PATENTING CRYPTOGRAPHIC TECHNOLOGY

GREG VETTER*

INTRODUCTION

Cryptographic technology[1] holds the potential to help solve problems of information security within computing and information technology. Realizing this potential depends on many factors, including patent law. When exclusive rights for cryptographic technology impact interoperability, technology diffusion or standardization, these supply-side influences undercut what is oftentimes fickle market demand for data security. Users want their data in their increasingly ubiquitous, mobile and powerful computing devices. They want data security if it is easy and transparent. Developers and manufacturers want reduced production costs and the feature advantages of embeddable cryptographic technology with positive network effects. Patent law allows the owner of a valid patent some possibility of control over the technology claimed in the patent. This control can sometimes limit or skew standardization and slow diffusion of interoperable technology.

The rise of patenting for cryptographic techniques[2] mirrors the general increase in software patenting.[3] Scholars have not reached consensus that the patent system has been beneficial for information technology as compared to traditional industrial technology areas, such as the pharmaceutical field.[4] Patenting cryptography can influence self-ordering[5] and reordering

* Greg Vetter is an Associate Professor of Law at the University of Houston School of Law.

1. Cryptography is "the art and science of keeping messages secure." BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 1 (2d. ed. 1996). For a discussion of cryptography, see, for example., David Banisar, *Stopping Science: The Case Of Cryptography*, 9 HEALTH MATRIX 253, 254 (1999); A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 713 (1995); Marcus Maher, *International Protection of U.S. Law Enforcement Interests in Cryptography*, 5 RICH. J.L. & Tech. 13 (1999).

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

3. For a discussion of software patents, see, for example, Kevin Afghani & Duke W. Yee, *Keeping it Physical: Convergence on A Physicality Requirement for Patentability of Software-Related Inventions under the European Patent Convention and United States Law*, 15 J. INTELL. PROP. L. 239, 241 (2008); John R. Allison, Abe Dunn & Ronald J. Mann, *Software Patents, Incumbents, and Entry*; 85 TEX. L. REV. 1579, 1589–90 (2007); Robert P. Merges, *Software and Patent Scope: A Report from the Middle Innings*, 85 TEX. L. REV. 1627, 1628 (2007).

4. BRUCE LEHMAN, THE PHARMACEUTICAL INDUSTRY AND THE PATENT SYSTEM (2003),

within information technology because cryptographic systems are increasingly fundamental technology.[6] The demand for information security is growing as everyone's dependence on computing deepens while consumers and businesses alike realize the consequences of lost or stolen data. Developers and manufacturers, as well as governments, all have a stake in solutions that facilitate standardized, embeddable cryptography.[7] The path toward that outcome will likely feature both collaborative and contentious responses, such as collaboration via patent pools and standard setting, or such as contention by product differentiation based on cryptographic capability and patent portfolio building.

I. SOFWARE PATENTS AND CRYPTOGRAPHY

To use the U.S. patent system to protect technology, such as cryptography, one applies for a patent with the U.S. Patent and Trademark Office (USPTO) and writes one or more "claims" to define the scope of exclusive right. A valid claim of an issued patent allows its owner to exclude others from making, using and selling what the claim covers.[8] In a practical sense, most cryptography will be deployed via software. Thus, many patent claims covering cryptography are method claims that recite a series of steps that comprise the method. Thus, cryptography is inherently algorithmic in ways similar to how software is algorithmic. A claim to a cryptographic method written in broad language without reference to software can be infringed, assuming the claim's validity under patent law, by software operated by a third party. For example, if that third party's software "makes" or "uses" the method without permission from the patent owner, that owner can bring a patent infringement action.

In this way, the patent owner has a possibility of control over the technology covered by the valid claims in a patent. The more patents a particular person holds, with more valid claims in each, the greater the possibility of control if the claims cover the technology desired in the market-

http://www.earth.columbia.edu/cgsd/documents/lehman.pdf.

5. Early theoretical discussion of self-ordering can be found in Hayek. *See* Friedrich HAYEK, THE ROAD TO SERFDOM (1944).

6. BERT–JAAP KOOPS, THE CRYPTO CONTROVERSY 33 (Kluwer Law International: The Hague 1999).

7. Besides its influence on data security, cryptography triggers other policy issues, such as privacy from government surveillance. *See* A. Michael Froomkin, *It Came From Planet Clipper*, 1996 U. CHI. LEGAL F. 15, 71-75 (1996), *available at* http://www.law.miami.edu/~froomkin/articles/planet_clipper.htm (last visited Apr. 15Mar. 18, 20095).

8. The patent right includes other exclusionary rights, but they are omitted for simplification. 35 U.S.C. § 271 (2006). The doctrine of "exhaustion" in patent law is a limitation on the proposition given in the text. For example, once a chattel has been unconditionally sold under the authority of the patent owner, the owner can no longer exclude others from using and selling the chattel.

place. While applying for patents (an activity called "patent prosecution") is expensive, the next part of this article will discuss the increase over the last several decades of software patents generally and of cryptographic patents in particular. Even with patent law doctrine waxing and waning over that time as to the potential validity of software and cryptographic claims, users of the patent system such as technology developers and manufacturers have continued to patent cryptographic technology. The continued upswing in patents is potentially understood as the hopes of manufacturers to gain control, leverage, and the upper hand in the competitive and intertwined information technology markets that deploy cryptography.

As further background for the next part, this part will briefly caricature patent law's uneasy dance with certain subject matter from information technology, particularly software and cryptography.

To obtain a patent, one must first invent something and apply to the USPTO. That agency looks at five legal criteria called the elements of patentability[9] to determine if a patent should issue: (1) statutory subject matter; (2) utility; (3) novelty and statutory bars; (4) non-obviousness; and (5) objective disclosure requirements, such as enablement. Once the USPTO issues a patent, it carries a presumption of validity.[10] However, a patent can be invalidated at any point in its life.[11] In a standard patent infringement situation, the alleged infringer will attempt to invalidate the patent by showing how the allegedly infringed claims do not actually fit one or more of the five elements of patentability.

The first element of patentability is that the invention must be of patentable subject matter (sometimes called "statutory subject matter").[12] Patentable subject matter, stated in its strongest conception, includes "everything under the sun made by man" that is not already patented, except three notable exceptions: abstract ideas, naturally occurring phenomena, and laws of nature.[13] Although one may not patent any of the three exceptions,

9. STEVEN A. BECKER, PATENT APPLICATIONS HANDBOOK, 3:1 (2009). [_GRV says: I don't know the Becker source. There are some who count the elements of patentability as 3, some as 4, but a vast super-majority of patent law professors and commentators use a taxonomy of 5 as I present in the main text; a different source may be necessary if Becker goes with a taxonomy of 3, but I don't believe a cite is needed for my main text proposition._]

10. For a discussion of the presumption of patent validity, see, Doug Lichtman, *Rethinking Patent Law's Presumption of Validity*, 60 STAN. L. REV. 45 (2007).

11. For a discussion of patent invalidation, see, Christopher R. Leslie, *The Anticompetitive Effects of Unenforced Invalid Patents*, 91 MINN. L. REV. 101 (2006).

12. For a discussion of patentable subject matter, see, for example, Lilly He, In Re Bilski *En Banc Rehearing on Patentable Subject Matter: Farewell to Business Method Patents*?, 14 B.U. J. SCI. & TECH. L. 252 (2008).

13. Diamond v. Diehr, 450 U.S. 175, 185 (1981). There was also at one point in patent law a fourth exception called "business methods," where the claims covered items such as an accounting method or perhaps a method of demonstrating a product or a method of compensating a manager. How-

one may patent an application of one of those exceptions, like a computer system that utilizes a mathematical equation or a man-made bacteria that transforms a naturally occurring bacteria.[14]

Nevertheless, pure mathematical equations, by themselves, are not patentable because they fit within the abstract ideas exception to patentable subject matter.[15] Thus, patenting software poses conceptual difficulties because these inventions rely on algorithms.[16] However, the case law has evolved to where a process can pass the statutory subject matter criteria if the claimed process does not preempt a field of activity by presenting a claim that has sufficient machine-like components or recites a qualifying transformation.[17]

In this approach, cryptographic technology has two areas of difficulty when measured against patent law's statutory subject matter requirements. First, cryptography is itself an algorithmic science relying on math. Second, it is often implemented in software. This does not mean that there cannot be valid patenting of cryptographic technology. It only means that those claims must be sufficiently non-abstract. How to measure such non-abstractness is where the case law has waxed and waned over the last several decades.

Aside from the unique difficulties with the statutory subject matter criteria due to its exception for abstract ideas, software and cryptography are otherwise evaluated against the other four criteria without notable difficulty. By this I mean that the legal tests underlying these criteria do not have particular niche doctrines that are particularly challenging for software or cryptography. Thus, to evaluate whether a claimed cryptographic method

ever, this exception no longer exists. State Street Bank & Trust Co. v. Signature Financial Group, Inc., 149 F.3d 1368, 1375 (Fed Cir. 1998); accord In re Bilski, __ F.3d ___ (200_) (en banc).

14. Diamond v. Diehr 450 U.S. 175, 185 (1981) (holding that a computer system that relies on a mathematical equation is patentable subject matter); Diamond v. Chakrabarty, 447 U.S. 303 (1980) (holding that a man-made bacteria that consumes oil is patentable subject matter).

15. For a discussion of patentability of mathematical algorithms, see, for example., David J. Kappos, *A Technological Contribution Requirement for Patentable Subject Matter: Supreme Court Precedent and Policy*, 6 NW. J. TECH. & INTELL. PROP. 152 (2008).

16. The Supreme Court originally determined that some inventions implemented with computer software were not patentable because the claims were merely algorithms. *See* Gottschalk v. Benson, 409 U.S. 63 (1972); Parker v. Flook, 437 U.S. 587 (1978).

17. The Supreme Court retreated from *Gottschalk* and *Parker* by allowing claims implemented with software to meet statutory subject matter as long as the algorithm used in the software was only part of the invention, not the whole invention itself. Diamond v. Diehr, 450 U.S. 175 (1981). Later, the U.S. Court of Appeals for the Federal Circuit concluded that a "machine or transformation" test would apply to screen process claims for statutory subject matter. In re Bilski, __ F.3d ___ (200_) (en banc). As of this writing, the Supreme Court has heard oral argument after granting certiorari to hear *In Re Bilski* on appeal, but an opinion has not issued from the Supreme Court. [_cite needed?_] [_GRV says: the Supreme Court opinion will arrive within the next two months_]

meets utility,[18] novelty, non-obviousness,[19] or enablement, follows the same legal analysis as those tests are applied across other technologies. This is generally the case for patent law: it is mostly a unitary system that does not vary dramatically in legal doctrine for different areas of technology. This does not mean, however, that the appearance of patenting in a particular technology has the same market or innovation effects as patenting in other technologies or the same effect on the public domain.[20] This is because factors external to patent law, such as industrial structure and technology deployment modes, will influence patent law's effect in a field.

II. THE INCREASE IN CRYPTOGRAPHIC PATENTS

Cryptography's story includes non-patent legal issues. The United States government controls the export of cryptographic technology.[21] Basically, the more effective the cryptographic technology, the more stringently the government regulates it. The details of the export regulations are beyond this writing's scope, but cryptography's main public and press notoriety is from disputes about the extent of this regulation.[22] There is a rich literature reviewing the debates, which includes concerns by United States developers that they will lose market share to foreign cryptography developers. Some foreign countries do not regulate cryptographic technology export.

The other non-patent legal issue is that the United States government is involved in *de facto* standard setting with respect to cryptographic technology. This technology leadership involves both the government's own significant use of cryptography as well as its general interest in security for the informational assets that support the economy.[23] This governmental role in selecting a cryptography standard for its use appears in the next sec-

18. For a discussion of the utility doctrine, see, for example, STEVEN A. BECKER, PATENT APPLICATIONS HANDBOOK, 4:2 (2009).

19. For a discussion of non-obviousness, see, Gregory N. Mandel *Another Missed Opportunity: The Supreme Court's Failure to Define Nonobviousness or Combat Hindsight Bias in KSR v. Teleflex*, 12 LEWIS & CLARK L. REV. 323 (2008).

20. For a discussion of the public domain, see, e.g., Amanda Fitzsimmons, National Security Or Unnecessary Secrecy? Restricting Exemption 1 to Prohibit Reclassification of Information Already In The Public Domain, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 479 (2008). [_GRV says: The Heald article is about copyright, so I don't think it makes a good cite for the public domain contribution made by an expired patent._]

[21] *See* Commercial Encryption Export Controls, U.S. Dept. of Commerce, Bureau of Industry and Security, *available at* http://www.bis.doc.gov/encryption/ (last visited Mar. 18, 2009).

[22] *See* A. Michael Froomkin, *It Came From Planet Clipper*, 1996 U. CHI. LEGAL F. 15, 71-75 (1996), *available at* http://www.law.miami.edu/~froomkin/articles/planet_clipper.htm (last visited Mar. 18, 2009).

[23] *See* National Institute of Standards and Technology: Computer Security Division: Computer Security Resource Center (CSRC), *available at* http://csrc.nist.gov/ (last visited Mar. 18, 2009).

tion discussing early, yet still important, cryptographic patenting. Ongoing government standard-setting also influences patenting effects later as well.

Pioneer Patents for Modern Cryptography

Modern cryptography emerged in the 1970's from new solutions to the key exchange problem for encrypted communications. A cryptographic function, whether complex and implemented in software or simple and implemented by hand, uses a key to convert plaintext to ciphertext and to reverse the operation when necessary. When the encryption's only use is to keep data on one's hard drive secret, there is no need to share the key with anyone else. Only the user needs the key when accessing the data. The purpose of cryptography in that case is to keep everyone else from accessing the protected data. But when users want to communicate over an insecure channel, such as the Internet, they can do so by sending ciphertext so long as each user involved in the communication has the key. This creates a "chicken and the egg" problem: how do I send the key, which must be kept secret, to someone with whom I have never communicated when the only channel to that person is insecure?[24]

The cryptography system, where both sender and recipient must have the secret key, is called "symmetric." The pioneer patents that spawned modern cryptography and gave it applicability to the Internet did so by splitting the key into a public part and a private part. This is why the system is called public key cryptography. The sender looks up the recipient's public key (which is available through the Internet[25]), encodes a message with it, sends the resulting ciphertext to the recipient over an insecure channel (such as much of the Internet), and the recipient can use her private key to decode the message. The discovery behind public key cryptography

[24] Peter Wayner, *A Patent Falls, and the Internet Dances*, N.Y. TIMES, Sept. 6, 1997, at Tech.: Cybertimes, *available at* http://www.nytimes.com/library/cyber/week/090697patent.html (last visited Mar. 18, 2009).

[25] Saying that the recipient's public key is on the Internet, or that the recipient has previously sent the sender the recipient's public key, exposes another problem: verifying that the recipient is who she says she is and that the public key is hers. Cryptography is also used against this problem to implement a "digital signature." This technique essentially inverts the public/private key system described in the main text. To generate the digital signature, one cryptographically processes a signature-private-key against some information about the recipient, including her public key. There is then a signature-public-key which is used to verify that the information originated from whoever had the signature-private-key. For full effectiveness, however, the digital signature system requires a trusted third party to verify the recipient's digitally signed information. These authorities for the Internet are called Certificate Authorities (CA). There can be a hierarchy or chain of CA so that they can cross-verify each other. The CA issues a "certificate" which is "a computer-based record which: (1) identifies the CA issuing it, (2) names, identifies, or describes an attribute of the subscriber, (3) contains the subscriber's public key, and (4) is digitally signed by the CA issuing it." *See* A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 50-57, 58 (1996).

was how to arrange the mathematics so that it was nearly impossible to derive the private key from the public key. It is also nearly impossible to derive the plaintext from the ciphertext and the public key. This innovation arrived just as computers were becoming increasingly interconnected in a commercial setting and sufficiently powerful to quickly solve the equations required by these cryptographic functions.

Two groups secured patent rights related to these innovations. Martin E. Hellman, a professor at Stanford, and his graduate students first patented an approach for generating a shared private key for a sender and recipient using communications across an insecure channel. This is called the Diffie-Hellman patent.[26] Hellman and another graduate student also patented the "split" key approach described above. This formed the basis of the public key infrastructure system that underlies much of the Internet's information security apparatus.[27] This second patent is known as the Hellman-Merkle patent.[28] These patents are also known collectively as the "Stanford Patents."

Following in part the work at Stanford, a group of three professors at MIT patented an implementation of the public key approach. This patent is known as the RSA patent, each of the letters standing for the first letter of the last name of the three inventors.[29] The acronym also became the name of a Boston company that, as of 2009, is an important provider of information security technology and products.[30]

These three patents are among the pioneer patents of modern cryptography. Another notable pioneer is IBM's Data Encryption Standard (DES) patent.[31] This patented cryptographic technology was the United States government standard for non-classified sensitive data for over twenty years (1976 to 1997).[32]

[26] U.S. Patent No. 4,200,770 (filed Sept. 6, 1977), issuing in 1980 and expiring in 1997 (Diffie-Hellman patent).

[27] *See* Internet Engineering Task Force (IETF), Public-Key Infrastructure (X.509) (pkix), http://www.ietf.org/html.charters/pkix-charter.html (last visited Mar. 18, 2009); The Open Group, Public Key Infrastructure, http://archive.opengroup.org/public/tech/security/pki/ (last visited Mar. 18, 2009).

[28] U.S. Patent No. 4,218,582 (filed Oct. 6, 1977), issuing in 1980 and expiring in 1997 (Hellman-Merkle patent).

[29] U.S. Patent No. 4,405,829 (filed Dec. 14, 1977), issuing in 1983 and expiring in 2000 (RSA patent).

[30] RSA Security Inc., http://www.rsasecurity.com (last visited Mar. 18, 2009).

[31] U.S. Patent No. 3,962,539 (filed Feb. 24, 1975), issuing in 1976 and expiring in 1993 (IBM DES patent).

[32] *See* National Institute of Standards and Technology, *Commerce Secretary Announces New Standard for Global Information Security*, Dec. 4, 2001, *available at* http://www.nist.gov/public_affairs/releases/g01-111.htm (last visited Mar. 18, 2009). *See also* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 735-38 (1995) (discussing how DES became the U.S. government standard and the controversy surrounding its selection).

The federal government is a big customer. When they specify a technology as their standard, vendors work to supply products implementing the standard. But if the standard is patented, and the patent is held by a third party such as IBM, do all of these vendors have patent infringement liability to IBM if they sell products embodying the standard to the government? The answer is yes – unless there is a license.

A license is a permission that acts as a defense in the case of a law suit. The simplest example comes from property law: if I pass you a note that says "come on my front yard and let's play catch," I won't succeed in suing you for trespass when you step onto my grass. Your defense is the license, i.e. the permission I gave you in the note. I granted you permission to violate a right I otherwise have: to exclude you from my property. Your act was technically a trespass, but one that was licensed. Sometimes the word "license" also means a contract spelling out this permission, along with other promises between the parties.

In the case of DES, the government announced that IBM would grant nonexclusive royalty-free licenses for use of the standard, even if the resulting device, software, or technology infringed the DES patent.[33] The government needed IBM to do this so that vendors could develop and supply products without fear of patent infringement liability.[34]

The pioneer patents each hold a unique place in modern cryptography's early history. The DES patent became notorious because it was the government's standard. There was suspicion about a "back door," a concern that aligned with separate but highly controversial United States government efforts in the 1990s to promulgate, through a variety of indirect pressures, cryptography technology that gave government access to the decrypting keys for law enforcement.[35]

The RSA patent and the Stanford patents had some commercial activity spring from their technology.[36] In particular, the lineage of the RSA patent lead to a primary vendor in the marketplace for cryptographic technology, software, solutions, and systems as of 2009.[37] Unlike the DES patent,

[33] Department of Commerce - National Institute of Standards and Technology, Announcing Draft Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard (DES), and Request for Comments, Vol. 64, ¶ 10, Jan. 15, 1999, *available at* http://csrc.nist.gov/groups/STM/cmvp/documents/des/fr990115.html (last visited Mar. 18, 2009).

[34] *See* Froomkin, *supra* note 32, at 895-96 (discussing how in the early 1990's the U.S. federal government's selected digital signature standard (DSS) was ignored by vendors until the government was able to cause the general availability of a royalty-free license for the patents that covered the DSS).

[35] *See* Froomkin, *supra* note 32, at 734-38.

[36] *See* RSA Data Sec., Inc. v. Cylink Corp., Civ. No. 96-20094 SW., 1996 WL 107272, at *1-*3 (N.D. Cal. Nov. 12, 1996).

[37] RSA Security Products, http://www.rsasecurity.com/node.asp?id=1155 (last visited Mar. 18, 2009).

the RSA and Stanford patents were not licensed under royalty-free generally applicable terms. As a result, there was some occasional patent litigation among developers and vendors. This litigation tended to follow the pattern where the pioneer patent holders sought to assert their patents against potential market entrants.[38] For a time, the pioneer patents were managed as a "pool" where complimentary technology holders cross-licensed the patents and sometimes offered all the patents in the pool as a licensing package to others.[39] The pioneer patents were so broad that they cast an influential shadow across the entire industry.[40] Even so, there was plenty of room to patent aspects of cryptography, as the next section shows.

The Growth in Cryptography Patenting

In raw numbers, cryptography patenting has grown dramatically since the pioneer patents issued. Table 1 below presents an assessment of the growth in the quantity of patents issued in the United States system over time that are assigned to cryptography under certain classes used by the U.S. PTO.

While the table shows substantial patenting increases each year, more information would be necessary to understand the numbers in full context. Undoubtedly, the increases are significant in their own right. One wonders, however, how the patenting increase compares to: (i) research and development expenditure increases for cryptography; (ii) increases in cryptography products introduced; or (iii) increases in cryptography-implementing code written and/or deployed. Another perspective would be to compare increases in cryptography patenting to increases in all software patenting, or to information technology patenting during the time frames presented in Table 1 below. The goal would be to understand, among other questions, whether the cryptography patenting increase is simply part of a larger phenomenon, or whether it outpaces the general rise in information technology patenting observed during the 1990's and early 2000's.

This article does not take the additional empirical steps suggested in the preceding paragraph. Even without these comparative baselines, the growth in cryptography patenting is fascinating. It illustrates that even

[38] *See, e.g.*, Schlafly v. Public Key Partners, No. Civ. 94-20512 SW, 1997 WL 542711, at *2 (N.D. Cal. Aug. 29, 1997). In this case, an RSA-related company asserted its patent against another entity selling digital signature technology. The case went in RSA's favor, resulting in a determination that the defendant entity should no longer sell the technology.

[39] Edward J. Radlo, *Legal Issues in Cryptography*, 13 No. 5 COMP. LAW 1, *10 (1996).

[40] RSA Laboratories, *What are the important patents in cryptography?*, http://www.rsasecurity.com/rsalabs/node.asp?id=2326 (last visited Mar. 18, 2009) (listing RSA's description of the cryptography patents that had or have influence on the technology).

with the pioneer patents in the backdrop, the patent system allows for significant patenting growth in a technology.[41] The Stanford Patents expired in 1997, and the DES and RSA patents expired in 1993 and 2000, respectively.

Even while the pioneer patents were active, there was still room in the field of cryptographic technology for patents to issue. This is in part due to the nature of the patent system. Most of these patents will never be litigated, and thus are unchallenged as to their validity after they issue from the PTO. And while the PTO applies the prior-art-based novelty and obviousness criteria, it is well known that PTO examiners spend a relatively small amount of time on each patent application, perhaps between one and three dozen hours.

Moreover, applicants can always claim narrowly which increases the possibility of issuance but decreases the likelihood that the patent will be valuable. As patenting increases in a field of technology, patent attorneys might be heard to say that the prior art in a field is "crowded." As patent density increases, it can decelerate the rate of patenting because there is now more prior art to overcome for new applicants. Additionally, as firms build substantial patent portfolios, other firms may be deterred from entering that particular market sector.[42] The result may be an aggregate deceleration in the rate of patenting.

However, from 2005 to 2009, as suggested by the classes of cryptography patenting shown in Table 1 below, the software industry saw an increase in software patenting. One possible explanation for this is that the increase in the rate of software patenting is a function of the growth of software products and services.[43] As a firm increases its available successful products or services it becomes more vulnerable to competitors desiring to enter the market for such.[44] In response, firms may increase their patent portfolios.[45] While an information technology recession existed from 2000-2002 during the dot-com era, thereafter there was a "rebirth of sales in many areas of software and services."[46] This rebirth may be one expla-

[41] *See generally* Ronald J. Mann, *Software Patents, Incumbents, and Entry*, 85 Tex. L. Rev. 1579, 1587 (2007) (arguing through empirical studies that the dramatic increase in software patenting from the 80's to the 90's was a result of an increase in confidence in the availability of patent protection for software, and a responsive market response to build a patent portfolio to protect investments against competitors).

[42] Mann, *supra* note 41, at 1606.

[43] *Id.* at 1600. (while an increase in products and services both accelerate the rate of software patenting, firms that specialize in putting more products into the market tend to have a bigger patent portfolio as there is a higher risk of competitors infringing on available products than services).

[44] *Id.*

[45] *Id.*

[46] Software & Information Industry Association. Packaged Software Industry Revenue and Growth, *available at* http://www.siia.net/software/pubs/growth_software05.pdf.

nation for the increase in software patenting, and in particular the surge in cryptography patenting.

The table also shows that the number of patents classified to cryptography in most cases at least doubled for each five-year period from 1980 to 2000. There were increases in the next five-year period, 2000 to 2004, but not a doubling in all classes. From 2005 to 2009, cartography patenting again increased, almost doubling the amount of patents from the previous five year period.

One cannot total the counts across columns in Table 1 below to arrive at the number of cryptography patents issued because some of the patents may be classified in multiple classes/subclasses – meaning that they would be counted multiple times in the total.[47] A little investigation and spot checking for the extent of the overlap suggests that the total is around fifteen thousand. Perhaps several thousand would have expired by the time of publication of this writing.

The increase in patenting does not appear to have launched an equivalent increase in cryptography patent litigation. The patent infringement suits involving cryptography, i.e. those that persisted long enough to generate a reported opinion from the federal court system, number only in the several dozen since the early 1980's.[48]

The character of these patent infringement suits is typical of patent litigation generally: developers suing other developers and/or their distributors. In other words, it is likely that only a small percentage of the commercial disputes among cryptography technology providers resulted in a patent infringement suit. This assumes many more disputes than suits, but if the logic is correct, the most likely explanation is two-fold. First, parties are probably willing to license their technology, perhaps to help promote user adoption of the technology. Second, perhaps developers can readily patent around the existing patents. This second reason is especially plausible when an entire field of technology is growing and many practical advances are occurring to apply the principles in a wide variety of technological contexts.

For example, just because the pioneer patents discussed issues related to cryptographic keys this does not mean that there aren't many opportunities to claim new inventions for keys. A search in the United States PTO's patent database, around the time of this writing, for patents in the general

[47] The data in the table was obtained using the U.S. PTO's public advanced search interface, which limits the query text length and prohibits a combined query to get a true total.

[48] This conclusion is based on a search and review of U.S. Federal court cases that were reported but not necessarily precedential, and having terminology related to cryptography.

cryptography class (denoted with the number 380) with the word roots "key" and "manage" in the patent title returns one-hundred and six results, with issue dates beginning in 1981 and running through 2009.[49]

In Table 1 below which presents an assessment of the U.S. patents issued that are classified to cryptography, of importance is the definition that the PTO assigns to the three classes that implicate most U.S. cryptography patents: U.S. Class 380[50]; U.S. Class 705[51]; and U.S. Class 713[52]. Thus, the footnotes give further details about those classes and the searching within each. Specifically, the quantities reported under the columns in classes 705 and 713 do not exclude patents reported in the counts of the other column because they are classified in both, but do exclude patents reported in class 380. On the other hand, the column reporting counts in

[49] The search text is: ccl/380$ and ttl/key$ and ttl/manage$. On March 22, 2009, this search in the U.S. PTO database returned one-hundred six results. One example is U.S. Pat. No. 6,738,905 (filed Apr. 14, 1999), entitled "Conditional access via secure logging with simplified key management." The patent relates to encrypting content for distribution, with likely applications in entertainment delivery.

[50] U.S. Class 380 is defined as follows.

This class includes equipment and processes which (a) conceal or obscure intelligible information by transforming such information so as to make the information unintelligible to a casual or unauthorized recipient, or (b) extract intelligible information from such a concealed representation, including breaking of unknown codes and messages.

Class Definitions, Class 380, 380-1, *available at* http://www.uspto.gov/go/classification/uspc380/defs380.pdf (last visited Apr. 17, 2009). Class 380 does not include all cryptography, however, because it excludes cryptography in "the specific environments of (a) business data processing or (b) electrical computer or digital processing system support. Such subject matter is classified elsewhere in the classes." *Id.* Note that in item (b) the word "support" means technical, internal operational capabilities that enable the computer to function. "Support" does not mean human assistance to help users with the computer or digital processing system.

The search in Class 380 used the following search text in the U.S. PTO's Advanced Patent Search page, with the years changed accordingly for each entry in the table and setting the year filter from 1790 - present:

ISD/1/1/1970->12/31/1974 and ccl/380/$

[51] U.S. Class 705 is for data processing and calculation where "the apparatus or method is uniquely designed for or utilized in the practice, administration, or management of an enterprise, or in the processing of financial data." Class Definitions, Class 705, 705-1, *available at* http://www.uspto.gov/go/classification/uspc705/defs705.pdf (last visited Apr. 17, 2009).

The Search in Class 705 excluded patents in the Class 380 to prevent double-counting among those two classes. The search in Class 705 used the following search text to target subclasses related to cryptography in the U.S. PTO's Advanced Patent Search page, with the years changed accordingly for each entry in the table, and setting the year filter from 1790 - present:

ISD/1/1/1970->12/31/1974 and (ccl/705/5? or ccl/705/6? or ccl/705/7? or ccl/705/8? andnot ccl/380/$)

[52] The Search in Class 713 excluded the Class 380 and Class 705 patents to prevent double-counting among those two classes. U.S. Class 713 is for the internal aspects of electrical computers and digital processing systems, including items such as memory management, hardware interfacing, and system security and protection. Class Definitions, Class 713, 713-1, *available at* http://www.uspto.gov/go/classification/uspc713/defs713.pdf (last visited Apr. 17, 2009).

The search in Class 713 used this search text to target subclasses related to cryptography in the U.S. PTO's Advanced Patent Search page, with the years changed accordingly for each entry in the table, and setting the year filter from 1790 - present:

ISD/1/1/1970->12/31/1974 and ((ccl/713/15$ or ccl/713/16$ or ccl/713/17$ or ccl/713/18$ or ccl/713/19$ or ccl/713/20$) andnot (ccl/705/5? or ccl/705/6? or ccl/705/7? or ccl/705/8? or ccl/380/$))

class 380 will include any patents also additionally classified in either class 705 or 713. Fundamentally, two realities generate these complications. First, the fact that a particular patent can, and often will be, classified into multiple classes and subclasses. Second, there was a preference to undertake this research using the most publicly available searching tool, the PTO website itself, and its searching tools limit the efficacy of the reported counts for absolute quantization purposes. For purposes of the article's argument, the main point, however, is reasonably well evidenced: the substantial growth in cryptographic patenting.

Table 1 – Patents Linked to Cryptographic Classifications in the U.S. Patent System

PTO Class	380	705	713
1970-74	155	3	7
1975-79	257	8	10
1980-84	310	25	16
1985-89	608	59	57
1990-94	1,145	106	199
1995-99	1,809	319	385
2000-04	2,155	638	1,106
2005-09	4,486	1,920	4,882
Total:	10,925	3,078	6,662

III. CRYPTOGRAPHIC PATENTS MOVING FORWARD

The PTO's classification scheme for cryptography highlights its embeddable characteristic and effectively optional nature for most systems where it might be embedded. The broad cryptography class, number 380, differentiates two classes, 705 and 713, where cryptography is, respectively, embedded in enterprise information technology or in the internals of a computer or its operating system. By total patent classifications in Table 1 above, the patents issued and classified for the embedded classifications probably outnumber those in the general class, assuming that the overlap due to patents with multiple classifications does not upend this estimation.[53]

[53] The main text estimates that the total is around fifteen thousand, with perhaps several thousand expired. In addition to these three classes, the inquiry examined scattered subclasses in ten other classes not so directly tied to cryptography: section 380 is the class for cryptography, but 705 and 713 are the

The embeddable nature of cryptography, however, is more pronounced than this comparison suggests: the technology is usually deployed as part of a larger system for communications, computing or entertainment delivery. For example, personal computers and notebook computers recently started providing internal smartcard readers where the smartcard is envisioned to hold cryptographic key information and perform some information security functions. Just because cryptography can be embedded, however, doesn't mean that it always is: information technology systems provide plenty of value without the high degree of information security modern cryptography promises. Their use has grown even in the face of spotty and incomplete information security, and while patenting for information security is on the rise.

Strategic or competitive policy responses to increased patenting should keep in mind the challenge of gaining critical mass with an embedded technology of wide applicability. An embedded component of a larger system can infringe a patent claiming only the component. Thus, for example, if a patent claim covers a smartcard interface method, a smartcard with the method implemented in its software would infringe. Likewise, a notebook computer would also infringe if it practices the method. A patent can have a laser-beam focus, targeting some small component of an overall system or device. But if making, using or selling that component is patent infringement, then making, using or selling the entire system or device is also infringement. If the component is critical to the overall system or device, the patent can inhibit the entirety even though its claims only cover the component. Patent attorneys sometimes state this result as follows: adding extra "elements" to a device that satisfies the claim does not avoid infringement of the claim.

There are several related vehicles to minimize patents in the product development and deployment landscape and minimize the patent risk for embedded cryptographic components: patent pools; privately governed patent-aware standard setting organizations; and patent-aware government driven standards. Cryptography has seen all three. The pioneer patents

delivery methods of cryptography via computing devices and information systems. Among the other ten examined classes, most had just a couple of subclasses that used cryptography (as opposed to directly emphasis on it as in class 380): 340, 358, 382, 386, 455, 463, 700, 902. Two, 725 and 726, had many dozens of subclasses that might use cryptographic technology. Among these ten classes, within the searched subclasses, the inquiry estimates that yet another (approximately) fifteen thousand patents could exist. All of the counts from searches of these ten classes are on file with the author. Finally, it should be noted that the inclusion of a subclass was based on an evaluation of the title of the subclass, not by extensive examination of all of the patents assigned to the subclass. Some spot checking occurred during the inquiry, but the numerical data reported herein is fundamentally based on the PTOs classification scheme and is thus limited to whatever categorization decisions the PTO made on a patent by patent basis.

were managed as a patent pool during the early 1990's.[54] In some patent pool arrangements, a group of companies each agree to allow the others in the group to use their patents under a cross-licensing arrangement.[55] The entire pool is sometimes available to others to license, perhaps by joining the group/pool, or perhaps at arms-length.[56]

Standard setting organizations are closely related to patent pools. Depending on how the standard setting organization deals with intellectual property, it may create mechanisms similar to patent pools by clearing a zone defined by the standard where competing developers can operate without fear of patent infringement liability from organization members. Smart policy demands that practicing the standard does not infringe any patents, or at least, it does not infringe any patents held by those organizations associated with, or who helped form, the standard. Within computing generally there is a widely observed variety in how such organizations deal with intellectual property: some organizations have done a good job setting ground rules upfront for patents, while others have not, sometimes to the detriment of the standard setting effort.[57] Good ground rules typically require standard-setting patent holders to commit in advance to at least reasonable and nondiscriminatory ("RAND") licensing terms, as well as perhaps identify all the patents that might cover the standard.

A recent example of private standard setting for embedded cryptographic functionality is the trusted computing initiative. The Trusted Com-

[54] Radlo, *supra* note 39, at *10.

[55] Carl Shapiro, *Navigating the Patent Thicket: Cross Licenses, Patent Pools, and Standard-Setting*, , Soc. Sci. Research Network, Working Paper, at 12-13 (2001), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=273550 (last visited Mar. 18, 2009).

[56] Patent pool licensing varies based on industry and technology factors, so this article is not the place to enumerate the possibilities. It suffices to note that pooling sometimes clears patents from blocking the path of product deployment, but may create a number of problems including the incentive for developers and suppliers to acquire patents in a race to gain leverage and influence within the pool. *See* Michael J. Meurer, *Business Method Patents and Patent Floods*, 8 WASH. U. J.L. & POL'Y 309, 324-26 (2002); Steven C. Carlson, *Patent Pools and the Antitrust Dilemma*, 16 YALE J. ON REG. 359, 367-69 (1999) ("[p]atent pools are private contractual agreements whereby rival patentees transfer their rights into a common holding company for the purpose of jointly licensing their patent portfolios.").

One well-known patent pool sometimes associated with data encryption is the DVD pool. *See* DVD 6C Licensing Agency: Patent Catalogue, http://www.dvd6cla.com/catalogue.html (last visited Mar. 18, 2009). This patent pool, however, does not directly cover the well-known Content Scrambling System (CSS)-a relatively weak cryptographic approach used by the entertainment industry to inhibit DVD copying. *See* The Openlaw DVD/DeCSS Forum Frequently Asked Questions (FAQ) List, § 2.11.2, *available at* http://cyber.law.harvard.edu/openlaw/DVD/dvd-discuss-faq.html (last visited Mar. 18, 2009).

[57] Mark A. Lemley, *Intellectual Property Rights and Standard-Setting Organizations*, 90 CAL. L. REV. 1889, 1904-07 (2002) (describing "standard-setting organization intellectual property rules as private ordering in the shadow of patent law," and noting that in "many industries IP owners regularly cross-license huge stacks of patents on a royalty-free basis. These patents are used defensively rather than offensively; their primary economic value is as a sort of trading card that reduces the risk that their owner will be held up by other patent owners").

puting Group (TCG) formed in 2003 to develop a secure PC architecture.[58] From this effort, personal computers have been available since 2005 with Trusted Platform Module (TPM) security chips.[59] TCG requires RAND licensing from its members.[60]

The cryptographic capabilities in TPM arose from critical mass in both demand-side need and supply-side feasibility. For the TCG, intellectual property management facilitated the supply-side feasibility. As a consortium of hundreds of companies, the TCG founding members had to decide ex ante how to deal with intellectual property rights including patent rights. The TCG operates as a non-profit corporation. Its bylaws prescribe patent licensing conditions for member companies. The consortium's goal is to develop a private standard with sufficient market potential for a bandwagon effect: many companies build to the standard so user adoption reaches critical mass with network economies. To do this, each member agrees to license any patented technology it contributes. They must grant licenses appropriate for the field of use as it maps to the consortium's standard. Also, when additions to the TCG specifications come from other members, each member has a review period: if they don't withdraw from the organization they are agreeing to license any patent claims that would be covered. Thus, the TCG's bylaws implement a type of patent pool. It is a standard setting organization with an embedded patent pool guarantee.

Besides recently-established standard setting organizations like the TCG, there are a number of longstanding industry association standardizing efforts. Within cryptography, one prominent organization is the Institute of Electrical and Electronics Engineers (IEEE). Standard setting by the IEEE (or other industry associations[61]) needs patent-aware mechanisms similar to those illustrated in the discussion about TCG. Even government promulgated standards must pay attention to patent law.

One of the pioneer patents, IBM's DES patent, was the government standard for non-classified data for about twenty years. In the late 1990's the National Institute of Standards and Technology (NIST) ran a competi-

[58] *See* Trusted Computing Group, https://www.trustedcomputinggroup.org/home (last visited Mar. 18, 2009); Bill Goodwin, *Trusted computing could lead to more supplier lock-in*, ComputerWeekly.com, Nov. 14, 2002, *available at* http://www.computerweekly.com/Articles/2002/11/14/190933/trusted-computing-could-lead-to-more-supplier-lock-in.htm (last visited Mar. 18, 2009).

[59] *See* Trusted Computing Group Backgrounder, at 5 (Jan. 2005), *available at* http://www.ict-economic-impact.com/images/TCGBackgrounder_revised_012605.pdf (last visited Mar. 18, 2009). [hereinafter TCG Backgrounder].

[60] TCG Backgrounder, *supra* note 59, at 5.

[61] Besides the IEEE, the Internet Engineering Task Force (IETF) is an important standard setting organization for cryptography. *See* Overview of the IETF, http://www.ietf.org/overview.html (last visited Mar. 18, 2009). The IETF manages the Public-Key Infrastructure standard. *See* Public-Key Infrastructure (X.509) (pkix), http://www.ietf.org/html.charters/pkix-charter.html (last visited Mar. 18, 2009).

tion for a new standard, which it called the Advanced Encryption Standard (AES). Its new standard became effective in 2001, specifying the Rijndael algorithm.[62] The Rijndael algorithm was not believed to be covered by any patents, and the cryptographers who submitted the algorithm did not desire patent protection for it. In addition, the NIST had the following to say about patents:

> NIST reminds all interested parties that the adoption of AES is being conducted as an open standards-setting activity. Specifically, NIST has requested that all interested parties identify to NIST any patents or inventions that may be required for the use of AES. NIST hereby gives public notice that it may seek redress under the antitrust laws of the United States against any party in the future who might seek to exercise patent rights against any user of AES that have not been disclosed to NIST in response to this request for information.[63]

The AES efforts lead to a significant number of products embedding the AES algorithm and submittal of their implementation to the government for conformity testing. Thus, the AES program not only promulgated a patent-aware open standard, it provides a certification for vendors who wish to prove that their implementation works according to the standard.[64] The number of certified implementations includes many hundreds at the time of this writing. Certification was more plausible for vendors because they did not have to be as concerned with patent infringement risk for the AES algorithm. In this way, the government's patent-aware standard setting activity virtually eliminated patent risk for the core algorithm, enabling developers to compete on non-patent benefits. It is also plausible that the winning algorithm's anti-patent stance helped it in the NIST evaluation.

In patent pooling and in private or public standard setting efforts, patents influence the competitive environment, but these mechanisms can ameliorate direct blocking effects. In other words, while patents cast a shadow on industrial self-ordering, they might not, under a patent-aware open standard or a patent pool, prohibit technology deployment by those in the pool or subscribing to the standard.

In the future, free and open source software sharing and collaborative development techniques may also engender these effects for cryptography. Open source software is a copyright-based licensing system. It requires that those who distribute such software ensure its free and open nature by

[62] *See* Advanced Encryption Standard (AES) Development Effort, http://csrc.nist.gov/archive/aes/index.html (last visited Mar. 18, 2009). [hereinafter NIST AES].
[63] *See* NIST AES, *supra* note 62.
[64] *See* Advanced Encryption Standard Algorithm Validation List, http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html (last visited Mar. 18, 2009).

not charging a royalty and by making the source code available.[65] While open source software may have patent liability like any other technology, the exposed source code is prior art that can inhibit future patent density. Open source software can help the prior art for some programming technology become "crowded," which makes future patenting more difficult or produces narrower patents in the future.[66]

The free and open source software movement has already indirectly influenced cryptography patenting. IBM is the leading patent holder of United States patents. In the early 2000's, IBM embraced the GNU/Linux operating system and generally converted to certain aspects of the open source software movement. The move wasn't altruistic. Open source software is complementary to IBM's hardware and service offerings. GNU/Linux is a more standardized and affordable operating system than IBM's proprietary version of UNIX, and this makes IBM's offerings more competitive. Due to its immersion in free and open source philosophy, however, IBM reevaluated which patents in its portfolio should be leveraged for product differentiation and which ones should be contributed, royalty-free, to support open standards and open source software: in early 2005 it decided to make hundreds of patents freely available for use by others.[67] It also pledged that any future patent contributions to an important information technology standard setting organization, the Organization for the Advancement of Structured Information Standards (OASIS), would be freely available. The free and open source community applauded this move because freely available patents are viewed as better than patents available under RAND licensing terms (although better for the free and open source software movement, it is not better than being patent free in the movement's view). OASIS is the source of a number of technical

[65] *See generally* Greg R. Vetter, *The Collaborative Integrity of Open Source Software*, 2004 UTAH L. REV. 563 (2004).

[66] The United States PTO initiated an effort in early 2006 to systematically make open source software available as searchable prior art for its examiners. John Markoff, *U.S. Office Joins an Effort To Improve Software Patents*, N.Y. TIMES, Jan. 10, 2006, *available at* http://www.nytimes.com/2006/01/10/technology/10blue.html (last visited Mar. 18, 2009).

[67] Steve Lohr, *I.B.M. Hopes to Profit by Making Patents Available Free*, N.Y. TIMES, Apr. 11, 2005, *available at* http://www.nytimes.com/2005/04/11/technology/11ibm.html (last visited Mar. 18, 2009). The article reported IBM's approach as follows below:

> [IBM] announced in January [2005] that it would make 500 patents – mainly for software code that manages electronic commerce, storage, image processing, data handling and Internet communications - freely available to others. And it pledged that more such moves would follow. [In April 2005], the company said that all of its future patent contributions to the largest standards group for electronic commerce on the Web, the Organization for the Advancement of Structured Information Standards, would be free.

Id.

standards in the forefront of cryptography.[68] IBM saw benefits in helping clear the patent-dense field for cryptography to obtain critical mass, and these benefits must have outweighed any potential benefit of following a product differentiation strategy with the contributed patents.

Not all companies have IBM's business mix, however, so some will choose the alternative to these cooperative approaches: product differentiation using patents. Companies sometimes base marketing claims on the fact that a "product is patented" - which really means that the company owns patent(s) with claims that presumably cover the product. Touting the patent(s) as a marketing benefit is not the only way to use them competitively: competitors risk infringement if their designs fall within the claim language. Some technology developers use portfolios of patents to create a buffer zone around a new product where competitors perceive risk to enter. One or two patents is usually a weaker buffer zone than a handful or dozen(s) of patents.[69] In cryptography, some companies are following the portfolio approach to technology differentiation.[70] This is typically effective when vendors already have significant market share and can license a portfolio that comprehensively covers an important technological strand or covers a user function end-to-end.

While many companies both in cryptography and in other fields build patent portfolios, there is no consensus as to what ultimate effect this produces.[71] Proffered explanations range from shielding future in-house product development and innovation, to having the portfolio available for cross-licensing in a patent pool or standard setting organization, to defensive patenting where the portfolio is an arsenal in the case of a patent litigation war.[72] Portfolio building will also "crowd" the prior art, making it

[68] *See* OASIS Committees by Category: Security, http://www.oasis-open.org/committees/tc_cat.php?cat=security (last visited Mar. 18, 2009).

[69] *See* Emily Nelson, *Toilet-Paper War Heats Up With New, Wet Roll*, WALL ST. J., Jan. 17, 2001, at B1 (noting that for its new product, Cottonelle Fresh Rollwipes, Kimberly-Clark is "guarding the roll and its plastic dispenser with about 30 patents").

[70] *See* Certicom Inellectual Property, Certicom Overview Brochure, Certicom: securing innovation http://www.certicom.com/index.php/certicom-intellectual-property (last visited Mar. 18, 2009) ("The Certicom Patent Portfolio includes more than 350 patents and patents pending worldwide… [c]erticom is known for many patents related, but not limited to the area of Elliptic Curve Cryptography (ECC) "); Voltage Security, *Voltage Security Awarded Five New Patents for Critical Innovations in Encryption Technology* (2007), *available at* http://www.voltage.com/pressreleases/PR070625.htm (last visited Apr. 17, 2009) (Voltage has recently been awarded five new patents for encryption technology innovations).

[71] *But see* Carl Shapiro, Navigating the Patent Thicket : Cross Licenses, Patent Pools, and Standard-Setting, in INNOVATION POLICY AND THE ECONOMY 119, 121 (Adam B. Jaffe et al. eds., 2001) (stating that the U.S. patent system "is in danger of imposing an unnecessary drag on innovation by enabling multiple rights owners to 'tax' new products, processes, and even business methods").

[72] Ronald J. Mann, *Do Patents Facilitate Financing in the Software Industry?*, 83 TEX. L. REV. 961, at 996-97 & n.180 (2005) ("The only stable equilibrium response of IBM is to obtain a sufficiently large portfolio of patents to induce Microsoft to enter into a formal or informal cross-licensing arrangement

more difficult for new entrants to both obtain broad patents and design around existing patents, unless the new company has a truly unique technological advance.

Cryptography patenting has produced collaborative responses in pooling and standard setting, and differentiating responses within portfolio building. Sometimes the two responses combine: a developer may build a portfolio for a differentiation strategy, but later decide to place the portfolio into a pool or offer it as a standard.

This reflects a vibrancy and dynamism in the field as developers perceive a growing market and try to meet the information security needs of individual and corporate users. Corporate users and even individual users have a heightened appreciation of the need for information security, even if at the individual level the propensity to take action toward greater information security is fragile. Increased patenting is a marketplace fact for this embeddable technology. Given that cryptography's primary uses are in communications and information storage/delivery, it needs critical mass for greatest effect. Critical mass on the Internet comes from the interoperability of standards and the resulting beneficial network economies from greater use.

The patent challenge to embedding cryptography is unlikely to go away. New responses, such as approaches based on open source software collaboration, may provide additional options for the future. Even as these take hold, the evolving patent landscape for software and business methods that began in the late 1990's continues to influence patenting in the field. No amount of information security will hide that fact.

under which neither side will sue the other for patent infringement.").