THE ANTIQUITY OF ALGORITHMIC PATENTS

STEVEN M. BELLOVIN*

Software patents have long been controversial. Although they are accepted today, if only implicitly—there is nothing in the patent statute that explicitly permits them—the Patent Office and the courts have gone back and forth on the patentability of software. In the early 20th century, though, patents were routinely issued for what today would be termed software—more precisely, programs—even though this was long before computers existed. I recount some of this history and give several examples of such patents, including objections (or the lack thereof) from patent examiners per the file histories—and later examples of where similar claims were disallowed by the courts. Policy arguments aside, the precedents suggest that algorithmic patents should be allowed, but their precise scope has never been clearly delineated.

* Steven M. Bellovin is the Percy K. and Vida L.W. Hudson Professor of Computer Science at Columbia University and affiliate faculty at Columbia Law School. I am grateful for the assistance of archivist Robert Beebe at the National Archives and Records Administration in obtaining patent history files. James Grimmelman, Ben Lee, John Levine, Clarisa Long, Sunoo Park, and Pamela Samuelson made many useful suggestions.

Software patents have long been controversial. Apart from the questions of policy and practicality—and they are many—it was long unclear if they were actually permitted by statute. That said, software patents—more precisely, algorithmic[1] or software-like patents, since they far antedate computers—were long accepted, despite minimal changes to the relevant text in the Patent Act.[2]

I will not recount the policy arguments here—this is an article on legal history—save to note that they focus on conceptual difficulties and on patents as a drag on innovation, especially for open-source software.[3] Practicality arguments center on the intense creativity in every part of a computer program, creativity possessed by every person "having ordinary skill in the art."[4] Most such algorithms are never "described in a printed publication";[5] while the code may be "in public use"[6] or "on sale,"[7] users do not know this. Indeed, software license terms often explicitly prohibit trying to find out.[8]

Beyond that, software patents have often been held to be invalid under relevant statutes, as "abstract" ideas or "mental processes," which

---

[1] *Algorithm*, A DICTIONARY OF COMPUTER SCIENCE 16 (7th ed. 2016) (defining "algorithm" as:

> A prescribed set of well-defined rules or instructions for the solution of a problem, such as the performance of a calculation, in a finite number of steps. Expressing an algorithm in a formal notation is one of the main parts of a program; much that is said about programs applies to algorithms, and vice versa)

(note the correct omission of today's colloquial meaning: the software that produces the opaque behavior of today's complex systems, e.g., search engines).

[2] 35 U.S.C. §§ 100–212 (2018).

[3] *See, e.g.*, Simson L. Garfinkel, Richard M. Stallman & Mitchell Kapor, *Why Patents Are Bad for Software*, 8 ISSUES SCI. & TECH. 50 (1991). *But see also, e.g.*, Martin Campbell-Kelly, *Not All Bad: An Historical Perspective on Software Patents*, 11 MICH. TELECOMM. & TECH. L. REV. 191 (2005); Donald S. Chisum, *The Patentability of Algorithms*, 47 U. PITT. L. REV. 959 (1989) (providing a legal perspective on why software patents should be allowed); Allen Newell, *The Models Are Broken, the Models Are Broken!*, 47 U. PITT. L. REV. 1023 (1986) (providing a response showing the conceptual problems with software patents).

[4] 35 U.S.C. § 103.

[5] 35 U.S.C. § 102(a)(1).

[6] *Id.*

[7] *Id.*

[8] *See, e.g.*, *Microsoft License Terms*, MICROSOFT § (2)(c)(vi) (June 2018), https://www.microsoft.com/en-us/Useterms/Retail/Windows/10/UseTerms_Retail_Windows_10_English.htm [https://perma.cc/9XUM-9Q57] ("[Y]ou may not . . . reverse engineer, decompile, or disassemble the software.").

are not patentable.[9] The Supreme Court reiterated that more recently,[10] adding "[s]tating an abstract idea while adding the words 'apply it with a computer' simply combines those two steps, with the same deficient result."[11] A prohibition against patenting "mental steps" was set forth by the Ninth Circuit in 1944[12] and echoed by the Court of Claims and Patent Appeals a few years later.[13] Indeed, at least as early as 1854 the Supreme Court indicated that abstract ideas were not patentable.[14] The question, though, is whether algorithms are mental steps. I show that in the early 20th century such algorithmic patent claims were not rejected, and indeed were commonly accepted, at least in some contexts.

In the late 19th and early 20th century, the telegraph was a principal means of long-distance communication.[15] Because telegraph companies charged by the word, codebooks were constructed to permit phrases and sentences to be specified in a single word.[16] Accordingly, a lot of inventive effort was directed towards the construction of better codes.[17] Areas for improvement included ease of use, better compression,[18] correctness of transmitted messages,[19] and

---

[9] Gottschalk v. Benson, 409 U.S. 63, 67 (1972) ("[M]ental processes, and abstract intellectual concepts are not patentable . . . .").

[10] Alice Corp. v. CLS Bank Int'l, 573 U.S. 208, 209 (2014).

[11] *Id.*

[12] Halliburton Oil Well Cementing Co. v. Walker, 146 F.2d 817, 821 (9th Cir. 1944) ("We think these mental steps, even if novel, are not patentable.").

[13] *In re* Abrams, 188 F.2d 165, 170 (C.C.P.A. 1951) ("The *Halliburton v. Walker* case, . . . seems to us to be sound in its reasoning and directly applicable here.").

[14] O'Reilly v. Morse, 56 U.S. 62, 135 (1854).

> [I]f the essence of his invention consists in compelling this hitherto useless element to record letters and words, at any distance and in many places at the same moment, how can it be said that the claim is for a principle or an abstraction?

[15] *See generally* TOM STANDAGE, THE VICTORIAN INTERNET: THE REMARKABLE STORY OF THE TELEGRAPH AND THE NINETEENTH CENTURY'S ON-LINE PIONEERS VIII–IX (1998).

[16] DAVID KAHN, THE CODEBREAKERS 838 (Scribner 2nd ed. 1996) ("Cable messages cost so much that the reduction in length made possible by code afforded enormous economies.").

[17] Campbell-Kelly, *supra* note 3, at 217–18.

[18] KAHN, *supra* note 16, at 846.

> The intrinsic factor, or the quality of a code, refers primarily to its condensing power: how many plain-language words are represented by a single five-letter codeword. The later codes average a condensing power of between 5:1 and 10:1, which means that they reduce messages to one fifth or one tenth of their plain-language length.

[19] *See, e.g.*, Primrose v. Western Union Tel. Co., 154 U.S. 1 (1894); *see also* Steven

confidentiality. Indeed, concern for the confidentiality of telegraph messages goes back to the earliest days of the telegraph; Samuel Morse's business partner, Francis O. Smith, devised a codebook intended for confidentiality.[20]

Patents for such codes and ciphers were routinely granted.[21] There are a number of interesting examples; I describe a few here.[22]

Elmer Cassel received two closely related patents in 1900, for a "Cipher Code System"[23] and for a "Cipher-Code."[24] The patents were intended for both compression and error detection. While they differ in detail, both patents describe algorithms for constructing telegraph codebooks. An actual codeword is constructed by combining two English words, one for the page and line (in the '586 patent) and two for separate phrases (in the '587 patent).

The first claim of the '586 patent reads: "A cipher-code in which words or syllables capable of literal translation are so compounded as to form a complete cipher-word without literal meaning, as set forth."[25]

This is an "art" patent in the statute of the time,[26] in that it does not describe a "machine, manufacture, or composition of matter."[27] The error detection and correction comes from using a very small set of words, ones carefully chosen "with especial reference to accuracy in transmission by telegraph."[28]

M. Bellovin, Compression, Correction, Confidentiality, and Comprehension: A Look at Telegraph Codes (unpublished manuscript) (on file with the Columbia University Department of Computer Science), https://www.cs.columbia.edu/~smb/papers/codebooks.pdf.

[20] *See* FRANCIS ORMOND JONATHAN SMITH, THE SECRET CORRESPONDING VOCABULARY: ADAPTED FOR USE TO MORSE'S ELECTRO-MAGNETIC TELEGRAPH, AND ALSO IN CONDUCTING WRITTEN CORRESPONDENCE, TRANSMITTED BY THE MAILS, OR OTHERWISE (1845).

[21] In today's terminology, a "code" operates on semantic concepts such as a phrase or sentence, while a "cipher" operates on purely syntactic units such as letters or bytes. In this time frame, however, terminology was not standardized. *See* KAHN, *supra* note 16, at xv–xviii.

[22] I deliberately searched for cipher- and code-related patents, since they are inherently about manipulating information.

[23] *See* Cipher Code System, U.S. Patent No. 657,586 (filed Mar. 10, 1900) (issued Sept. 11, 1900).

[24] *See* Cipher-Code, U.S. Patent No. 657,587 (filed June 23, 1900) (issued Sept. 11, 1900).

[25] '586 Patent, *supra* note 23, at p. 3 col. 1 l. 15–18.

[26] See the discussion of the meaning of "art" and especially the definition given in 1 WILLIAM C. ROBINSON, THE LAWS OF PATENTS FOR USEFUL INVENTIONS 230–257 (1890).

[27] Patent Act of 1870 § 24, 16 Stat. 198, R.S. § 4886.

[28] '586 Patent, *supra* note 23, at p. 2 col. 2 l. 106–07.

The novelty of this patent is unclear. The examiner objected,[29] citing an essay "Cryptography" by none other than Edgar Allen Poe.[30] Cassel objected, pointing out differences, and the examiner accepted his explanation. However, the notion of combining short words to form a non-word was apparently known at the time. Major William F. Friedman quotes the 1893 *Book of Rules* of the Western Union Telegraph Company as saying: "All pronounceable groups of letters, when such groups are not combinations of dictionary words, will be counted as one word. When such groups are made up of improper combinations of dictionary words, each dictionary word so used will be counted as one word."[31]

In other words, people were likely using his exact scheme, albeit for economy in transmission, a concept Cassel does not discuss. That said, his claims do not limit his system to his described objectives.

Henry Newton and Anthony Michell's patent for a "Cipher System" was intended to prevent undetected errors in the transmission of a message.[32] It worked by assigning to each possible vowel-consonant pair of letters a number.[33] The numbers for each group of ten letters are added; if the sum is greater than 100, the first digit is dropped. Consulting a table tells the user which syllables to interchange in that word. There are four claims; the first of which reads:

> In a cipher system employing a number of syllables each consisting of one consonant and one vowel; the assignment to each pair of such syllables having the same consonant and vowel of a common numerical value the distinction of the two syllables of each such pair as normal or reversed according as the consonant or vowel

---

[29] Pat. Hist. 657,586 p.19 (on file with Columbia University Department of Computer Science), https://www.cs.columbia.edu/~smb/doc/Patent_Histories/657586.pdf. (I have obtained scans from the National Archives of the patent history files for many of the patents referred to in this document. They are available at https://www.cs.columbia.edu/~smb/doc/Patent_Histories.)

[30] EDGAR ALLAN POE, *Cryptography*, *in* 1 THE WORKS OF EDGAR ALLAN POE 431, 441 (Richard H. Stoddard ed., 1884).

[31] WILLIAM F. FRIEDMAN, INTERNATIONAL RADIOTELEGRAPH CONFERENCE OF WASHINGTON 31–32 (U.S. Gov't Printing Off. 1927), https://books.google.com/books?id=64QmBwf3W38C&pg=PP1#v=onepage&q&f=false [https://perma.cc/7Q52-4ZPG].

[32] Cipher System, U.S. Patent No. 879,667 (filed Aug. 30, 1907) (issued Feb. 18, 1908).

[33] The use of consonant-vowel pairs was used to create artificial, pronounceable words as a way to work around telegraph tariffs of the time. *See* FRIEDMAN, *supra* note 31, at 24.

> precedes; the combination or resolution of a message as a succession of such syllables either normal or reversed; the division of such message into sections each consisting of a definite number of such syllables; the assignment to each of such sections of a check number according to the succession of normal and reversed syllables and the establishment of a correspondence between the check-number so assigned to such section and a totality of the numerical values assigned to its separate syllables all for the purposes set forth.[34]

Again, here are no physical mechanisms described; only the fourth claim references an external table. In other words, the entire process involves mental steps.[35]

To my knowledge, the Newton-Michell scheme is novel. The earlier error detection schemes I'm aware of were designed to authenticate banking transactions.[36] The "mutilation tables" of the 1920s were far more complex.[37] The general outline does bear a striking resemblance to modern "check digits."[38]

There are also some interesting hybrid patents, hybrid in the sense of combining algorithmic steps and a physical mechanism. Willis Roussel invented a device aimed at providing confidentiality;[39] assuming novelty, this would clearly be patentable since it was a

---

[34] '667 Patent, *supra* note 32, at p. 3 col. 1 l. 23–42.

[35] This patent was clearly intended for use with telegraphs, but as the specification itself says, it can be used for "the transmission of telegraphic and similar messages". *Id.* at p. 1 col. 1 l. 14–15. There were many older types of telegraph, including optical semaphores. *See, e.g.*, KAHN, *supra* note 16, at 836; ARTHUR C. CLARKE, HOW THE WORLD WAS ONE, ch. 2 (Bantam Books, 1992). The radiotelegraph had also been invented and publicized by the time this patent was filed. MARC RABOY, MARCONI: THE MAN WHO NETWORKED THE WORLD 68 (Oxford Univ. Press 2016). It was even working across the Atlantic Ocean. *Id.* at 175.

[36] *See* ROBERT SLATER, BANKING TELEGRAPHY: COMBINING AUTHENTICITY, ECONOMY, AND SECRECY, A CODE FOR THE USE OF BANKERS AND MERCHANTS (W.R. Gray 1876), http://books.google.com/books?id=6A4EAAAAQAAJ [https://perma.cc/58EJ-UQPB]; FRANK MILLER, TELEGRAPHIC CODE TO INSURE PRIVACY AND SECRECY IN THE TRANSMISSION OF TELEGRAMS (Charles M. Cornwell 1882), http://books.google.com/books?id=tT9WAAAAYAAJ&pg=PA1#v=onepage&q&f=false [https://perma.cc/58EJ-UQPB].

[37] *See* Bellovin, *supra* note 19.

[38] *See, e.g.*, Computer for Verifying Numbers, U.S. Patent No. 2,950,048 (filed Jan. 6, 1954) (issued Aug. 23, 1960).

[39] Cipher Code System, U.S. Patent No. 642,721 (filed May 16, 1899) (issued Feb. 6, 1900).

"machine." He clearly did contemplate a physical mechanism, as is shown by some of the diagrams and the accompanying text. The details are complex; let it suffice to say that his preferred instantiations combine a machine (in one case, a set of wheels; in another, a grooved base) with a codebook.[40] Nevertheless, the first claim simply reads:

> A cipher-code index having a column of cipher-words on each page, a parallel column of cipher-letters corresponding each respectively to a cipher-word, the information represented by said cipher-words inscribed in the same line with its corresponding cipher-word and the subjects contained on any page being inscribed on the right-hand margin of the folio, substantially as described.[41]

Not until the sixth claim is his physical "machine" mentioned. The first five claims are all directed to how to construct the necessary codebook: an informational transformation, not a "machine."

One of the most fascinating cryptographic patents was awarded to Lyman Morehouse in 1920.[42] Morehouse was attempting to solve a practical problem with Gilbert Vernam's ground-breaking one-time

---

[40] The physical design, though not in the mode of use, is similar to the wheel cipher first invented by Thomas Jefferson, BETSY ROHALY SMOOT, PARKER HITT: THE FATHER OF AMERICAN MILITARY CRYPTOLOGY 55 (Univ. Press of Ky. 2022), independently reinvented by Étienne Bazeries in 1891, KAHN, *supra* note 16, at 247–48, again reinvented by Parker Hitt in 1913, SMOOT, *supra*, at 55, and adopted by the U.S. Army in 1922, *id.* The grooved base is physically similar (though again, not in use) to Hitt's "strip system," invented in 1914 and used by the U.S. Navy and State Department through the mid-20th century. *Id.* Jefferson's invention was not rediscovered until examination of his papers in the Library of Congress in 1922. KAHN, *supra* note 16, at 195.

[41] '721 Patent, *supra* note 39, at p. 4 col. 1 l. 32–40.

[42] Ciphering System, U.S. Patent No. 1,356,546 (filed Dec. 4, 1918) (issued Oct. 26, 1920).

tape encryption system.[43] Vernam invented a truly secure[44] encryption mechanism that required a paper tape of never-reused random characters. His design, however, was impractical. Not only would the reel of paper tape be large,[45] it was seen as infeasible at the time to produce enough large, random tapes.[46] Accordingly, Morehouse invented a variant machine that used two looped paper tapes of relatively prime lengths.[47] In other words, this was clearly a hardware invention, complete with circuit diagrams. However, Morehouse's patent did not stop there. The specification says:

---

[43] Secret Signaling System, U.S. Patent No. 1,310,719 (filed Sept. 13, 1918) (issued July 22, 1919); Gilbert S. Vernam, *Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications*, *in* XLV JOURNAL OF THE AMERICAN INSTITUTE OF ELECTRICAL ENGINEERS 109, 109 (1926); Steven M. Bellovin, *Vernam, Mauborgne, and Friedman: The One-Time Pad and the Index of Coincidence*, *in* THE NEW CODEBREAKERS: ESSAYS DEDICATED TO DAVID KAHN ON THE OCCASION OF HIS 85TH BIRTHDAY 40 (Peter Y.A. Ryan et al. eds., 2016); *see also* KAHN, *supra* note 16, at 397–98. *But see* Steven M. Bellovin, *Frank Miller: Inventor of the One-Time Pad*, 35 CRYPTOLOGIA 203 (2011) (discussing who actually invented the one-time pad).

[44] KAHN, *supra* note 16, at 398.

> And it is an unbreakable system. Some systems are unbreakable in practice only, because the cryptanalyst can conceive of ways of solving them if he had enough text and enough time. The one-time system is unbreakable both in theory and in practice. No matter how much text a cryptanalyst had available in it, or how much time he had to work on it, he could never solve it.

The one-time system is so secure that it is used to protect the Washington-Moscow hot line. *Id.* at 715–16.

[45] I calculated that a tape holding 100,000 characters, the minimum for a day's traffic in a production setting, would require a reel about .6 meters (two feet) in diameter. Bellovin, *Vernam, Mauborgne, and Friedman: The One-Time Pad and the Index of Coincidence*, *supra* note 43, at 41.

[46] William F. Friedman, *Letter to R.D. Parker* (May 1944), William F. Friedman Collection, George C. Marshall Foundation Library, Item 669.4 (on file with author).

[47] The observation that the lengths of the two tapes should be relatively prime is due to William F. Friedman. William F. Friedman, *Mechanics of Differential Primary Keys* 57 (1920), William F. Friedman Collection, George C. Marshall Foundation Library, Item 1056 (on file with author). Two integers are relatively prime if their greatest common divisor—that is, the largest integer that evenly divides both of them—is 1. This is discussed in any number theory book. *See, e.g.*, IVAN NIVEN, HERBERT S. ZUCKERMAN & HUGH L. MONTGOMERY, AN INTRODUCTION TO THE THEORY OF NUMBERS 9 (John Wiley & Sons, Inc. 5th ed.). Without going into the mathematical or cryptologic details, using relatively prime lengths maximizes the time before a sequence of actual key characters repeats. This was intended to make the system very secure, though Morehouse's goal was ultimately not met. *See* KAHN, *supra* note 16, at 398; Bellovin, *Vernam, Mauborgne, and Friedman: The One-Time Pad and the Index of Coincidence*, *supra* note 43, at 41.

> It will be clear that the invention is not limited to the use of perforated tapes, or any other particular form of record for the series of ciphering characters nor to any particular electrical or mechanical means for combining the characters from the several series to produce the running key by which the enciphering and deciphering are accomplished. It is not important in the use of the invention that the effect of combining the two or more characters from different series should be actually manifested in a discernible form.[48]

In other words, he explicitly disclaimed the need for any physical mechanism. The first claim makes it even clearer that this is what he meant:

> The method of enciphering or deciphering messages which consists in forming a plurality of series of ciphering characters different in each series, selecting characters from each series in a fixed order to form a continuous sequence by retraversing the series as it is exhausted, and altering the message characters in accordance with a predetermined rule whose effect upon successive message characters is dependent upon the concurrent use of characters so selected from different cipher series.[49]

Claim 8 mentions a "device,"[50] but a specific hardware "machine" is not mentioned until claim 12.[51] By contrast, Vernam's patent mentions "current values" and "code impulses" in the very first claim.[52]

A lot is known about the context of Morehouse's patent, which

---

[48] '546 Patent, *supra* note 42, at p. 3 col. 1 l. 43–55.
[49] *Id.* at p. 3 col. 2 l. 95–107.
[50] *Id.* at p. 4 col. 1 l. 58.
[51] *Id.* at p. 4 col. 2 l. 120.
[52] *George E. Folk, 83, A Patent Attorney*, N.Y. TIMES, Jan. 15, 1956, at 92. George E. Folk was the patent attorney for both Vernam and Morehouse. Folk was the General Patent Attorney for AT&T from 1915–1937 and published a number of pieces on the interaction of patent law with antitrust law. In a book he edited and contributed to on the impact of patents, there is no discussion of what is or is not patentable. *See* PATENTS AND INDUSTRIAL PROGRESS: A SUMMARY, ANALYSIS, AND EVALUATION OF THE RECORD ON PATENTS OF THE TEMPORARY NATIONAL ECONOMIC COMMITTEE (Harper 1942).

lets us guess why the claims were drafted as they were. Vernam, Morehouse, and their colleagues at AT&T were working on secure, automated encryption systems, which they reported to the U.S. Army. Major Joseph O. Mauborgne, head of the research and engineering division of the U.S. Army's Signal Corps, was tasked with working with them.[53] My earlier research suggests that Major Mauborgne worked closely with the engineers;[54] in fact, there is some evidence that he participated in drafting the Morehouse patent and its claims.[55] The most common use of superencipherment[56] in that era was to first encode the message using a codebook, and then encrypt the resulting code words with a cipher.[57] Mauborgne undoubtedly knew this—and knew of the vulnerabilities of such schemes; as Kahn put it, he was an "extraordinary cryptanalyst."[58] But superenciphering with Morehouse's scheme, albeit with two written series of numbers instead of two looped paper tapes, would have been far more secure than the older schemes for working with codebooks. A paper series of numbers would also have been far more suitable for tactical use, since it would not require carting a large, delicate piece of apparatus from trench to trench. (In a different vein, it raises anew the question of whether Mauborgne knew of Frank Miller's invention of the one-time pad several decades earlier, a question I previously investigated:[59] Miller's scheme did use a written list of numbers.[60]) In other words, it seems likely that the Morehouse patent was written as it was precisely to cover manual use.

It seems, then, that despite the Supreme Court's holding in *Morse*,[61] many patents for algorithms—mental steps, if you will—were issued in the early part of the 20th century.[62] The language in the patent law then, the Patent Act of 1870, allowed patents for "any new and useful art, machine, manufacture, or composition of matter."[63] This is

---

[53] KAHN, *supra* note 16, at 397.
[54] Bellovin, *Vernam, Mauborgne, and Friedman: The One-Time Pad and the Index of Coincidence*, *supra* note 43, at 41.
[55] *Id.* at 45.
[56] KAHN, *supra* note 16, at xv–xviii (defining "superencipherment" as the process of taking the output of an encryption process, often a code, and applying a cipher to it).
[57] SMITH, *supra* note 20, at 9–10; KAHN, *supra* note 16, at xv–xviii.
[58] KAHN, *supra* note 16, at 398.
[59] *See* Bellovin, *Frank Miller: Inventor of the One-Time Pad*, *supra* note 43.
[60] *Id.*
[61] O'Reilly v. Morse, 56 U.S. 62, 135 (1854) ("[I]f the essence of his invention consists in compelling this hitherto useless element to record letters and words, at any distance and in many places at the same moment, how can it be said that the claim is for a principle or an abstraction?").
[62] *See* '667 Patent, *supra* note 32.
[63] Patent Act of 1870 § 24, 16 Stat. 198, R.S. § 4886.

almost identical to today's "any new and useful process, machine, manufacture, or composition of matter,"[64] where "process" is defined recursively as "process, art or method, and includes a new use of a known process, machine, manufacture, composition of matter, or material."[65] But this is not how the law was applied.

The first claim in the Roussel's original '721 patent application began: "In a cipher code system, the method of translating communications into and out of cipher . . . ."[66] The examiner rejected it, saying that it was "drawn to a system, a thing unknown to the patent law"[67] and cited *Ex parte Berolzheimer*: "Systems of book-keeping, recording, tabulating, and the like, are not inventions, nor are they the subjects of letters patent."[68]

The examiner's objection was apparently supported by case law. The Supreme Court wrote in 1877 that

> [a] process is a mode of treatment of certain materials to produce a given result. It is an act or series of acts, performed upon the subject-matter, to be transformed and reduced to a different state or thing. If new and useful, it is just as patentable as a piece of machinery. In the language of the patent law, it is an art.[69]

The Court repeated this definition many years later in *Gottschalk v. Benson*,[70] a case where the justices unanimously rejected the notion of algorithmic patents.[71]

John MacNab, a principal examiner in the patent office, cited Prof. William Robinson's succinct definition:[72]

---

[64] 35 U.S.C. § 101.
[65] 35 U.S.C. § 100(b).
[66] Pat. Hist. 642,721 p.14 (on file with Columbia University Department of Computer Science), https://www.cs.columbia.edu/~smb/doc/Patent_Histories/642721.pdf.
[67] *Id.* at p.24.
[68] *Ex parte* Berolzheimer, 1870 C.D. 33, https://www.google.com/books/edition/Decisions_of_the_Commissioner_of_Patents/vMRSAAAAcAAJ?hl=en&gbpv=0 [https://perma.cc/5MKM-8QTR] ("C.D." is the compilation of the decisions of the Commissioner of Patents; it does not appear to be available via Westlaw or LexisNexis).
[69] Cochrane v. Deener, 94 U.S. 780, 781 (1877).
[70] Gottschalk v. Benson, 409 U.S. 63, 69–70 (1972).
[71] *Id.* at 71–73.
[72] John F. MacNab, *Invention and Patentability Under the Patent Statutes as Applied to So-Called Printed Matter and Methods or Systems of Doing Business*, *in* PAT. OFF. PAPERS 1914–1917, at 4 (1917),

> But though an art embraces so wide a field of inventive skill, it includes only such operations as are capable of producing physical effects. Every invention, when applied according to the design of its inventor, must accomplish some change in the character or condition of material objects.[73]

Roussel deleted the word "system." The examiner also rejected some later claims as anticipated by Bazeries;[74] those claims were not reinstantiated. After a few more exchanges with the examiner on other matters, the '721 patent was approved.

Cassel's '586 patent[75] ran into similar objections. The original version of the first claim began "[a] cipher code system"; the examiner objected that it was "drawn to a system—a thing unknown in the Patent [sic] law."[76] When the offending word "system" was deleted, the application was approved. Cassel learned from this encounter. His '587 patent[77] did not use the word "system" in the claims, which was likely deliberate; he noted in a discussion with the patent office about novelty that: "Claim 1 and 2, as above presented, are drawn in a form which entitles them to favorable consideration."[78] This letter was dated June 23, 1900; the initial rejection due to use of "system" in the '586 patent was about three months earlier, on March 22, 1900.[79]

Perhaps the most fascinating patent history is for the Morehouse '546 patent: the examiner's only issues were minor matters of wording. There was no discussion at all about the abstract nature of the claims or of any part of the specification.[80]

---

https://books.google.com/books?id=KMs9AAAAIAAJ&pg=PA4&lpg=PA4&dq=Ex+parte+Berolzheimer,+%221870+C.+D.+33%22&source=bl&ots=V89MFDaQkG&sig=ACfU3U2Q3PFSM5U5DOf-a6twh5_kUMAgPQ&hl=en&sa=X&ved=2ahUKEwjNtba20u7-AhXyF1kFHRAjAPsQ6AF6BAgJEAM#v=onepage&q&f=false [https://perma.cc/L4J9-9S8B].

[73] ROBINSON, *supra* note 26, at 249. Robinson's book is so respected that it has been cited at least as recently as 2009. *E.g.*, Abbott Labs v. Sandoz, 566 F.3d 1282, 1313 (Fed. Cir. 2009).

[74] Pat. Hist. 642,721, *supra* note 66, at p.24.

[75] '586 Patent, *supra* note 23.

[76] Pat. Hist. 657,586, *supra* note 29, at p.24.

[77] '587 Patent, *supra* note 24 (this patent and the '586 patent are related but describe different systems).

[78] Pat. Hist. 657,586 *supra* note 29, at 14.

[79] KAHN, *supra* note 16, at 398.

[80] Pat. Hist. 1,356,546 p.28 (on file with Columbia University Department of

To sum up: patent claims for cryptographic or coding systems were regularly accepted, as long as they did not use the prohibited word "system."

The Newton and Michell patent did not encounter any substantive objections from the examiner, though there is one amusing note: "Claim 4 is very informal as it is objectionable to refer in a claim to other claims for a portion of the structure."[81]

Somewhat later, the Patent Office appeared to take a more negative view of what today we might think of as algorithm steps. In *Ex parte Toth and Nutter*,[82] the Patent and Trademark Office Board of Appeals rejected two claims as purely mental steps:[83]

> In addition it may be said that the act of "correcting said indicated pressure" in claim 4, and the "determining the well pressure", etc. claim 9 do not constitute steps of a patentable process. These acts are purely mental and hence do not come within the definition of an "art" as given by Robinson in his work on patents or by the Court in *In re Weston*, 1901 C.D. 290.[84]

The patent was eventually issued,[85] but without the offending claims.

Armand Abrams appealed his patent rejection to the Court of Claims and Patent Appeals.[86] Abrams urged a more nuanced reading of

---

Computer Science), https://www.cs.columbia.edu/~smb/doc/Patent_Histories/1356546.pdf. There is a certain irony here, in that from a technical perspective, one could argue that some of Morehouse's claims were not even novel. Again omitting a mathematical explanation, the essence of what Morehouse did was to encrypt first with one cryptographic key and superencipher with a second key, a technique that was well known at the time. *See* SMITH, *supra* note 20; *see also* KAHN, *supra* note 16, at 397–98. But that would not have been clear except to a cryptographer, and his mechanism to accomplish this was undoubtedly novel. Furthermore, in Morehouse's scheme both encryptions took place simultaneously, which would also be novel.

[81] Pat. Hist. 879,667 p.30 (on file with Columbia University Department of Computer Science), https://www.cs.columbia.edu/~smb/doc/Patent_Histories/879667.pdf.

[82] *Ex parte* Toth and Nutter, 63 U.S.P.Q. 131 (1944).

[83] There were also novelty issues raised by the examiners; the claims were rejected by the Board on those grounds, too. *Id.*

[84] *Id.* at 132.

[85] Apparatus for Determining Production Potentials of Oil Wells, U.S. Patent No. 2,360,742 (filed Mar. 8, 1941) (issued Oct. 17, 1944).

[86] *See In re* Abrams, 188 F.2d 165 (C.C.P.A 1951). The file history (U.S. Patent

the "mental steps" rule: that a claim should be rejected if it was entirely mental steps, or if the asserted novelty was in the mental steps, but should be allowed if the novelty was in the physical steps of a claim incorporating both.[87] The court neither adopted nor rejected the definition. Rather, it said:[88]

> In the statement of the examiner following the appeal to the board it was said: "All claims have been rejected as improper under the statutes in setting forth a process that predominately involves merely a mental process in obtaining the result. This mental process is indicated by such terms in the claims as 'calculating' applied for instance to mathematically making certain computations from figures taken down from pressure observation, 'comparing' applied to mere mental comparison of figures on a sheet 'converting' as related to mathematically calculating the flow data or pressure rise with respect to a standard reference pressure, 'determining' applied, for instance, to the reading of the pressure rise figures; 'correcting' involving mere mathematical calculations."[89]

These were all felt to be mental steps.

The court then quoted the Ninth Circuit in *Halliburton v. Walker*[90] as saying that "the steps of the method claimed were described in the claims taken together by the descriptive words 'determining,' 'registering,' 'counting,' 'observing,' 'measuring,' 'comparing,' 'recording,' and 'computing,' . . . . We think these mental steps, even if

---

Application serial no. 533,203) on my web page is likely incomplete. The National Archives and Records administration retains file histories only for issued patents. Private communication with Archivist Robert Beebe. The excerpt I have posted is from the court record, also obtained from the National Archives.

[87] *Id.* at 166.

[88] *Id.* at 167.

[89] *Id.*

[90] *See* Halliburton Oil Well Cementing Co. v. Walker, 146 F.2d 817 (9th Cir. 1944). This is a complex opinion dealing with three patents: Method of Measuring Location of Obstructions in Deep Wells, U.S. Patent No. 2,209,944 (filed Sept. 25, 1939) (issued Jul. 30, 1940); Method of Determining Fluid Density, Fluid Pressure, and the Production Capacity of Oil Wells, U.S. Patent No. Re. 21,383 (filed Oct. 26, 1937) (reissued Mar. 5, 1940); Means For Measuring the Location of Obstruction in Wells, U.S. Patent No. 2,156,519 (filed Sept. 7, 1937) (issued May 2, 1939). We are concerned in this article with only the first two. The third was appealed to the Supreme Court. *See* Halliburton v. Walker, 329 U.S. 1 (1946). Its holding is not relevant here.

novel, are not patentable."[91] The *Halliburton* court went on to quote the Patent Act as protecting the "invention of a 'new and useful art, machine, manufacture, or composition of matter."[92] and rejected the claims as mental steps.

It is hard to argue with the consistency of the later rulings in *Ex parte Toth and Nutter*[93] and *In re Abrams*.[94] However, there is serious tension with the claims allowed, without even argument from the examiners, in Morehouse's '546 patent[95] and the others I have discussed. The first claim in '546 speaks of "forming," "selecting," and "altering," without mentioning any physical mechanisms. Why is this different from the "registering," "counting," "observing," "comparing," "recording," and "computing" in *Halliburton*?[96]

There is perhaps some insight to be gained by looking at one of the earliest Supreme Court cases involving patentability, *Morse*.[97] Morse sued O'Reilly, claiming that his patents[98] on the telegraph were infringed; O'Reilly countersued, claiming invalidity. The fifth claim is of interest to us: Morse patented what has become known as Morse code:[99] "I claim, as my invention, the system of signs, consisting of dots and spaces, and of dots, spaces, and horizontal lines, for numerals, letters, words, or sentences, substantially as herein set forth and illustrated, for telegraphic purposes."[100] The Court extensively quoted the circuit court opinion,[101] but that court did not analyze this claim in detail. It simply noted that it "is a claim to the system of signs . . . for telegraphic purposes; being an improved instrumentality in the art of telegraphing . . ."[102] and went on to note that "[a]n art is patentable by

---

[91] *Abrams*, 188 F.2d at 169.
[92] *Halliburton*, 146 F.2d at 169 (internal citations omitted).
[93] *See Ex parte* Toth and Nutter, 63 U.S.P.Q. 131 (1944).
[94] *See Abrams*, 188 F.2d at 165.
[95] '546 Patent, *supra* note 42.
[96] *Halliburton*, 146 F.2d at 821.
[97] *See* O'Reilly v. Morse, 56 U.S. 62 (1854).
[98] We are concerned here with only one of his patents, Telegraph Signs, U.S. Patent No. 1,647 (issued June 20, 1840).
[99] The system used today is commonly known as International Morse Code, which is not the same as the system originally patented by Morse. *See* William B. Taylor, *Henry and the Telegraph*, *in* ANNUAL REPORT OF THE BOARD OF REGENTS OF THE SMITHSONIAN INSTITUTION 359–60 (1879).
[100] *Morse*, 56 U.S. at 86.
[101] *Id.* at 63 ("Permission has been given by Judge Monroe that the reporter may use his statement as preliminary to this report, and he avails himself with pleasure of this kindness . . . .").
[102] *Id.* at 101.

the act of 1836 and so is an improvement on it."[103] It went on to note that:[104]

> He who discovers a principle and devises one mode by which the same can be rendered practically useful, is entitled to a patent which shall protect him to the full extent of his invention and against all other devices for using it.
>
> If Morse, therefore, was the first to discover that the power of electro-magnetism could be used for the purpose of recording telegraphic signs, and devised one practical mode for using it, he may, by a general claim, secure to himself the right of so applying it, as well as the particular devices by which he did so.

The Supreme Court did not further engage with this claim or any of the others of the first seven; it instead analyzed (and struck down) the eighth claim as overbroad, and went on to analyze the issue of novelty.[105]

Apart from the irony of the opinion's use of the word "system," in contravention to the patent examiners' holdings in the '721 and '586 patents, the important part of that fifth claim is the last clause: "for telegraphic purposes." This is crucial: Morse was not just patenting the abstract notion of an encoding of letters into dots and dashes, he was limiting it to a particular purpose. Much later, the Federal Circuit *en banc* explained this in *CLS Bank v. Alice*:[106]

> [T]he animating concern is that claims should not be coextensive with a natural law, natural phenomenon, or abstract idea; a patent-eligible claim must include one or more substantive limitations that, in the words of the Supreme Court, add "significantly more" to the basic principle, with the result that the claim covers significantly *less*. Thus, broad claims do not necessarily

---

[103] *Id.*

[104] *Id.* at 101–02.

[105] *Id.* at 107–11. A broader reading of the history of the telegraph makes it impossible to dismiss the thought that some degree of nationalism was involved in the novelty discussion. *See, e.g.*, STANDAGE, *supra* note 15, at 22–56; CLARKE, *supra* note 35, at ch. 2.

[106] CLS Bank v. Alice Corp., 717 F.3d 1269, 1281 (Fed. Cir. 2013), *aff'd*, 573 U.S. 208 (2014).

> raise § 101 preemption concerns, and seemingly narrower claims are not necessarily exempt. What matters is whether a claim threatens to subsume the full scope of a fundamental concept, and when those concerns arise, we must look for meaningful limitations that prevent the claim as a whole from covering the concept's every practical application.[107]

To be sure, the Court's analysis in *Morse* is rather hard to read and is based on a different patent law,[108] which can make it hard to draw firm, modern conclusions from it. Professor Adam Mossoff writes that "Chief Justice Taney did not follow this settled legal practice in patent law in the Antebellum Era, even given the evolving, embryonic nature of U.S. patent law in the early nineteenth century."[109] He goes on to note that to discuss the opinion, "one must first understand the nature of patents, patent law, and patent litigation in the Antebellum Era, which differed fundamentally from how patents are drafted by modern lawyers and interpreted by courts today."[110] Most specifically, the structure of claims was very different: "In the Antebellum Era, however, the nature and function of a patent, including its claims, was to secure 'the principle' of an invention, not the boundaries of the property right in the invention."[111] That said, and despite those flaws, the opinion in *Morse* has continued to be cited as authoritative today.[112]

Despite how often *Morse* has been cited, the principle that a purpose limitation can save a more abstract claim was apparently lost. In 1946, the Ninth Circuit ruled that:

> Given an apparatus for initiating an impulse wave in a well and a means for differentiating between and for recording echoes returned from obstruction in it, anybody with a rudimentary knowledge of arithmetic will be able to do what Walker claims a monopoly of doing. If his method were patentable it seems to us that the patentee would have a monopoly much broader than

---

[107] *Id.* (internal citations omitted).
[108] Patent Act of 1836, ch. 357, 5 Stat. 117 (1836).
[109] Adam Mossoff, O'Reilly v. Morse *and Claiming a "Principle" in Antebellum Era Patent Law*, 71 CASE W. RES. L. REV. 735, 738 (2020).
[110] *Id.* at 743.
[111] *Id.* at 745.
[112] *Id.* at 737 n.14.

would the patentee of a particular apparatus.[113]

But Walker's claim was very specifically limited to a means for locating obstructions in an oil well. The courts were not impressed. "By the time Halliburton and Walker first went to court in the 1940s, these nineteenth-century cases provided sufficient precedent for judges to develop a near-total ban on processes that involved mathematical computations."[114]

We do, of course, need to be careful about overthinking these early patents in terms of software, which of course did not exist 100 years ago. It is worth recalling what Prof. Newell wrote in 1986:

> But a more confounding answer flows from the general nature of computer science. All of computer science is directly related to use. There is essentially no gap, no matter how pure or basic the science is. With rare exceptions, scientific knowledge in computer science is in the form of means-ends relationships—what to do to obtain something of value. Indeed, this is just the essence of algorithms: what to do to perform a task.[115]

The examples we have discussed here fit that definition: "what to do to perform a task."

In some sense, the question isn't that new. Professor Michael Risch has noted that in the years before and immediately after the Patent Act of 1836, there were many patents issued for what today we would call business methods.[116] He even identified one he labeled a software-like patent from 1836.[117] But it is more akin to *Diamond v. Diehr*,[118] in that a physical process was being controlled. This is distinct from the cases I am considering here, where the object of the early cryptographic patents was to produce information rather than to control a physical

---

[113] Halliburton Oil Well Cementing Co. v. Walker, 146 F.2d 817, 821 (9th Cir. 1944).
[114] Gerardo Con Díaz, *Patent Law and the Materiality of Inventions in the California Oil Industry: The Story of* Halliburton v. Walker*, 1935–1946*, 24 ENTER. & SOC'Y 174, 187 (2023).
[115] Newell, *supra* note 3, at 1026.
[116] *See* Michael Risch, *America's First Patents*, 64 FLA. L. REV. 1279 (2012).
[117] Loom for Weaving Knotted Counterpanes and Other Fabrics in Which the Woof is Raised from the Surface, U.S. Patent No. 546 (filed Jun. 17, 1836) (issued Jan. 6, 1838). The fifth claim reads: "The application of a prism and pattern card, to regulate the operation of the hooks or teeth or dents to produce the variations in the pattern or figure." *Id.* at p. 9 col. 1 l. 3–6.
[118] *See* Diamond v. Diehr, 450 U.S. 175 (1981).

machine. The Cassel, Roussel, Newton and Anthony, and Morehouse patents discussed here are—not by accident—cryptographic patents. Cryptography is all about transforming one form of information into another, in an eerie echo of Prof. Robinson's definition of art: "accomplish some change in the character or condition of material objects."[119]

We are thus left with a dilemma. Apparently, in the early 20th century algorithmic patents were allowed, despite not producing "physical effects,"[120] only information effects. (It is perhaps worth mentioning that the Supreme Court's reversal of *Benson*, in *Diehr*, involved using a computer to control a physical process.) Arguably, that was in accordance with *Morse*,[121] though there is no documentary evidence for that in the patent file histories I examined. Furthermore, it does not account for the apparent reversal of policy in *Toth and Nutter*,[122] *Abrams*,[123] and *Halliburton*.[124] Why the change?[125]

One could argue that the issue in these cases is enablement,[126] not the use of an abstract idea. However, these decisions do not invoke enablement; rather, they rely on "mental steps" as a reason for invalidity.[127]

It is tempting to argue that one issue in the early 20th century cases might have been the unfamiliarity of patent examiners and judges with encoding and encryption. That does not hold up. First, it should not have been true of examiners; their job was to evaluate new technologies.

---

[119] ROBINSON, *supra* note 26, at 249.
[120] *Id.*
[121] *See* O'Reilly v. Morse, 56 U.S. 62 (1854).
[122] *See Ex parte* Toth and Nutter, 63 U.S.P.Q. 131 (1944).
[123] *See In re* Abrams, 188 F.2d 165 (C.C.P.A. 1951).
[124] *See* Halliburton Oil Well Cementing Co. v. Walker, 146 F.2d 817 (9th Cir. 1944).
[125] It is noteworthy that the first two cases were decisions of the Patent Office, not the Federal courts. In other words, it is not a matter of the Patent Office disregarding judicial decisions.
[126] Hybritech Inc. v. Monoclonal Antibodies, Inc., 802 F.2d 1367, 1384 (Fed. Cir. 1986) ("Enablement is a legal determination of whether a patent enables one skilled in the art to make and use the claimed invention."). The previous quote is derived from 35 U.S.C. § 112(a) (2012) ("The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to *enable* any person skilled in the art . . . to make and use the same.") (emphasis added).
[127] *Ex parte* Toth and Nutter, 63 U.S.P.Q. 131, 132 (1944) ("These acts are purely mental and hence do not come within the definition of an 'art' as given by Robinson in his work on patents . . . ."); *Abrams*, 188 F.2d at 169 ("Such purely mental acts are not proper subject matter for protection under the patent statutes . . . ."); *Halliburton*, 146 F.2d at 823 ("What we have said about the mental steps detailed in No. 2,209,944 applies with equal force to the steps we have described here.").

Judges may not have been familiar with encryption, but they were almost certainly familiar with telegraph codebooks. At least two were marketed to tourists,[128] and such codebooks were sufficiently part of popular culture that there was even a light-hearted essay on them in the *New Yorker* only slightly later than the time of these patents.[129] For that matter, the Supreme Court had been dealing with such codebooks since at least 1894.[130] Telegraphy was an extremely important and pervasive means of communication then, long before email;[131] it is not plausible that it was unfamiliar to those involved. It also leaves unanswered why all parties concerned, up to and including the Ninth Circuit, had sufficient expertise in oil wells.

This history raises several questions, some with implications for today. First, of course, is why these early 20th century cryptographic patents were allowed? Second, given that they were allowed, do they constitute adequate precedent for allowing algorithmic patents today, possibly beyond those permitted by the Supreme Court in *Alice*?[132] None of the patents I cite were ever challenged, so we have no way of knowing what the courts would have said, though around that period the Supreme Court rejected the idea of patenting abstract ideas[133] and endorsed the transformation test.[134] Conceivably, though, they could have been raised in *Gottschalk*,[135] though of course *Toth and Nutter*,[136] *Abrams*,[137] and *Halliburton*[138] would have been cited in opposition. And that raises a last question: why did the Patent Office change its policy

---

[128] *See* THOMAS WALTER HARTFIELD, ATLAS, THE, UNIVERSAL TRAVELLERS' AND TOURISTS' TELEGRAPHIC CIPHER CODE (1896); E.B. GILBURT, TOURISTS' TELEGRAPHIC CODE (Brown Brothers & Co. 1900).

[129] Jack Littlefield, *Melancholy Notes on a Cablegram Code Book*, NEW YORKER, July 28, 1934, at 18.

[130] *See* Primrose v. Western Union Tel. Co., 154 U.S. 1 (1894).

[131] *See* STANDAGE, *supra* note 15.

[132] *See* Alice Corp. v. CLS Bank Int'l, 573 U.S. 208 (2014).

[133] Boyden Power-Brake Co. v. Westinghouse, 170 U.S. 537, 556 (1898) ("We find here no authority to grant a patent for a 'principle,' or a mode of operation, or an idea, or any other abstraction.").

[134] Expanded Metal Co. v. Bradford, 214 U.S. 366, 384 (1909).

> A process is a mode of treatment of certain materials to produce a given result. It is an act, or a series of acts, performed upon the subject-matter to be transformed and reduced to a different state or thing. If new and useful, it is just as patentable as is a piece of machinery. In the language of the patent law, it is an art.

[135] *See* Gottschalk v. Benson, 409 U.S. 63 (1972).

[136] *See Ex parte* Toth and Nutter, 63 U.S.P.Q. 131 (1944).

[137] *See In re* Abrams, 188 F.2d 165 (C.C.P.A. 1951).

[138] *See* Halliburton Oil Well Cementing Co. v. Walker, 146 F.2d 817 (9th Cir. 1944).

by the 1940s?

The policy questions surrounding software patents still remain. But the legal landscape is murkier than ever.


MORITZ COLLEGE of LAW
THE OHIO STATE UNIVERSITY
SUUM CUIQUE TRIBUENDI