize the concept in the field of computer communications. It clearly implicates the constitutional concern of preemption, because such claims threaten to preempt a basic tool of human endeavor by disproportionately tying up the use of the tool (securing access) in a particular technology (computer communication). *See Alice*, 134 S. Ct. at 2354-55.

In fact, based on Wetro's mass filing practice against a wide variety of products, it seemingly has taken the position that its asserted claims are so sweeping that they cover and tie up virtually *any* practical use of computer technology to secure a computer from hackers. *Benson*, 409 U.S. at 68 (warning against the damage of tying up general concepts). Securing access and its basic steps, even in the field of computer communication, are ubiquitous. *See, e.g.,* U.S. Pat. No. 5,802,320, Ex. CC, at Abstract (1995 application disclosing a system for securing access to a private network or computer from a public network by screening data packets for source, destination and incoming port on a proxy computer and permitting or denying access).

The idea of securing access is no less abstract when limited to the technological environment of computer communication. In *CertusView Techs., LLC v. S & N Locating Servs., LLC*, No. 2:13CV346, 2015 WL 269427, at *22 (E.D. Va. Jan. 21, 2015), the court rejected the argument that limiting application of a database to the environment of geo-locate operations, even if never done before, was an inventive concept and sufficient to satisfy step two. Here too, securing access does not become patentable simply because it is limited to computer security.

As discussed *supra*, securing access has long been a fundamental practice in human history and activities.[5] The ubiquitous nature of securing access has been the basis of post-*Alice* courts decisions invaliding patents directed to **securitizing** aspects of computer activity. A very recent decision invalidated a patent similarly directed to packet filtering according to rules as a means of serving as a firewall. In *Intellectual Ventures II LLC v. JP Morgan Chase & Co.,* No. 13-cv-3777 (AKH), 2015 WL 1941331, at *7-*9 (S.D.N.Y. April 28, 2015), the Court held that such a patent was directed to an abstract idea for three reasons: 1) the patent claimed the mental process of filtering packets according to unclaimed rules; 2) the breadth of the claim raised preemption concerns; and 3) it failed the machine-or-transformation test. The Federal Circuit has likewise invalidated patents claiming similar abstract ideas. *See e.g., Content Extraction,* 776 F.3d at 1343 (patent for extracting data from documents, recognizing specific information and the selected information invalid as patent-ineligible); *Cybersource Corp. v. Retail*

[5] The *Alice* Court cited two historical academic sources to buttress its view that this was a “long prevalent” practice. *Alice,*134 S. Ct. at 2356. Other courts similarly resort to historical sources to support a finding of a fundamental, long-standing idea to qualify as one of the building blocks of human ingenuity. *See, e.g., buySAFE*, 765 F.3d at 1355; *Bascom Research, LLC v. LinkedIn, Inc*., No. 12-CV-06293-SI, 2015 WL 149480, at *6 (N.D. Cal. Jan. 2, 2015) (linking documents based on relationship is centuries old idea); *Enfish, LLC v. Microsoft Corp*., No. 2:12-CV-07360 MRP-MRW, 2014 WL 5661456, at *6 (C.D. Cal. Nov. 3, 2014) (using tables to store data); *Vehicle Intelligence & Safety v. Mercedes Benz USA, LLC*, No. 13C4417, 2015 WL 394273, at *4 (N.D. Ill. Jan. 29, 2015) (citation to encyclopedia re expert system). However, historical prevalence is not essential to establishing a patent’s abstract purpose. *Content Extraction*, 776 F.3d at 1347 (data extraction); *Ultramercial*, 772 F.3d at 715 (advertising to pay for content); *Fairfield Inds., Inc. v. Wireless Seismic, Inc.*, No. 4:14-CV-2972, 2014 WL 7342525, at *4 (S.D. Tex. Dec. 23, 2014) (relaying information); *Joao Bock Transaction Sys., LLC v. Jack Henry & Assoc., Inc*., No. 12-1138-SLR, 2014 WL 7149400, at *5-6 (D. Del. Dec. 15, 2014) (real-time monitoring of banking transaction security).

Decisions, Inc., 654 F.3d 1366 (Fed. Cir. 2011) (pre-*Alice*, method for securing credit card transactions over the Internet unpatentable); *Cyberfone Sys., LLC v. Cellco Partnership*, 885 F. Supp. 2d 710, 719 (D. Del. 2012), *aff'd* 558 Fed.Appx. 988 (Fed. Cir. 2014) (pre-*Alice*, system for capturing data at point of transaction and transmitting to databases for processing and storage invalid under Section 101). Other district courts reach similar results. *See, e.g., Intellectual Ventures I LLC v. Symantec Corp.*, No. 10-1067-LPS, 2015 WL 1843528 (D. Del. April 22, 2015) (method of creating content identifier and comparing to a database for filtering e-mail messages, spam and viruses and method of filtering and restricting distribution of e-mail and files according to rule engine invalid under Section 101); *Joao Bock Transaction Sys.*, 2014 WL 7149400, at *5-6 (method of real-time authorization, notification and security of electronic banking and credit transactions invalid at patent ineligible); *Loyalty Conversion Sys. Corp. v. American Airlines, Inc.*, No. 2:13-cv-655, 2014 WL 4364848 (E.D. Tex. Sept. 3, 2014) (using computer to convert one vendor's loyalty credits to another vendor's credits patent ineligible). These decisions, *inter alia*, indicate the same finding is warranted here.

Therefore, step one of the *Mayo* analysis is satisfied as a matter of law. The claims in this case are directed to an ineligible abstract idea that, if allowed, would, per Wetro's mass filing of complaints, result in monopolization of either all of, or most of, the entire field of using computers to secure access to computers by analyzing data packet information and comparing it against pre-set rules, decision blocks or look-up tables. The patent discloses no specific improvements to the rules, hardware and software that secure access. *See, Vehicle Intelligence & Safety*, 2015 WL 394273, at *3 (no new or improved computer technology or hardware); *Cloud Satchel, LLC v. Amazon.com, Inc.*, No. 13-

941-SLR, 2014 WL 7227942, at *8 (D. Del. Dec. 18, 2014) (no improvements to the computer; just apply abstract idea to pre-existing conventional computers); *Compression Tech. Solutions LLC v. EMC Corp.*, No. C-12-01746RMW, 2013 WL 2368039 (N.D. Cal. May 29, 2013), *aff'd*, 557 F. App'x 1001 (Fed. Cir. 2014) (holding that software patent claiming method for "parsing similar information streams into identical packets" amounted to patent-ineligible mental process). The patent also does not transform or change the contents of the data packets. *Intellectual Ventures II*, 2015 WL 1941331, at *9. The inventor merely claimed using any computer hardware and any software to implement any system of analyzing and comparing data packet contents for ubiquitous categories of information.

The ‘918 patent simply uses computers to do what computers do, namely make a process that could be done by humans *faster and more efficient*. Given the data packet information and a look-up table or a set of rules to apply, a human could do what the firewall or router device does, but only a computer can extract, analyze, decide and take action (drop or let the communication in) faster and more efficiently than a human. Cyber-attacks are one of the greatest threats facing our modern society. Technological devices for securing access, such as physical locking mechanisms, are clearly patentable, but Wetro wants to cover the abstract idea of using a locking mechanism to protect computers from hackers without disclosing a new and improved lock. The basic concept of securing computers from cyber-attacks is simply too fundamental and too essential to permit the breadth of monopolization threatened here.

2. Step Two: The Additional Elements of the Asserted Claims Of The ‘918 Patent Do Not Add An “Inventive Concept” That Is “Significantly More” Than The Abstract Idea Of Securing Access

Under *Alice*, an abstract idea can become patentable if the claims add an “inventive concept” that is “significantly more” than the abstract idea: “an element or combination of elements that is sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the ineligible concept itself.” *Alice*, 134 S. Ct. at 2355 (quotations omitted). Step two of the *Mayo* analysis inquires whether any claimed element, other than the concept of securing access, “transform[s] the nature of the claim into a patent-eligible application.” *Id*. at 2355 (quotations omitted).

The role of the inventive concept requirement is to provide “practical assurance” that the method is not a drafting effort to monopolize the idea. *Mayo*, 132 S. Ct. at 1297. For an abstract idea to satisfy step two, there must be “additional features” that are ***more than “well-understood, routine, conventional activity.”*** *Id.* at 1297-98 (emphasis added); *see also, Ultramercial*, 772 F.3d at 715 (same).

The elements of the asserted claims do not pass this test because they are all directed to routine, conventional activity for securing access, particularly in a computer communication environment. The claims merely recite a “series of steps instructing how to” do something at a very general level and all steps are the germane essence of securing access in the current computer and Internet environment. *Ultramercial*, 772 F.3d at 715. The additional elements of the ‘918 patent do not add “significantly more” than, and do not transform the patent into anything other than, an ineligible patent on the abstract idea of securing access.

The elements of representative claim 1 broadly and abstractly foreclose improvements to network security that involves data packer filtering according to any rule set. They are not limited to any **specific** machine or program. These claims add nothing more than a directive to use long-standing, readily available computer components, to implement a network security firewall. *Intellectual Ventures II*, 2015 WL 1941331, at *9-*12 (data packet filtering firewall fails second step of *Mayo* because it simply takes “information conventionally sent to a firewall” and implements the process with generic computer).

Stripping out relevant data and comparing it to a look-up table claims the basic building blocks for securing access to computer communications. Nothing more specific is claimed. Based on Wetro’s broad-sweeping filing practices, to allow the patent claims to stand seemingly means that any company, whether an innovator like Emerson and its subsidiaries or an end user, would infringe by collecting and analyzing the contents of data packets for source, destination and protocol information as a means of determining which communications pass through and which are dropped. There is no disclosure of an improved analysis technique, improved computer hardware or functionality or particular improved software for performing the required analysis. To permit a patent on an essential abstract concept without adding sufficiently innovative value or benefit is exactly what the Supreme Court sought to foreclose in *Alice*.

a. Collecting and Analyzing Data Packets for Source, Destination and Protocol Information Is Not “Significantly More”

The broad, general steps of collecting and analyzing data packets for source, destination and protocol information adds no patentable subject matter. It is settled law that merely requiring a specific activity be conducted with computers or on the Internet neither adds the requisite inventive concept nor transforms the claim to something other than a claim to an abstract concept. *Alice*, 134 S. Ct. at 2352. *See also, Ultramercial*, 772 F.3d at 715-16; *Content Extraction*, 776 F.3d at 1347; *buySAFE*, 765 F.3d at 1355; *Cybersource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1370 (Fed. Cir. 2011); *Clear with Computers*, 2015 WL 993392, at *4-5; *Fuzzysharp Techs. Inc. v. Intel Corp.*, No. 12-CV-04413-YGR, 2013 WL 5955668, at *11 (N.D. Cal. Nov. 7, 2013); *Bascom Research*, 2015 WL 149480, at *9-12; *Intellectual Ventures I*, 2014 WL 7215193, at *4; *Open Text S.A., v. Box, Inc.*, No. 13-CV-04910-JD, 2015 WL 269036, at *3 (N.D. Cal. Jan. 20, 2015); *Wolf v. Capstone Photography, Inc*., No. 2:13-CV-09573, 2014 WL 7639820, at * 9 (C.D. Cal. Oct. 28, 2014). So too, collecting and analyzing data packets for source, destination and protocol information does not convert an abstract concept into something more. "Electronically transmitting and/or storing" data are nothing more than the "abstract process of taking input information" to conduct some operation. *See CertusView Techs.*, 2015 WL 269427, at *16. Soo, too, filtering data according to pre-set criteria. *AmDocs (Israel) Ltd. v. Openet Telecom, Inc.*, No. 1:10CV910 (LMB/TRJ), 2014 WL 5430956 (E.D. Va. Oct. 24, 2014) (correlating and enhancing network data usage patent ineligible).

b. Performing Data Packet Analysis With Generic Computer/Software to Detect Unauthorized or Authorized Access Is Not "Significantly More"

The '918 patent specifies computer hardware and software at the most generic and generalized level: "data packet", "source, destination and protocol information", "receiving", "extracting", "decision block", "lookup table", "dropping", "permitting", "communication interface", "packet analyzer", "storage device". The '918 patent does not purport to lay claim to inventing such hardware or software or to applying computer automation to the field of computer communication security. Indeed, the background of the "invention" discloses that the relevant computer technology was already known and available in many name-brands. Ex. A, Col. 2, ll. 20-22 ("hardware and software solution already available on the market"), Col. 2, l. 32 ("present software solutions"), Col. 4, ll. 43-Col. 7, ll. 34 (description of non-limiting and wide array of existing and "already available" devices and software on which the method can be performed). The description of the invention also demonstrates that what is claimed is not limited to any particular computer: "this description is not intended to be construed in a limiting sense." Ex. A, Col.8, ll.7-9. Simply tying the "system" to generic computer technology provides no meaningful limitation on the application of the abstract idea.

Numerous courts since *Alice* have considered applications of such existing computer technology to implement various abstractions and found them patent ineligible. *See, e.g., Vehicle Intelligence & Safety,* 2015 WL 394273, at *5-8 (expert system modules, artificial intelligence systems, database modules, decision modules, interface modules, processors). Predictive applications of computer software are also not inventive. *See, e.g., Genetic Techs. Ltd. v. Lab. Corp. of Am. Holdings*, No. 12-1736-LPS-CJB, 2014 WL 4379587, at *11-14 (D. Del. Sept. 3, 2014) (predicting athletic performance based on genetics); *IpLearn, LLC v. K12 Inc.*, No. 11-1026-RGA, 2014 WL 7206380, at *7 (D. Del. Dec. 17, 2014) (predicting student weaknesses).

The insufficiency of the added elements here is confirmed by the fact that the activity controlled by the computer could be done by humans. *Bascom Research*, 2015 WL 149480, at *12; *Clear with Computers*, 2015 WL 993392, at *4-5; *Fuzzysharp Techs.*, 2013 WL 5955668, at *11-3. It is not enough that a computer or the Internet makes the activity more efficient. *Bancorp Servs., LLC v. Sun Life Assurance Co. of Canada (U.S.)*, 687 F.3d 1266, 1278 (Fed. Cir. 2012); *IpLearn*, 2014 WL 7206380, at *7. Yet, the ‘918 patent itself does not purport to invent anything other than a method to secure access to a computer in a manner that is “simple to implement, inexpensive, relatively fast, efficient and non-user configurable.” Ex. A., Col. 3, ll. 4-6. *See also,* Ex. A, Col. 3, ll. 64-67 (“quick performance”). Humans could perform the tasks of comparing data packet information, once stripped out, against a look-up table to determine whether to accept the communication, just as caller identification empowers a human to decide whether to accept an in-coming call. Humans just could not do it as fast as computers, which is exactly what computers are expected to do. Conventional results are achieved by the ‘918 patent using conventional means.

Specific computer hardware and software is not *essential* to performing the tasks of securing computer communications. To implement the method with a computer, though, *does require* the generic computer hardware and software components described in the most general terms in the ‘918 patent claims. The ‘918 patent’s failure to innovate past the commonplace and describe any particular hardware or methodology for the computer to perform, whether it be a new device for filtering data packets or software requirements for the rules contained in a look-up table, renders it devoid of an inventive concept.

c. Requiring the Filtering Rules to Be “Non-Configurable” By the User Is Not “Significantly More”

The claim elements that the rules in the packet analyzer/look-up table be “non-configurable” and “substantially free from user adjustment” do not add a sufficiently inventive concept to overcome preemption concerns. The ‘918 patent is expressly directed to the *home and small business environments* where users presumably do not have the ability to configure a firewall or computer security system. Ex. A, Col. 1, ll. 28-29, Col. 2, ll. 25-26, 51-52, 60-62, Col. 3, ll. 6-8. The apparent inventive notion was to make the security system's generic look-up tables "non-configurable", *i.e.*, ready to use for this unsophisticated market.

Making the firewall rules free from adjustment is *entrepreneurial* rather than *technological*. As Circuit Judge Mayer stated in his concurring opinion in *Ultramercial*, the problem with the arguably innovative intermediated settlement technique was not that it was not new and useful, but that it did not "improve the functioning of the computer itself" or "effect an improvement in any other technological or technical field." *Ultramercial*, 772 F.3d at 721 (Mayer, C.J., concurring) (quoting Alice, 134 S.Ct. at 2359). *See also, Diamond v Diehr,* 450 U.S. 175, 177-79 (1981) (patent valid because it improved "technological process"). Judge Mayer thus characterized *Alice* as articulating a "technological arts test for patent eligibility." *Id*. The notion that Internet users would be willing to watch ads in return for access to content (notably another example of a means of securing access in the computer realm) did not advance technology.

Similarly, the concept of removing the burden of configuration completely or substantially from a user does not advance technology. Rather than solving a problem unique to the Internet or transforming or improving the functioning of a computer, the element merely removes from the user the burden of performing an essential element of data packet filtering in firewalls and routers–establishing rules. What is claimed is nothing more than the generic–"look-up table", or even more generic "decision block" or "packet analyzer"–and adding the concept of a more convenient and enjoyable user experience. The generic hardware and software is essentially locked from user tampering or customization. This elimination adds convenience and ease, not technological progress.

Many technological activities require a user to make settings to enable functionality, thus requiring both effort and expertise. Eliminating these makes the user experience easier, simpler and faster, which is precisely how the specification described the advantages of the element. It does not change the contents of the data packets, does not make the filtering process faster, and does not even make Internet communications more secure. *Cf., DDR Holdings, LLC v. Hotels.com L.P.*, 773 F.3d 1245, 1257 (Fed. Cir. 2014) (the claimed solution is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks).

Here, the '918 patent does not define and claim a solution to a new hacking technique that is plaguing computer users and posing a serious security threat. Rather, the "non-configurable" element of the claim is directed to a **marketing** concept by making the most basic of design choices, i.e., making the look-up tables non-configurable (or at least "substantially" non-configurable), to make the router/firewall more marketable to a home user/small business market segment. The patent does not purport to introduce a new computer, new software, or any new procedures for improving security–not even for the home or user market. It merely compares standard data packet information to a basic look-up table. There is no technological innovation set forth anywhere in the patent.

Although prior art concepts common to Section 102 novelty and Section 103 non-obviousness are directed to different concerns[6] than Section 101 patentable subject matter, an indication that rendering the data packet filtering rules non-configurable is not inventive is the fact that *non-configurability* was already ubiquitous in Internet security before the ‘918 patent. For example in “*A History of and Survey of Network Firewalls*”, written by University of New Mexico Computer Science Department members in 2002, it relied on articles dating to 1989-1999 to note that packet filtering did not require “the cooperation of the users” or “any special action on their part.” Ex. R at 13.

Finally, the purpose of Step 2 of the *Mayo* test is to allay disproportionate preemption risks when a patent is directed to an abstract idea. The “non-configurable”[7] element exacerbates rather than allays preemption risks. In the context of data packet filtering using rules set out in look-up tables, there are, of course, only two options for look-up tables: user modifiable or user non-modifiable. Only one of those options improves the user experience. In other words, the ‘918 patent purports to monopolize *half* of potential security solutions - non-modifiable. This is so even though it would be a basic concept to any firewall designer that a look-up table could be non-modifiable for simple, unskilled, homer user applications as opposed to situations that require evolving and more complicated security where the look-up table must be modified to account for changing circumstances. Hackers are constantly figuring out new ways to circumvent

[6] *Intellectual Ventures II*, 2015 WL 1941331, at *9; *Synopsys, Inc. v. Mentor Graphics Corp.,* No. C12-6467MMC, 2015 WL 269116, at *5 (N.D. Cal. Jan. 20, 2015) (lack of prior art not relevant in step two of Mayo, because inventive concept is different than novelty and non-obviousness); *Cogent Med., Inc.*, 2014 WL 4966326, at *4 n.3 (same).

[7] As part of any response, Wetro should explain what it believes “non-configurable” means as used in the patent claims. Of course, whether the look-up table is modifiable or non-modifiable reflects merely the most basic of design choices and should not be patentable under Section 101 regardless of what it means.

firewalls and corporate protection needs.

Here, though, the preemption risk also gets worse not better, than half of solutions. The claims use the term “non-configurable” to signal not capable of modification at all, yet the claims also add words of degree–“*substantially* free from user adjustment” (emphasis added). This creates greater preemption risk, because the patent discloses no means or direction as to what can be modified, how to modify it or how much modification still qualifies as “non-configurable”. What is clear is that the claims on their face *attempt* to cover both modifiable and non-modifiable look-up tables–100% of solutions. In other words, it’s far from clear what the claims would *not* cover, which is presumably why Wetro thinks it is entitled to money from such a diverse group of defendants marketing such a diverse group of products. Such breadth is disproportionate to the complete lack of technological advancement, because nothing in the patent makes Internet communication more secure from hacking.

Thus, there is nothing in the asserted claims of the ‘918 patent which satisfies the *Mayo* search for an “inventive concept.” The additional elements offer no assurance that the “‘patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.’” *Alice*, 134 S.Ct. at 2355 (quoting *Mayo*, 132 S. Ct. at 1294).

VI. CONCLUSION

The ‘918 patent serves no useful purpose and impedes the progress of innovations for securing access to computers. The basic steps/building blocks disclosed in the ‘918 patent belong to the public. For the foregoing reasons, Emerson respectfully requests that the complaint be dismissed pursuant to Rule 12(b)(6), because the ‘918 patent is invalid under 35 U.S.C. §101.

Dated: May 18, 2015

Respectfully submitted,

Michael Smith

By:
Michael C. Smith
State Bar Card No. 18650410
michaelsmith@siebman.com
SIEBMAN, BURG, PHILLIPS & SMITH, LLP
P.O. Box 1556
Marshall, Texas 75671-1556
Telephone: (903) 938-8900
Facsimile: (903) 767-4620

and

Rudolph A. Telscher, Jr.*
email: rtelscher@hdp.com
Steven E. Holtshouser*
email: sholtshouser@hdp.com
HARNESS, DICKEY & PIERCE, P.L.C.
7700 Bonhomme, Suite 400
St. Louis, MO 63105
Telephone: 314-726-7500
Facsimile: 314-726-7501
**Pro Hac Vice Pending*

Attorneys for Defendant Emerson Electric Co.

CERTIFICATE OF SERVICE

I hereby certify that on this 18th day of May, 2015, the foregoing was filed electronically with the Clerk of Court to be served via the Court's Electronic Filing System upon the following:

AUSTIN HANSLEY P.L.L.C.
Austin Hansley
Texas Bar No.: 24073081
Brandon LaPray
Texas Bar No.: 24087888
5050 Quorum Dr. Suite 700
Dallas, Texas 75254
Telephone: (469) 587-9776
Facsimile: (855) 347-6329
Email: Austin@TheTexasLawOffice.com
Email: Brandon@TheTexasLawOffice.com

Attorneys for Plaintiff

Michael Smith