Marquette Intellectual Property Law Review

Volume 16 | Issue 2 Article 5

God in the Machine: Encryption Algorithms and the Abstract Exemption to Patentability

Jeremy R. Hager

God in the Machine: Encryption Algorithms and the Abstract Exception to Patentability

I. INTRODUCTION 483
II. THE SUM OF ITS PARTS: AN OVERVIEW OF DIGITAL RIGHTS MANAGEMENT TECHNOLOGY AND THE RELEVANT LAW 485
A. Is for Algorithms 488
1. Encryption: The Common Denominator 488
2. Strength in Numbers 490
B. The Industry Standard 491
1. The Chain Rule 491
2. Sine on the Dotted Line 493
3. The Prime Variable 493
III. THE PATENT-DRM CONUNDRUM 494
A. Knowledge and Not On Numbers 495
1. Arithmus ex Machina 495
2. "As a Whole" 497
3. A Slippery Slope 498
4. A Solution? 501
B. What the Circuit Giveth, the Supreme Court Taketh Away 502
1. Division of the Issues 502
2. Remainder Questions 503
IV. SOLVING THE EQUATION 505
V. CONCLUSION 506

I. INTRODUCTION

Tensions were high when the Supreme Court announced its decision in the long-awaited *Bilski v. Kappos,*[1] a case expected to settle a dispute that had spanned more than thirty years[2] over the proper method for determining the patentability of processes under 35 U.S.C. § 101. Hanging in the balance were the futures of business methods patents, risk management patents, software patents, and other processes that skirted the bounds of 35 U.S.C. § 101. Some speculated an end to

1. Bilski v. Kappos, 130 S. Ct. 3218 (2010).
2. *See, e.g.,* Gottschalk v. Benson, 409 U.S. 63 (1972).

software patents in the United States entirely.[3] Others predicted clarification about the physical requirements of the "machine-or-transformation test," which had been determined by the Court of Appeals for the Federal Circuit as the *sole* means for determining patentable subject matter for process patent applications.[4] Anticipations and expectations were high for some clarity on the prevailing questions about software patents. Opponents to the existing system argued that current patentability standards were too broad, which overburdened the United States Patent and Trademark Office and hindered progress in e-commerce and other areas.[5] Proponents said that the current system worked just fine, as evidenced by the United States being a global leader in technological innovation.[6] What these interested parties got instead was little clarification on the machine-or-transformation test, or on software patentability as a whole. Rather, the Supreme Court confounded the debate by clarifying that the machine-or-transformation test was *one* means for determining whether a proposed process patent was eligible for patentability, but not the *sole* test[7] . . . oh and abstract ideas still cannot be patented.[8] Obviously, this ruling fell considerably short of the paradigm-shifting ruling expected, and commentators on both sides of the software patent issue are in no better position than they were previously. The resounding question remained—what is the definition of "abstract?" It had long been established that algorithms, existing alone as mathematical formulae, were abstract,[9] but where does that leave software, which relies on algorithms to function and transform data? The Court reaffirmed its belief that Congress contemplated that patent's scope would be broad and encompassing,[10] while reiterating section 101's outer bounds.[11] The

3. David Worthington, *In Re Bilski - The End of Software Patents?*, SOFTWARE DEVELOPMENT TIMES (July 8, 2009, 12:51 PM), http://www.sdtimes.com/blog/post/2009/07/08/In-re-Bilski-The-end-of-software-patents.aspx.

4. *See In re* Bilski, 545 F.3d 943, 954 (Fed. Cir. 2008) ("An argument can be made that the Supreme Court has only recognized a process as within the statutory definition when it either was *tied to a particular apparatus* or operated to *change materials to a 'different state or thing.*'") (emphasis added); *see also In re* Bilski, 545 F.3d at 955–56.

5. Kevin Coughlin, *Technology upends the meaning of invention Patent requests shift to ideas, know-how*, THE STAR-LEDGER, March 12, 2000, at A1.

6. *Id*.

7. Bilski v. Kappos, 130 S. Ct. 3218, 3227 (2010).

8. *Id.* at 3230.

9. *See, e.g.,* Gottschalk v. Benson, 409 U.S. 63 (1972); Parker v. Flook, 437 U.S. 584 (1978); Diamond v. Diehr, 450 U.S. 175 (1981).

10. *Bilski*, 130 S. Ct. at 3221.

11. *Id.* at 3225 ("[T]hree specific exceptions to § 101's broad patent-eligibility

question further stood that, if software, which is classified as a process patent, must stand to subject matter muster, would it pass the machine-or-transformation test? Seeing as how the Supreme Court failed to rule definitively on the issue, if a software patent did not pass this test, would there be any other threshold for determining whether it was patentable, given the various tests hammered out by the circuit courts over the years? Hovering on the outskirts of this debate is the fate of DRM, a heavily algorithm-based technology that currently enjoys patent protection.[12] At the center of the nebulous DRM cloud is its most vital technological component, encryption. It is this patented[13] encryption technology that remains most vulnerable in *Bilski*'s wake, and its future could make or break the industry as a whole.

II. THE SUM OF ITS PARTS: AN OVERVIEW OF DIGITAL RIGHTS MANAGEMENT TECHNOLOGY[14] AND THE RELEVANT LAW

There really is no generally-accepted definition for "Digital Rights Management."[15] Put simply, DRM is the layering of both technological and legal means[16] to prevent and discourage third parties from gaining unauthorized access to digital content. The scope of DRM is very broad. In their simplest forms, DRM systems act as copy-prevention systems by preventing, or at the least, impeding, consumers from copying digital content from various tangible sources, such as DVDs and CDs, cell phones, and eBook readers.[17] In their more complex forms, DRM systems differ in scope, from facilitating diverse complex business models, such as pay-per-use[18] systems, to secured

principles: 'laws of nature, physical phenomena, and abstract ideas.'").

12. Greg Vetter, *Patenting Cryptographic Technology*, 84 CHI.-KENT L. REV. 757, 759 (2010).

13. Currently, the United States Patent and Trademark Office (USPTO) uses the "380" numerical classification for patents in the general cryptographic class. *Id.* The USPTO's website allows one to explore the various types of patentable subjects under each class. Class 380 contains several subclasses of encryption claims. *See* Class 380 Cryptography, U.S. PAT. & TRADEMARK OFFICE, http://www.uspto.gov/web/patents/classification/uspc380/sched380.htm (last modified Aug. 11, 2011).

14. This section in no way attempts to explain, in any major detail, the technologies associated with DRM. It is merely an attempt to summarize the technologies briefly, leading then into the more relevant topic of encryption.

15. Stefan Bechtold, *Digital Rights Management in the United States and Europe*, 52 AM. J. COMP. L. 323, 324 (2004) (hereafter Bechtold).

16. *See infra* A(3).

17. *See* Bechtold, *supra* note 15.

18. Pay-per-use models involve systems in which consumers pay for their individual

communication, such as wireless (Wi-Fi) networking and Bluetooth technologies,[19] to secure distribution systems, such as music[20] and video downloading/streaming,[21] and secured web browsing, or even online transactions. While the DRM systems that exist are multifarious, most share one common trait. The common trait in these systems, and arguably the most important facet of DRM as a whole, is encryption.[22] Encryption is essentially the process of modifying data systematically, so as to make that data unreadable, while allowing for the data to be restored to its original state by an (in theory, anyways) authorized user.[23] The science of using secret codes or methods to prevent unauthorized reading of content is called "cryptography,"[24] and is crucial to encryption.

Cryptography is by no means a new science. It has existed as a means for securing information for centuries, dating back to antiquity. Spartan commanders used a cipher system involving batons and paper, the combination of which was called a "scytale," to encode messages.[25] Gaius Julius Caesar communicated with his field generals during military campaigns with a relatively simple form of cryptography, the "Caesar Cipher," in which the letters were shifted three places forward

---

use of digital content. *Id.*

19. Joseph Kashi, *Hi-Tech in the Law Office: We're all Confronted by the Mobile Security Sieve*, 28 ALASKA BAR RAG 26, 27 (2004).

20. *See* Bechtold, *supra* note 15, at 327. Though, the trend of using DRM encryptions on music sites is a trend that is falling out of favor. *See* Christopher Breen, *DRM-Free iTunes: What it Means for You,* PCWORLD (created Apr. 7, 2009 12:50 PM), http://www.pcworld.com/article/162732/drmfree_itunes_what_it_means_for_you.html.

21. *See* Tim Conneally, *Hulu whips up its own DRM to block people from watching videos outside browsers*, BETANEWS, http://www.betanews.com/article/Hulu-whips-up-its-own-DRM-to-block-people-from-watching-videos-outside-browsers/1238697188, April 2, 2009 (last visited Feb. 28, 2011) (detailing one such DRM system implemented by online video provider Hulu).

22. Bechtold, *supra* note 15, at 326 (citing Dean S. Marks and Bruce H. Turnbull, *Technical Protection Measures: The Intersection of Technology, Law and Commercial Licenses,* 22 EUR. INTELL. PROP. REV. 198, 204 (2000), *available at* http://www.wipo.int/edocs/mdocs/copyright/en/wct_wppt_imp/wct_wppt_imp_3.pdf at 11 ("Encryption of content is *key* for distinguishing clearly between authorized uses and unauthorized uses, especially in computer environments. No individual or device can decrypt content 'by accident'. [sic] Hence, *encryption is the keystone* of current copy protection efforts.") (emphasis added)).

23. *See* JOAN VAN TASSEL, DIGITAL RIGHTS MANAGEMENT 85 (2006).

24. KENNETH R. REDDEN & GERRY W. BEYER, MODERN DICTIONARY FOR THE LEGAL PROFESSION 257 (2001).

25. Oliver Pell, *A Brief History of Cryptography and Cryptanalysis*, CRYPTOLOGY, http://www.ridex.co.uk/cryptology/#_Toc439908853.

in the alphabet.[26] The commander in receipt of the encrypted correspondence would simply shift the letters backwards three spots in the Roman alphabet, and read the newly formed message.[27] During the middle ages, European governments relied on coded vocabularies, called *nomenclatures*, to communicate sensitive diplomatic information.[28] Allied success at capturing and breaking the German aptly-named "Enigma Machine" and its code, respectively, contributed greatly to the Allied victory in World War II.[29] Historically, with new advances in technology, came the need for more advanced copyright laws. This "intertwining" of technology and copyright, wherein the progress of the former demands expansion of the latter, has spiraled onward with the march of time, demanding new copyright protections with new advances in technology.[30] But the story of cryptography in regards to DRM begins in the mid-20th Century. The creation of new, more accessible content-copying technologies through the 1960s and 1970s, such as copy machines, audio recording devices, and video recording devices, made it much easier for the average consumer to copy and distribute media and content, which rendered content-producing industries all but helpless to enforce copyright protections.[31] This technologically-induced expansion of inexpensive means for dissemination of information paved the way for newer technologies to do the same for digital content preceding the turn of the century.[32] As expected, these technological revolutions necessitated the expansion of the protections afforded to content producers. What resulted was a partnership between industry-created technological protections—DRM—and legislative expansion—the Digital Millennium Copyright Act.[33]

The first thing one must realize when examining DRM encryption technologies and DRM software is that while they both are considered synonymous, insofar as patentable subject matter claims (that being a

---

26. CHRISTOPHER SWENSON, MODERN CRYPTANALYSIS 2 (2008).

27. *Id*.

28. Bechtold, *supra* note 15.

29. *See* Jerry C. Russell, *Ultra and the Campaign Against the U-Boats in World War II*, (created Sept. 2, 1996 1:16 PM), http://www.ibiblio.org/pha/ultra/navy-1.html.

30. *See generally* Gary S. Lutzker, *Dat's All Folks: Cahn v. Sony and the Audio Home Recording Act of 1991 - Merrie Meldoies or Looney Tunes?*, 11 CARDOZO ARTS & ENT LJ 145, 149 (1992).

31. *See generally* Joseph H. Sommer, *Against Cyberlaw*, 15 BERKELEY TECH. L. J. 1145, 1220 (2000).

32. *Id.*

33. The DMCA is discussed in more detail *infra* (B)(3).

"process" or "method" patent claim), they are intrinsically different. While not all systems that fall into the DRM classification use encryption, encryption is the most common means of copy protection and the core technology most associated with DRM.[34] Oftentimes DRM encryption technology is deployed via software.[35] The algorithms that make up the bulk of encryption schemes are based in advanced mathematical concepts, and the difficulty of breaking these encryption schemes depend on the keylength and the system/software implementing the encryption.[36] As time progresses and cryptographic research advances, new algorithms and new investors arise to put money into patenting new encryptions devices.[37] It is of no surprise then that the increase in software patenting has directly led to a rise in the need for new cryptographic techniques.[38] A DRM encryption device inventor will typically apply for a patent on his encryption technology as a "method claim,"[39] which recites the series of steps that comprise the method.[40] Thus, a patent application for a DRM encryption technology will be considered by the patent examiner as a process patent.

A. Is for Algorithms

1. Encryption: The Common Denominator

The technology employed in DRM is vast and complex.[41] A basic understanding of the encryption and decryption process is necessary before delving into the issues of patentable subject matter *of* these encryption devices. Whether the technology is the type of DRM found on DVDs,[42] downloadable music,[43] or streaming digital content,[44] most

---

34. VAN TASSEL, *supra* note 23, at 89.

35. Vetter, *supra* note 12, at 758.

36. VAN TASSEL, *supra* note 23, at 91–93.

37. *Id.* at 95.

38. Brian Spear, *Cryptographic Patents: At War and in Peace*, 22 WORLD PATENT INFO 177, 180–81 (2000).

39. For example, the HDCP encryption key patent. U.S. Patent No. 7,034,891 (filed Jan. 31, 2003).

40. *Supra* note 14.

41. This article will not attempt to explore the numerous and varied technologies involved in cryptology and DRM, but will instead focus on the common types of encryption schemes used in DRM, and more specifically, the encryption and decryption devices themselves. To go any further into the technological wilderness would fill many books. In fact, there are already some interesting writings on the more technical and mathematical aspects of DRM. *See e.g.,* Sommer, *supra* note 31; BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C (1994).

42. Such as CSS. *See* VAN TASSEL, *supra* note 23, at 155. (Author's note: CSS was not

DRM technologies employ patented encryption devices, or technologies that encrypt or scramble, using an algorithm, the digital content so that it is unreadable without the decryption key.[45] Encryption is the most common means of copy protection, and is the core technology associated with DRM.[46] The content-provider will then license, to device manufacturers, the encryption scheme, with the encryption and decryption keys necessary to first encrypt their content, rendering it unreadable, and then decrypt and thus access and display/play it.[47]

Two common types of encryption schemes[48] are "symmetric" encryption and "asymmetric" encryption.[49] Symmetric encryption schemes, such as the Data Encryption Standard (DES) encryption, involve the encryption of data by one party, who then shares the key that decrypts it with the second party, who decrypts the data with that key.[50] A second type of encryption scheme is an asymmetric or "public-key" scheme.[51] This type of scheme, such as RSA,[52] is more complex. In a public-key encryption scheme, each party has two keys—a public key and a private key. One party sends his public key to the other party. The other party uses his private key in conjunction with the first party's public key to encrypt the data. The first party can then use his private key to decrypt the data.[53]

---

patented. Robert Warren, et al., *Frequently Asked Questions (FAQ) List § 2.11.2*, OPENLAW DVD/DECSS FORUM, http://cyber.law.harvard.edu/openlaw/DVD/dvd-discuss-faq.html#ss2.11.2.

43. *See* INTERNET USER IDENTITY VERIFICATION, http://www.pat-rights.com/InternetUserIdentityVerification.html.

44. HDCP encryption key patent. U.S. Patent No. 7,034,891 (filed Jan. 31, 2003).

45. HOW STUFF WORKS, http://computer.howstuffworks.com/encryption.htm (last visited March 22, 2012) ("But the most popular forms of security all rely on encryption, the process of encoding information in such a way that only the person (or computer) with the key can decode it."); Thomas Claburn, *Apple, Dell, Intel Sued Over Encryption Patents*, INFORMATION WEEK (Mar. 31, 2009, 3:20 PM), http://www.informationweek.com/news/global-cio/legal/216402041 (listing examples of encryption patents and the lawsuits that result).

46. VAN TASSEL, *supra* note 23, at 94.

47. *See infra* Section A(3).

48. "Schemes" should, for our purposes, be considered synonymous with "algorithms." *Compare* Schneier, *supra* note 41, at 11 *with* VAN TASSEL, *supra* note 23, at 94.

49. Schneier, *supra* note 41.

50. *See supra* note 47.

51. *Id.*

52. The RSA encryption was named after its creators, Ron Rivest, Adi Shamir, and Leonard Adleman. *See RSA Algorithm*, SEARCHSECURITY, (Aug. 1, 2000), http://searchsecurity.techtarget.com/definition/RSA. For an excellent and easy-to-digest explanation of the algorithm, see http://www.youtube.com/watch?v=b57zGAkNKIc.

53. *Id.*

DRM technology vendors have begun to realize the importance of selecting the right encryption algorithms and implementations. Symmetric-key algorithms are now popular for encrypting content.[54] Examples include RC5 and RC6 from RSA Security, Blowfish and Twofish from Counterpane Labs, and AES, the government successor to DES, which is based on a Belgian algorithm called Rijndael.[55] Public-key algorithms are still used for generating digital signatures and can be used to add further protection to symmetric-key algorithms, by encrypting them again.[56]

These examples show the important role that algorithms play within the encryption/decryption process.[57] Having established the importance of encryption to the DRM landscape, we must now briefly look at why these various encryption schemes come about. This begs the question: If encrypting content is the industry standard for protecting that content from unauthorized users, and an encryption scheme's effectiveness is gauged by the "strength" of its algorithm, how do cryptographers make these encryption algorithms "stronger"?

2. Strength in Numbers

As stated previously, the strength of DRM encryption schemes depend on the "strength" of their respective encryption algorithms.[58] An algorithm's strength is derived from different factors including the length of time it would take a cracker to break the algorithm using a *brute-force-attack*[59] or the algorithm's susceptibility to cryptanalysis.[60] The most basic and obvious measure of an algorithm's strength is the

54. VAN TASSEL, *supra* note 23, at 95.

55. *Id.*

56. *Id.*

57. These are very basic, simple examples of the encryption/decryption process; however, the role of algorithms within the encryption process cannot be downplayed. Algorithms are crucial to the encryption process, and thus DRM as a whole.

58. VAN TASSEL, *supra* note 23, at 90.

59. A "cracker" is a general term used to describe someone who attempts to decrypt or otherwise circumvent the encryption protections on encrypted content. A brute-force-attempt is one example of measures used by crackers. In this method, the cracker uses a program that runs through a massive list of letter and number combinations until the key is found. *See Brute-force Attack*, COMPUTER HOPE (last viewed Jan. 29, 2012), http://www.computerhope.com/jargon/b/brutforc.htm. This tactic is still very much in use today, as users of Sony's Playstation Network discovered when 60,000 accounts were hacked using this very same method. John Leyden, *Sony network ransacked in huge brute-force attack*, THE REGISTER (posted Oct. 12, 2011, 10:37 AM), http://www.theregister.co.uk/2011/10/12/playstation_network_brute_force_attack/.

60. VAN TASSEL, *supra* note 23, at 91–93.

algorithm's key length.[61] The key is the secret number necessary to decrypt the encrypted content; the longer the key, the more difficult it is to discover.[62] If a key can be up to N digits, the total number of possible keys that it could be is 2 to the Nth power.[63] Thus, a key length of 18 returns 262,144 possible keys, only one of which works. While key length is a general provision for determining the strength of an encryption algorithm, it should not be assumed that a longer key is automatically more impervious to cracking than a shorter key. Keys can be broken merely by educated guess, finding patterns within the generated numbers,[64] or even ignoring the encryption entirely and finding holes in other parts of the system.[65] Thus, more complex algorithms, in effect, make it more difficult for a cracker to find patterns or guess the key to decrypt content. Thus, not only is encryption dependent upon algorithms, but encryption's livelihood hinges on its effectiveness, and its effectiveness depends, at least in part, on the strength of its encryption algorithm.

B. The Industry Standard

1. The Chain Rule

Behind DRM's forward line of troops—encryption algorithms, stands a second and equally complicated array of defenders—licensing agreements.[66] Encryption and decryption of content requires a license of the relevant encryption technology.[67] In order to completely protect digital content, every "link" of the "chain," from content producer to consumer, must remain secure. This is done through a complex set of licenses between encryption technology producers and digital content transmitting technology producers.[68] The device connections between these links must be licensed with the proper encryption and decryption keys from the encryption producer.[69] These links are more intricate than one may initially realize. In theory, every link must maintain the

61. *Id.*

62. *See* VAN TASSEL, *supra* note 23, at 91.

63. *Id.*

64. Many cryptosystems involve random number generators, which can sometimes exhibit patterns. *Id.* at 92.

65. *Id.* at 92–93.

66. As before with encryption, this is not meant to be all-inclusive, but rather a brief overview of licensing agreements.

67. Marks and Turnbull, *supra* note 22.

68. *Id.* at 13–24.

69. *Id.*

digital content's encryption as the content is passed to the next link.[70] With this in mind, take the example of a consumer watching a legitimately purchased DVD. The DVD itself must be encrypted, then the digital content contained therein decrypted by the DVD player, then re-encrypted by the DVD player as it travels through the DVD player's memory to the output jacks,[71] then finally decrypted within the ports connecting the output cables to the television.[72] Unlicensed devices may transmit encrypted content, so long as they do not decrypt the content in doing so.[73] The theory behind all of this encryption and decryption is that every link along the chain must be protected, lest a tech-savvy third party tap into the chain and copy un-encrypted digital content, thus circumventing the whole DRM system entirely. Standardizing DRM systems is a complex task, involving the intertwining interests of not just the content producers and end consumers, but also the computer, broadcasting, and telecommunications industries.[74] This complex licensing-technology hybrid guarantees that, at least in theory, digital content moving from point A to point B, through any medium, will have some sort of protection from being copied, whether that content is on DVDs, digital downloaded music, or other types of digital content.[75] "In order to be successful on the mass-market, DRM technologies have to be integrated into consumer devices in a standardized way . . . from the creation of content to its consumption by individual users, it must be assured that no single device or component can transmit the content in an unencrypted form, as this would compromise the security of the DRM

70. *Id.* at 11. Marks and Turnbull describe the devices and services that "are capable of playing back, recording and/or transmitting" secure digital content as "way stations" that must maintain content as securely as it was received . . . [that further] may not pass content which has been legitimately decrypted through either analog or digital connections to other devices and systems without the appropriate protections." *Id.*

71. For examples of the types of technology used to transmit and/or store encrypted digital data, see Bechtold, *supra* note 15, at 326 n. 11 ("digital container") and 327 ("Rights locker architectures") n. 12 (describing a rights locker architectures with sources for further information). As this paper deals primarily with encryption, expounding upon these in any further detail would prove irrelevant to its focus.

72. For a lengthy, fun example of a DVD's encryption licensing agreement for DVD players, see "Advanced Access Content System (AACS) Adaptor agreement," *available at* http://www.aacsla.com/license/AACS_Adopter_Agrmt_090605.pdf, or the plethora of other licensing agreements utilized by AACS, *available at* http://www.aacsla.com/license/.

73. Marks and Turnbull, *supra* note 22, at 11–13. To do so would violate the Digital Millennium Copyright Act. *See infra* section C.

74. Bechtold, *supra* note 15, at 330.

75. *See generally* Marks and Turnbull, *supra* note 22, at 12–25.

system."[76]

2. Sine on the Dotted Line

In addition to these technological licensing agreements are usage contract licensing agreements. Usage contracts tend to follow a similar pattern.[77] This pattern is that, prior to accessing the content, a consumer must agree to certain rules limiting the extent of that consumer's use of that content. Usage contracts take various forms, from a standard "Terms of Service" agreement to "End User License Agreement[s]".[78] Usage contracts provide another layer of protection for content producers and their licensees, as these contracts add one or more claims for breach of contract to circumventing or decrypting DRM protections. This adds the additional complication of breach of contract versus copyright infringement claims, actual damages versus disgorgement damages, and other issues that arise when a licensing agreement is breached.[79]

3. The Prime Variable

The slew of protections available to content producers does not end with contracts and the legal ramifications of breach of contract or breach of the licensing agreement. The big guns in DRM's arsenal, at least in regards to digital content that is copyrightable, is the Digital Millennium Copyright Act (DMCA).[80] The DMCA makes it not just a felony, but a very costly felony, to circumvent DRM protections on copyrighted material.[81]

The DMCA prohibits the circumvention of "a technological measure that effectively prevents access to a [copyrighted work[82]]."[83] Furthermore, the DMCA also prohibits the importation, manufacture,

76. Bechtold, *supra* note 15, at 330.

77. *See id.* at 339.

78. *Id.* at 339–40.

79. *See* Omri Ben-Shahar, *Damages for Unlicensed Use* 3–9 (Sept. 2010) (unpublished working paper, on file with the University of Chicago Institute for Law and Economics and *available at* http://www.law.uchicago.edu/files/file/534-obs-damages.pdf).

80. 17 U.S.C. § 1201 (2006) (hereinafter "DMCA").

81. 17 U.S.C. § 1201(a); *see also* 17 U.S.C. § 1203(c) (detailing the hefty fines associated with circumvention in violation of the DMCA).

82. It is important to note that in order for the circumvention to be of the type prohibited by the DMCA, the underlying work *must* be copyrighted or copyrightable. *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 534–44 (6th Cir. 2004).

83. 17 U.S.C. § 1201(a)(1)(A).

trafficking, or distribution of such a technological measure.[84] It is without question that most DRM encryptions would constitute a "technological device,"[85] and therefore, decrypting them would constitute circumvention.[86] It is important to remember that the DMCA itself only prohibits the *access* of copyrighted work through the process of circumvention of a technological measure to prevent such.[87] So insofar as mere decryption of the encryption algorithms on copyrighted work is concerned, the DMCA, in conjunction with licensing agreements forbidding circumvention of DRM, gives real "teeth" to the punishments available for would-be encryption crackers. If one were to decrypt the copyrighted content and thereafter distribute it somehow, then the double-whammy of violation of the DMCA and copyright infringement would be available remedies.

It is important to reiterate that the first link in the complex DRM technology and legal chain is encryption. Encryption is the crucial technology upon which the elaborate DRM system rests. Without encryption, a tech-savvy consumer would be able to access unprotected digital content and do whatever he wishes with that content, be it copy it, distribute it, or any of the other habits legally delegated to copyright holders and their respective licensees.[88] Encryption, as stated previously, is a heavily math-based science, implemented solely through algorithms. It is encryption's necessity to the DRM system as a whole that makes it so important. It is its complexity that makes it relevant. But it is this same complexity that presents issues for DRM patent-holders in the post-*Bilski* patent world. It is with this in mind that one must next look at the issues of patentability in regards to DRM.

III. THE PATENT-DRM CONUNDRUM

Section 101 of the Patent Act defines the subject matter that can be patented as "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof

84. 17 U.S.C. § 1201(a)(2) (2006).

85. *See* 17 U.S.C. § 1201(a)(3)(B). ("[A] technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.")

86. *See* 17 U.S.C. § 1201(a)(3)(A) ("[T]o 'circumvent a technological measure' means to descramble a scrambled work, to *decrypt an encrypted work*, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner.") (emphasis added).

87. *See* 17 U.S.C. § 1201(a)(1)(A) (2006).

88. *See* 17 U.S.C. § 107 (2006).

. . ."[89] Supreme Court precedent has determined that such an expansive term ("any") indicated that Congress contemplated that patent subject matter would be broad in scope, and that "ingenuity should receive a liberal encouragement."[90] Section 100(b) defines a "process" as "a new use of a process, machine, manufacture, composition of matter, or material."[91] There are three specific exceptions to the otherwise broad patentable subject matter: "laws of nature, physical phenomena, and abstract ideas."[92] But precedent on the matter has not been consistent or particularly understandable.

A. Knowledge and Not On Numbers[93]

The courts have historically struggled with the limits of patentability in this context. The difficulty has been determining whether inventions incorporating algorithms are within patent's bounds, or alternatively, fall into the exceptions to patentable subject matter and are thus non-patentable. The waxing and waning of the courts' willingness to broaden or constrict patent's scope in this regard has been tumultuous, and opinions have been less than consistent and strayed from hammering out any bright-line rules. What is an interesting point of guidance are the various tests implemented by the courts, and the Supreme Court's reluctance to formally adopt any of them. A brief examination of these decisions will show not just what was and became at stake in the ultimate question of patentability of algorithmic technology, but will also show the conflicting precedents available to the *Bilski* Court, as well as the back-and-forth between the federal courts and the Supreme Court.

1. Arithmus ex Machina

In *Gottschalk v. Benson*,[94] the United States Supreme Court examined a patent application involving claims as to a method for converting binary-coded-decimal numerals into pure binary numerals on any general-purpose computer.[95] The Court, in its determination,

89. 35 U.S.C. § 101 (2006).

90. Diamond v. Chakrabarty, 447 U.S. 303, 308 (1980).

91. 35 U.S.C. §100(b) (2006).

92. *Diamond*, 447 U.S. at 309.

93. THOMAS BENFIELD HARBOTTLE, DICTIONARY OF QUOTATIONS (CLASSICAL) 373 (2d ed. 1958) (Plato is quoted as having said "a good decision is based on knowledge and not on numbers.").

94. Gottschalk v. Benson, 409 U.S. 63 (1972).

95. *Id* at 64.

discussed the very issue of patentability of the algorithm involved,[96] finding that algorithms should be considered with the same scrutiny and wariness as other "phenomena of nature, though just discovered, mental processes, and abstract intellectual concepts," explaining that such are "the basic tools of scientific and technological work."[97] The Court found that this abstract idea (the algorithm), tied with no machine in particular (in this case, any general computer), would pre-empt the mathematical formula and be a patent on the algorithm itself.[98] Interestingly, the Court in finding this determination briefly touched on language that would be a motif in the patentability struggle. The Court said that "[t]ransformation and reduction of an article 'to a different state or thing'" is the clue to the patentability of a process claim that does not include particular machines."[99] This language would echo around the debate for the next thirty years. The Court had thus given some clarity as to what was *not* patentable, in this case an algorithm for converting numbers from one form to another, and categorized that algorithm as being within the exceptions to patentability, but gave no concrete definition for "abstract," "phenomena of nature," or any of the like.

The United States Court of Customs and Patent Appeals (CCPA) used this guidance in *In re Chatfield*.[100] While being careful to not be too focused on the term "algorithm,"[101] the court found that a method for improving the operating efficiency of a computing system containing a mathematical equation was not, in its entirety, non-patentable, merely because a portion of the claim is a non-patentable algorithm.[102] The court also held that the prior argument that a "process patent must either be tied to a particular machine or apparatus or must operate to change articles or materials to a 'different state or thing'" was not determinative.[103]

The Supreme Court contributed some clarity on the subject with its ruling in *Parker v. Flook.*[104] In *Flook*, a case involving a claim in which

96. *Id.* at 64–67.

97. *Id.* at 67.

98. *Id.* at 70.

99. *Id.*

100. *In re* Chatfield, 545 F.2d 152 (C.C.P.A 1976).

101. *Id.* at 156 n.5. "Over-concentration on the word 'algorithm' alone, for example, may mislead . . . . It would be unnecessarily detrimental to our patent system to deny inventors patent protection on the sole ground that their contribution could be broadly termed an "algorithm."

102. *See id.* at 157–58.

103. *Id.* at 156 n.4 (quoting Gottschalk v. Benson, 409 U.S. 63, 71–72 (1972)).

104. Parker v. Flook, 437 U.S. 584 (1978).

the only novel part of the claim was an algorithm,[105] the Court reiterated the unpatentability of mathematical formulae, despite post-solution applications, as an algorithm constitutes a "law of nature."[106] Citing its holding in *Benson*, the Court, yet again, covered the general rule of unpatentability of abstract principles,[107] and again mentioned, without holding determinative, what would become the machine-or-transformation test for determining process invention patentability.[108] The Court also remarked that while the subject matter as a whole must be considered,[109] "if a claim is directed essentially to a method of calculating, using mathematical formula, even if the solution is for a specific purpose, the claimed method is nonstatutory."[110]

2. "As a Whole"

In 1981, the Supreme Court backtracked a bit, in its ruling in *Diamond v. Diehr,*[111] a case involving a claim for a process for curing raw, uncured synthetic rubber into cured products.[112] The claim involved an algorithm, and while it involved a computer, the Court found that aspect not determinative as to its patentability.[113] Rather, the Court found, oddly enough, that taken "as a whole,"[114] and considering the "novelty of the combination they represent[],"[115] it was worthy of patent protection, "even though some or all of its elements are not 'novel.'"[116] This was despite the fact that the only novel part of the claim was the steps invoking the algorithm, and the algorithm itself.[117] Furthermore, the Court argued, dissecting the claims into old and new elements in such a way as done in *Flook* would render all inventions

105. *See id.* at 591 ("The process itself, not merely the mathematical algorithm, must be new and useful.").

106. *Id.* at 589.

107. *Id.*

108. *Id.* at 588 n.9 ("An argument can be made, however, that this Court has only recognized a process as within the statutory definition when it either was tied to a particular apparatus or operated to change materials to a 'different state or thing.'").

109. *Id.* at 594.

110. *Id.* at 595 (quoting *In re* Richman, 563 F.2d 1026, 2030 (1977)).

111. Diamond v. Diehr, 450 U.S. 175 (1981).

112. *Id.*

113. *Id.* at 181.

114. *Id.* at 188.

115. *Id.* at 193 n. 15 (quoting Great A. & P. Tea Co. v. Supermarket Equipment Corp., 340 U.S. 147, 152 (1950)).

116. *Id.* n. 15.

117. *See id.* at 192–93.

non-patentable.[118] In a scathing dissent, Justice Stevens points out the obvious discrepancies between this holding and the decisions in *Flook*[119] and *Benson.*[120] Justice Stevens pointed out that the only novel part of the claim was the algorithm[121], and that the process as a whole, as the majority stated, was not novel, in that the algorithm was applied to a computer to determine the amount of time that the rubber molding press should remain closed during the rubber-curing process.[122] It is with this decision that we see the paradigm shift towards a broader patent scope for algorithm-implemented inventions, possibly from the reasoning in *Diamond v. Chakrabarty*,[123] which gave the legislative intent to grant patent protection for "anything under the sun that is made by man."[124] Of course, the issue here is whether a new algorithm applied to a non-novel claim constituted something "made by man."[125]

3. A Slippery Slope

Yet again, the scope was broadened in the landmark cases *In re Alappat*[126] and *State Street Bank*,[127] the latter of which is attributed as being the catalyst for the "patent boom" that still continues.[128] *Alappat*'s invention involved a "rasterizer"[129] that performed the same overall function as prior art rasterizers; however, it did so "in a different way" thanks to the implementation of the new algorithm.[130] The Court of Appeals for the Federal Circuit cited the struggle the Supreme Court has had in pinning down and articulating a rule for mathematical subject

118. *Id.* at 189 n. 12.

119. *Id*. at 193 (Stevens, J., dissenting).

120. *Id.* at 201–02.

121. *Id.* at 208 ("[T]he only difference between the conventional methods of operating a molding press and that claimed in the application rests in those steps of the claims which [sic] relate to the calculation incident to the solution of the mathematical problem or formula used to control [the heating process].").

122. *See id.* at 208–09.

123. Diamond v. Chakrabarty, 447 U.S. 303 (1980).

124. *Id.* at 309 (citing S. Rep. No. 1979, 82d Congress., 2d Sess., 5 (1952)).

125. I think it is safe to assume that it is "under the sun."

126. *In re* Alappat, 33 F.3d 1526 (Fed. Cir. 1994).

127. State St. Bank & Trust Co. v. Signature Fin. Group, 149 F.3d 1368 (Fed. Cir. 1998) (hereinafter "State Street").

128. Lori E. Lesser, *We've Got Algorithm – Software Patents Boom*, FINDLAW, http://library.findlaw.com/1999/Aug/1/130894.html (last visited Jan. 14, 2012).

129. *Alappat*, 33 F.3d at 1537 (The court itself summarizes what Alappat's particular invention did: "in lay terms, the invention is an improvement in an oscilloscope comparable to a TV having a clearer picture."); *id*. at 1538 (The term "rasterizer" is a machine used specifically in claim 15.).

130. *Id.* at 1540–1542.

matter,[131] and found that the claim produced a "useful, concrete, and tangible result" that was "not so 'abstract and sweeping' that it would 'wholly pre-empt' the use of any apparatus employing the combination of mathematical calculations recited therein."[132] Essentially, this overturned the previous rulings that held software non-patentable, provided that it physically transformed the underlying subject matter.[133] This ruling cracked open the door to software patents even more, as the court found that a contrary ruling would render computers operating pursuant to software "may represent patentable subject matter, provided, of course, that the claimed subject matter meets all of the other requirements of Title 35."[134]

State Street opened the floodgates to software patenting. Reiterating this "useful, concrete and tangible result," language in *Allapat*, the court in *State Street* found section 101's bounds to be broad.[135] The court supported this contention by finding that the "repetitive use of the expansive term 'any' in §101 shows Congress's intent not to place any restrictions on the subject matter for which a patent may be obtained beyond those specifically recited in §101."[136] It was with this mindset that the court tackled the issue presented before it, which was one for a data processing system for implementing various aspects of administering investments for a mutual funds administrator.[137] The court found that the Freeman-Walter-Abele[138] test, as applied by the district court, was improper for determining the patentability of the data processing system.[139] The court argued that the test was misleading, because a patent claim "employing a law of nature, natural phenomenon, or abstract idea is patentable subject matter even though [the exceptions listed] would not, by [themselves] be entitled to such

131. *Id.* at 1543.

132. *Id.* at 1544 (quoting Gottshalk v. Benson, 409 U.S. 63, 68–72 (1972)).

133. *Id.* at 1543.

134. *Id.* at l545.

135. State St. Bank & Trust v. Signature Fin. Group, 149 F.3d 1368, 1373 (1998).

136. *Id.* The court also cited the Supreme Court's own words in *Diamond v. Chakrabarty*, 447 U.S. 303, 309 (1980), that Congress intended §101 to cover "anything under the sun that is made by man." *Id.*

137. *See id.* at 1370.

138. *See In re* Bilski, 545 F.3d 943, 958–59 (Fed. Cir. 2008); *State Street*, 149 F.3d at 1374–75 (This test is only mentioned in passing, for the sake of brevity. To delve further into it would go outside of the necessities of this Comment. Plus, the court in *In re Bilski* and *State Street* did away with this test, thus making it a non-issue in any further determination on encryption patentability.).

139. *State Street*, 149 F.3d at 1373–74.

protection."[140] This circular argument applies also to algorithms, the court explains.[141] This, the court reasons, follows from the new rule after *Diehr* and *Alappat*, and under that rule, the claim is still patentable subject matter if the claim produces "a useful, concrete and tangible result."[142] Thus, the court concludes, the transformation of data, for example, through an algorithm, produces a "useful, concrete and tangible result,"[143] regardless of the physical requirements stated in *Alappat*.[144]

The result of this decision was a "land rush mentality" of patent applications, which swarmed the Patent and Trademark Office (PTO) and Federal Circuit.[145] What followed was an "endless rush" of patents, from the mundane to the complex.[146] This overload has since overburdened the PTO, a warning prophesized long ago by Justice Stevens in his dissent in *Diehr* as reasoning for limiting the scope of patentability for process claims incorporating abstract ideas.[147] Regardless, the culmination of these decisions presented a broad area of patentability for an already overburdened patent office, finding difficulty in keeping up with the demands of the growing digital revolution.[148]

Thus the courts have had difficulty defining precisely where to draw the line on patent claims involving algorithms. Though, this is not to say that some clarity cannot be gleaned from the reaping in this area. There exists the machine-or-transformation test, slowly defined throughout this era to mean that a process claim that involves an abstract idea, such as an algorithm, is patentable if it either is tied to a particular machine or apparatus, or transforms material from one state to another. Alternatively, one could look at the holdings in *Alappat* and *State Street* and look at the patent claims as a whole, and see if it produces something that would be considered "useful, concrete, and tangible."[149]

---

140. *Id.* at 1374.

141. *Id.*

142. *See id.* (citing *In re* Allapat, 33 F.3d 1526, 1544 (Fed. Cir. 1994)).

143. *Id.* at 1373.

144. *See Allapat,* 33 F.3d 1526

145. Jay Dratler, Jr., Article: Alice in Wonderland Meets the U.S. Patent System, 38 AKRON L. REV. 299, 303 (2005).

146. *See id.*

147. Diamond v. Diehr, 450 U.S. 175, 197–98 (Stevens, J., dissenting).

148. Martha Groves, *A Patent Dispute; Lawsuit Raises a Hot Issue in Exploding Technology*, L. A. TIMES, Feb. 14, 1994, at D1.

149. *Allapat*, 33 F.3d 1526; State St. Bank & Trust Co. v. Signature Fin. Group, 149 F.3d 1368 (Fed. Cir. 1998).

4. A Solution?

It was with this multicolored backdrop that Bernard Bilski entered the patent arena. In the 1990s, Bilski developed a method for using hedge contracts to reduce the risk that a commodity's wholesale price might change, and applied for a patent.[150] Bilski's patent application was rejected in September 2006, as the claimed method was ruled to be merely an abstract idea by the Patent Examiner at the USPTO, and Bilski appealed to the Federal Circuit in early 2007.[151]

The Federal Circuit handed down its ruling on October 30, 2008, in *In re Bilski*.[152] In this decision, the Federal Circuit, seeing the numerous tests and commentary on the issue, decided to adopt the machine-or-transformation test as the sole means for testing the patentability of a process claim.[153] The court reconciled the conflicting commentary by finding that this test could explain the finding in the Supreme Court's holdings.[154] The court then systematically examined and rejected the remaining tests for patentability, ultimately concluding that the machine-or-transformation test was the best, and *only* test to be applied.[155]

What this long romp through the case law history has shown is the difficulty and frustration experienced by the courts in finding an appropriate means for determining the patentability of claims involving abstract subject matter. The machine-or-transformation test was a conclusion reached out of necessity by the Federal Circuit. The need for *some* kind of ultimate test seemed necessary to not only curb the growing number of patent applications and relieve some of the burden on the USPTO[156] and Federal Circuit that resulted from *State Street*, but also to prevent the stymieing of progress by overbroad patent claims and patent trolls.[157] Arguably, this rationale proved successful. From

150. Steven Seidenberg, *Bilski's Battle*, INSIDE COUNSEL (Oct. 20, 2007), http://www.insidecounsel.com/2007/10/01/bilskis-battle.

151. *Id.*

152. *In re* Bilski, 545 F.3d 943 (Fed. Cir. 2008).

153. *Id.* at 956.

154. *See id.* at 956 (applying the test to decisions in *Benson* and *Flook*); *see id.* at 957 (applying the test to Diehr).

155. *Id.* at 956–64.

156. *See generally* Kevin Coughlin, "Technology Upends the Meaning of Invention Patent Requests Shift to Ideas, Know-How," THE STAR LEDGER (Newark, NJ), Mar. 12, 2000, at 1.

157. And was successful. *See* Austin Modine, "US Court Blocks Amazon-style Patent Trolls," The Register, (Oct. 31, 2008), http://www.theregister.co.uk/2008/10/31/us_court_of_appeals_federal_circuit_business_method_patent_decision/.

October 30, 2008 (the date of the *Bilski* holding) until March 8, 2010, out of the 140 cases to the Board dealing with, *inter alia*, a section 101 rejection, the Board held that a claim was non-statutory subject matter 78.3% of the time.[158] Maybe the USPTO and interested onlookers had finally gotten some respite.

B. What the Circuit Giveth, the Supreme Court Taketh Away

1. Division of the Issues

The sigh of relief would not echo long, however. When the Supreme Court granted certiorari in July 2009, the arena was set. . . the fighters in their corners, and the peasants had gathered round to cheer for their respective champion. Whether Bernard Bilski was a hero or a villain depended on which side of the aisle one sat. Some saw him as continuing the status quo of the broad patent regime, while others simply saw him as an inventor trying to protect his creation. Regardless, the case was the culmination of decades of debate and frustration, and the Intellectual Property world was watching.

What they got instead, on June 28th, 2010, in *Bilski v. Kappos*,[159] was something of a letdown. Despite *In re Bilski*'s comprising a colossal 72 pages (including multiple dissents), the Supreme Court decided the complex issue in as few as 41 pages.[160] The Court held that while the machine-or-transformation test is "useful" and "important" and "an investigative tool" for determining process claims' patentability, it "is not the *sole* test."[161] Further, the Supreme Court ruled that business method patents were abstract,[162] and thus not patentable.[163] While this answered an important question in the debate, namely the patentability of algorithmic business method patents, it failed to give *any* clarity on arguably the biggest issue in the debate—the patentability of other algorithm-dependant processes, such as software and encryption schemes. The Supreme Court thus ruined yet another attempt by the lower courts to not only ease the patent workload for themselves and the USPTO, but also ruined another attempt by the Federal Circuit to prevent patent abuse and alleviate the alleged burden on innovation by

158. Peter Ludwig, *Machine-or-Transformation Test Hits the Board: Patent-Eligible Subject Matter Following Bilski*, 92 J. PAT. & TRADEMARK OFF. SOC'Y 139, 141 (2010).

159. Bilski v. Kappos, 130 S. Ct. 3218 (2010).

160. *See In re* Bilski, 545 F.3d 943 (Fed. Cir. 2008); *Bilski*, 130 S. Ct. 3218 (2010).

161. *Bilski*, 130 S. Ct. at 3227 (emphasis added).

162. *Id.* at 3231.

163. *Id.*

overbroad patent drafting.

2. Remainder Questions

One takeaway is that DRM might be in better standing had the Federal Circuit's ruling won out. Clearly, the machine-or-transformation test presents a tougher standard, and one that an algorithm-specific technology might not have been able to overcome. Some DRM encryption schemes and distribution processes are not restricted to one machine or apparatus,[164] and does the encryption and subsequent decryption of digital content really "transform material from one form to another?" It is a tough question to answer. In *Grams*, the court found that the algorithm involved "[did] not change any aspect of the *physical* process" of the material present.[165] This begs the question as to whether encryption itself changes the *physical* aspect of the data, merely by scrambling it and rendering it unreadable.

The issue regarding DRM encryption is not necessarily the rejection of the machine-or-transformation test, itself; rather, it is the damaging commentary in *Bilski v. Kappos* that endangers DRM encryption's survival. "Rather than adopting categorical rules[166] that might have wide-ranging and unforeseen impacts, the Court resolves this case narrowly on the basis of this Court's decisions in *Benson, Flook,* and *Diehr*. . . ."[167] The Court reiterated the three exceptions to section 101's patentability principles, those being "laws of nature, physical phenomena, and abstract ideas."[168] There is an unavoidable similarity between *Benson* and DRM encryption, and the Court's reverence to the former calls the patentability of the latter into question. In *Benson*, the Court observed a patent on a process for converting numerals to pure binary numerals would have, in effect, been a patent on the algorithm/formula itself.[169] It stands to reason then, that given encryption's very function—the transformation of digital content to unreadable content, and back to digital content— the Court's deference to *Benson* might call into question encryption's patentability. The Board often states that a claim fails to transform a particular article

164. Take for example, encryption on eBook files, which are readable on a computer, an eBook reader, a cell phone, or a tablet device.

165. *In re* Grams*,* 888 F.2d 835, 840 (Fed. Cir. 1989) (emphasis added).

166. Oh God forbid such a thing!

167. Bilski v. Kappos, 130 S. Ct. 3218, 3229 (2010).

168. *Id.* at 3225.

169. *Id.* at 3230.

because the data does not represent "physical" and "tangible" objects.[170] This also directly clashes with the chance of the machine-or-transformation test saving encryption from falling outside of section 101's bounds. The Court also cites *Flook*, describing the claim therein as containing nothing novel or innovative, save "reliance on a mathematical algorithm."[171] Taking this into consideration, it seems likely that DRM encryption schemes, which are novel only insofar as they contain new, "stronger" algorithms,[172] would likely be non-patentable subject matter, too. The Court finally accredited *Diehr* with its determination that business method claims are non-patentable.[173] There is no guarantee that the reasoning in *Diehr* will prove successful with DRM encryption schemes either, as it is a point of debate as to whether the claim in *Diehr* was ruled patentable simply because it involved an industrial process, or because it transformed matter from one form to another, as the decision is not entirely clear. Even considering DRM encryption "as a whole," per the lesson learned in *Diehr* and stated in *Bilski*, it is unlikely that, given the surrounding prior art and major role that the algorithms play in encryption, it will pass patent muster. Thus, DRM exists in a kind of grey area, not clearly qualifying for any of the numerous tests passed down through the precedent. Of course, the Supreme Court's reluctance to clarify *anything* on the matter only further complicates the debate.

The difficulty really lies in meting out just "how much" of a role the algorithm may play in a patentable claim, given the numerous tests available. Indeed, the USPTO itself needed help in determining how to approach this issue in *Bilski*'s wake.[174] In the case of DRM encryption schemes, none of these tests really seem to pass. Is it a "useful, concrete and tangible result"[175] to encrypt and/or decrypt digital content? Does encryption's act of encrypting data "transform" it from one state to another?[176] Must encryption be tied to a particular machine?[177] Finally,

---

170. Ludwig, *supra* note 158, at 154.

171. *Bilski*, 130 S. Ct. at 3230 (citing Parker v. Flook, 437 U.S. 584, 585–86 (1978)).

172. *See supra* Section A(2).

173. *Bilski*, 130 S. Ct. at 3230.

174. Ryan Paul, *As USPTO evaluates Bilski, Red Hat says end software patents*, ARS TECHNICA, http://arstechnica.com/tech-policy/news/2010/09/as-uspto-evaluates-bilski-ruling-red-hat-says-end-software-patents.ars?utm_source=rss&utm_medium=rss&utm_campaign=rss (last visited Mar. 22, 2011).

175. State St. Bank & Trust Co. v. Signature Fin. Group, 149 F.3d 1368, 1374 (Fed. Cir. 1998).

176. Per the second prong of the "machine-or-transformation" test.

177. Per the first prong of the "machine-or-transformation" test.

where do the encryption algorithms fit into the equation, and, if they are the only novel part of an encryption device, does that render the remainder of the application unpatentable? Will DRM encryption survive in a post-*Bilski* world?

IV. SOLVING THE EQUATION

The first step to solving this problem lies in the term "algorithm." In *Benson*, "algorithm" was defined as "a procedure for solving a given type of mathematical problem,"[178] a definition echoed in *Flook*[179] and *Diehr*.[180] This definition creates a paradox. Algorithms, by their very nature as problem solvers,[181] are useful and have application somewhere,[182] thus meeting the criteria in *State Street.*[183] In spite of that, the Court has said time and time again that algorithms are abstract ideas, and thus outside of patent bounds.[184]

One solution is that the Supreme Court should either re-define "algorithm," to expressly state what types of algorithms are not patentable, or it should just do away with the algorithm exception altogether. The former would present a circular problem of defining what types of "former" algorithms are abstract, thus warranting the "new" "algorithm" label within statutory limits. This could be more of a problem than it is worth, having expert witnesses and lengthy briefs explaining why one algorithm is "newer" than another algorithm, ad infinitum. Doing away with the notion that algorithms themselves are considered "abstract" would be doable if algorithms themselves were not patentable within larger claims, regardless of the surrounding prior art. Ultimately, there must be some ruling as to whether algorithms' role has changed in society, and whether they are now unique creations, worthy of patentability,[185] or whether they still remain "abstract" natural

178. Gottschalk v. Benson, 409 U.S. 63, 65 (1972).

179. Parker v. Flook, 437 U.S. 584, 586 (1978).

180. Diamond v. Diehr, 450 U.S. 175, 186 (1981).

181. Per the definitions provided by *Benson*, *Flook*, and *Diehr*, *supra* notes 178–80.

182. Allen Clark Zoracki, *When is an Algorithm Invented? The Need for a New Paradigm for Evaluating an Algorithm for Intellectual Property Protection*, 15 ALB. L.J. SCI. & TECH. 579, 590 (2005) (hereafter "Zoracki Article").

183. State Street Bank & Trust v. Signature Fin. Group, 149 F.3d 1368, 1374 (Fed. Cir. 1998).

184. Bilski v. Kappos, 130 S. Ct. 3218, 3229 (2010).

185. This may be a question more appropriately answered by a more engineering-oriented mind, as engineers with whom I have spoken have unanimously echoed the sentiment that a complicated algorithm applied to a useful function is itself creative and useful enough to warrant a patent.

phenomena.

Another option would be to cave into the open source demands[186] and do away with software patenting, and thus encryption patenting, altogether. Proponents for such argue that information is "the oxygen of the modern age," and thus needs to be free.[187] They argue that software and other information products do not provide any new information to the public, and thus a patent bargain, traditionally a "bargain" between the patentee and the public, presents a one-sided bargain.[188] Further, copyright protection exists for some software code as well,[189] so it could be argued that encryption algorithms fall within the realm of copyrights. This is the best method of achieving the ultimate goals of intellectual property law, believes prominent IP scholar Mark Lemley, giving it as little protection as possible.[190] Others argue that DRM may render traditional copyright laws completely irrelevant.[191]

V. CONCLUSION

Aside from an act of Congress further limiting or expanding the current scope of section 101, there are limited options for the courts in determining whether encryption schemes are patentable or not, and if not, what remedy exists to allow them to be, if necessary. If they are patentable, then the problem is what role algorithms play, and where to draw the line in regards to determining what constitutes a "novel" algorithm or an old, unpatentable algorithm. If they are not patentable, then the DRM industry is done for, or had better lobby for some contrary legislation. While there is no easy fix, as evidenced by, if nothing else, thirty years of arguing over the subject, it is clear that something must be done. Patent law is simply falling behind the technology it was intended to protect, which could prove very hazardous with the digital age screaming onward at breakneck speed. In regards to DRM encryption, a failure to do so could prove fatal to the DRM

186. *See* Paul, *supra* note 174.

187. Kristen Osenga, *Information May Want to be Free, but Information Products do not: Protecting and Facilitating Transactions in Information Products*, 30 CARDOZO L. REV. 2099, 2100 (2009).

188. *Id.* at 2106–07.

189. *Id.* at 2107.

190. Gary Miller, *On Federal Preemption of Contractual First Sale Waivers*, BOSTON COLLEGE INTELL. PROP. & TECH. FORUM 1 (Sept. 23, 2010), http://bciptf.org/wp-content/uploads/2011/07/2-ON-FEDERAL-PREEMPTION-OF-CONTRACTUAL-FIRST-SALE-WAIVERS.pdf.

191. Joseph H. Sommer, *Against Cyberlaw*, 15 BERKELEY TECH. L.J. 1145, 1223 (2000).

industry, for without patents to provide legal protections for licensing the encryption keys and devices, what incentive is there to produce them at all? This could have disastrous effects on not only the DRM industry, but also the various media and content outlets that rely upon that industry, which would be unable to protect digital content from unauthorized access and distribution. This danger is not limited to digital content providers, but also those who use encryption to buy and sell online, create digital signatures, and send confidential or sensitive information on secure networks. While mathematics might be "God-given," or naturally occurring phenomena, algorithms must lie somewhere between the human and the divine, and the courts must draw this line closer towards the former, or else risk bringing down the whole system. As the world continues to shrink, the need to protect information will continue to expand, and the role of DRM will become more and more important. Let us hope that for once law can match pace with technology.

JEREMY R. HAGER[*]

[*] B.A., History, Auburn University, 2006; J.D. Candidate, Marquette University School of Law, 2011. Thanks to Professors Irene Calboli, Bruce Boyden, and Kali Murray for their assistance. I would also like to thank Nicholas Smith for his advice on a topic I found very difficult. Thanks as well to my family and Rebekah Everett for their support. Yes, the math puns are intentional. War Eagle.