It's Not Just About The Money: A Comparative Analysis Of The Regulatory Status Of Bitcoin Under Various Domestic Securities Laws

Vesna Harasic

American University Washington College of Law

Follow this and additional works at: http://digitalcommons.wcl.american.edu/aublr

Part of the Securities Law Commons

Recommended Citation

This Note is brought to you for free and open access by the Washington College of Law Journals & Law Reviews at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in American University Business Law Review by an authorized editor of Digital Commons @ American University Washington College of Law. For more information, please contact kclay@wcl.american.edu.
NOTES

IT'S NOT JUST ABOUT THE MONEY: A COMPARATIVE ANALYSIS OF THE REGULATORY STATUS OF BITCOIN UNDER VARIOUS DOMESTIC SECURITIES LAWS

VESNA HARASIC

Introduction ........................................................................................................................................... 488

I. Bitcoin’s Unique Characteristics and Current Regulatory Classification ........................................... 488
   A. Entering the Bitcoin Market ........................................................................................................ 488
   B. Bitcoin Transfers ......................................................................................................................... 489
   C. Bitcoin’s Legal Uncertainty ........................................................................................................ 491

II. A Comparative Analysis of Bitcoin’s Classification as a Security in the United States, the U.K., Brazil, and Japan ................................................................. 491
   A. Although the United States Adopts a Broad Approach to Securities Regulation Compared to Other Countries, Bitcoin Does Not Fit Squarely Within its Securities Laws. .... 492
   B. Compared to the United States, the U.K., Brazil, and Japan Represent Varying Degrees of Flexibility for Securities Regulation ........................................................................ 496
   C. Despite Such Differing Jurisdictional Approaches, Bitcoin Does Not Fit Squarely within the Laws of the U.K., Brazil, or Japan ........................................................................ 498

III. Solution: Bitcoin as a “Quasi-Security” ......................................................................................... 501

*Staff member, American University Business Law Review, Volume 3; J.D. Candidate, American University, Washington College of Law, 2015; B.A. in Government, Cornell University, 2012. I would like to thank my editors, Heba Tellawi and Ernie Jolly, as well as, the entire American University Business Law Review staff for all of their hard work in editing this piece for publication. Most importantly, a special thank you to my family, especially my mother, for her constant love, support, and encouragement; I couldn’t have done it without you.
INTRODUCTION

The Internet revolutionized the world like nothing before. It allowed for various forms of communication and connectivity, yet produced a number of social, legal, and economic challenges. Evidently, scholars began to theorize that the Internet would lead to the development of new forms of digital currency. And, they were right.

This Note focuses on the regulatory status of a digital “currency” called Bitcoin. Specifically, it explores whether Bitcoin may be regulated as a “security” under various domestic securities laws. Part II summarizes the unique characteristics of Bitcoin and its current regulatory classification. Part III analyzes the securities laws of the United States, the United Kingdom (“U.K.”), Brazil, and Japan—four regional leaders in financial regulation. Part III also applies these laws to Bitcoin, arguing that Bitcoin does not fit squarely within the securities definitions of any country. Lastly, Part IV suggests a possible solution to regulating Bitcoin in the United States under a “quasi-security” framework. It recommends that the Securities and Exchange Commission (“SEC”) define Bitcoin as a “quasi-security” and pass regulations aimed solely at Bitcoin regulation, rather than trying to incorporate it into existing legislation. By promulgating new rules, the SEC can effectively spearhead the effort towards global Bitcoin regulation.

I. BITCOIN’S UNIQUE CHARACTERISTICS AND CURRENT REGULATORY CLASSIFICATION

This Section explains what Bitcoin is and how it works. It discusses the unique characteristics of Bitcoin, and gives a brief overview of its varying legal status around the world.

A. Entering the Bitcoin Market

Bitcoin is the first digital currency that allows two parties to directly exchange single monetary units without going through a central payment
system. The Bitcoin system is regulated entirely by computer software. It awards bitcoins to users through a “mining” program that solves various mathematical proofs and takes increasing amounts of computational power. Once users take time to download this program and use their computers to generate solutions, new bitcoins are issued. However, as the number of users in the system increases, the mathematical proofs become more difficult, which eventually slows down the production of bitcoins over time. Today, due to Bitcoin’s popularity, few users acquire bitcoins through the mining process; rather, they acquire bitcoins in exchange for goods and services, or they purchase them directly through online exchanges.

B. Bitcoin Transfers

Once a user enters the Bitcoin market, he or she may choose to engage in Bitcoin transfers. Transfers occur through a network operated by thousands of computers, similar to a music-sharing system like iTunes or Spotify.

3. See Derek A. Dion, I’ll Gladly Trade You Two Bits On Tuesday For A Byte Today: Bitcoin, Regulating Fraud In The Economy Of Hacker-Cash, 2013 U. Ill. J.L. TECH. & POL’Y 165, 168–69 (2013) (describing different ways that one can begin trading in Bitcoin and various forums that are used for this trading).


7. See Grinberg, supra note 5, at 163 (“As the number of miners in the network changes, the problem difficulty adjusts to ensure that bitcoins are created at a predetermined rate and not faster or slower. Currently, about 50 bitcoins are issued every ten minutes, although the rate will halve to 25 bitcoins in about two years and will halve every four years after that. At those rates, 10.5 million bitcoins will be created in the first four years, half that amount in the next four years, and so on, approaching but never reaching a total supply of 21 million bitcoins.”); see also Steve Forbes, Bitcoin: Whatever It Is, It’s Not Money!, FORBES (Apr. 16, 2013 10:50 AM), http://www.forbes.com/sites/steveforbes/2013/04/16/bitcoin-whatever-it-is-its-not-money/ (explaining that, unlike typical currencies, bitcoins have no intrinsic value and their real value is based entirely on supply and demand).

8. See Dion, supra note 3, at 169 (explaining that both legitimate and illegitimate organizations accept bitcoins in addition to traditional currencies).


individual messages. Each message has a personal identifier called an
“address,” and each address has an associated pair of public and private
keys, consisting of a string of numbers and letters. When an individual
transfers bitcoins to a recipient, the recipient sends his or her address to the
transferor. The transferor then adds the address and the amount of
bitcoins to the transfer message. Finally, the transferor signs the message
with his or her private key, and announces the public key to the recipient
for signature verification.

In addition, the Bitcoin system provides a built-in mechanism to prevent
individuals from copying and pasting the same digital addresses over and
over again—a process that is often referred to as “double spending.” The
traditional answer to the double-spending problem was a central
clearinghouse, such as a bank, to keep a database of all transfers made in an
account. However, Bitcoin found a way to alter this approach. After a
transfer is completed, the system automatically broadcasts the time of the
transfer and adds it to the Bitcoin “block chain.” The “block chain” is a
computer-generated, public record of all Bitcoin transactions, back to the
very first transaction. Every computer on the Bitcoin network has a copy
of the entire block chain. After an hour or two, each transfer is locked in
time by the massive amount of user transfers added to the block chain. The
use of this time-stamping process ensures that the same bitcoin is not
used in more than one transfer. Therefore, each individual bitcoin has an

work/ (last visited Jun. 19, 2014) (walking through the steps of a bitcoin transaction
using hypothetical individuals).
12. Id.
13. Id.
14. Id.
15. Id.
16. Id.; see Kaplanov, supra note 6, at 117 (describing the public key as an e-mail
address, and the private key as the password needed to authorize the email).
18. Cf. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System
(unpublished white paper), http://bitcoin.org/bitcoin.pdf (claiming that the Bitcoin
system was able to circumvent the concept of a clearinghouse because bitcoins do not
require any backing or “trust”).
19. See Kaplanov, supra note 6, at 11–18.
20. See Plassaras, supra note 10, at 385–86 (giving an in-depth description of
time-stamping and block chain procedures).
21. See id.
22. See id.
23. See Kelsey L. Penrose, Banking on Bitcoin: Applying Anti-Money Laundering
irreversible history of transfers, tracing its movement from one computer to
the next.24

C. Bitcoin’s Legal Uncertainty

Due to these unique characteristics, Bitcoin’s legal classification remains
uncertain. On the one hand, the United States has made significant efforts
to regulate Bitcoin as a currency, subject to federal anti-money laundering
regulations.25 On the other hand, the IRS recently announced that it would
consider Bitcoin a form of property, subjecting every Bitcoin transaction to
capital gains tax.26

Other countries have taken similar inconsistent approaches. Brazil has
refrained from labeling Bitcoin a currency, requiring Bitcoin holders to file
capital gains like any other security. The U.K. has stated that an official
legal classification is premature until regulators fully understand how
Bitcoin works;27 yet, it has also treated Bitcoin as a “taxable voucher.”28
Finally, Japan has openly acknowledged that Bitcoin is neither a currency
nor a financial product, but that digital currencies may be subject to new
trade rules in the future.29

Despite these differing views, one commonality remains: no country has
engaged in an analysis regarding Bitcoin’s classification under existing
securities laws.

II. A COMPARATIVE ANALYSIS OF BITCOIN’S CLASSIFICATION AS A

that the block chain stops others from “double-spending” their bitcoins and that if
someone tried to do this, the system would recognize the deficiency and reject the
transaction).

24. See id.

25. Angelo Young, US Treasury Department: Virtual Currencies (Read: Bitco
Need Real Rules To Curb Money Laundering, INTERNATIONAL BUSINESS TIMES (March

26. Richard Rubin & Carter Dougherty, Bitcoin is Property, Not Currency in Tax

27. Emily Spaven, HMRC: UK Bitcoin Exchanges Don’t Have to Register Under
Money Laundering Regulations, COINDESK (Jul. 8, 2013 2:39 PM), http://www.coindesk.com/hmrc-uk-bitcoin-exchanges-dont-have-to-register-under-
money-laundering-regulations.

28. David Gilson, Bitcoin in the UK: HMRC suggests bitcoins are ‘taxable

29. Tokyo Leaves Bitcoin Outside Financial Product Regulatory Framework,
ASIAN REVIEW (Mar. 10, 2014 7:00 PM), http://asia.nikkei.com/Politics-
SECURITY IN THE UNITED STATES, THE U.K., BRAZIL, AND JAPAN

The regulation of new, cross-border financial instruments, such as Bitcoin, is impeded by a lack of regulatory harmonization. Although the trend is shifting towards international harmonization of securities laws and standards, the existence of inconsistent national rules is a challenge for regulators around the world. Some jurisdictions, such as the United States and Brazil, have developed broad, inclusive definitions for securities in order to address new, unorthodox instruments, while other jurisdictions have not. This Part summarizes the securities laws of the United States, the U.K., Brazil, and Japan, and applies those laws to Bitcoin. These countries are not only considered leaders of securities regulation in their respective geo-political spheres, but also, have similar economic and financial structures.30 Taken together, they provide a representative sample of securities regulation around the world.

A. Although the United States Adopts a Broad Approach to Securities Regulation Compared to Other Countries, Bitcoin Does Not Fit Squarely Within its Securities Laws.

Securities regulation in the United States is broad due to its flexible definition of “securities.” According to the Securities Act of 1933,31 a security includes common financial instruments like stocks and bonds, as well as “investment contracts.”32 The Supreme Court has defined the broad, “investment contract” category through a four-part test—commonly known as the Howey test.33 According to this test, an investment contract

---

30. See INTERNATIONAL MONETARY FUND, UNITED KINGDOM: IOSCO OBJECTIVES AND PRINCIPLES OF SECURITIES REGULATION: DETAILED ASSESSMENT OF IMPLEMENTATION (2011), available at https://openknowledge.worldbank.org/bitstream/handle/10986/15973/807280ESWOBraz00Box379814B00Public0.pdf?sequence=1 (finding that the U.K. is the leading equity marketplace in Europe) appear to be in place”; see also INTERNATIONAL MONETARY FUND, BRAZIL: IOSCO OBJECTIVES AND PRINCIPLES OF SECURITIES REGULATION: DETAILED ASSESSMENT OF IMPLEMENTATION (2013), available at https://openknowledge.worldbank.org/bitstream/handle/10986/15973/807280ESWOBraz00Box379814B00Public0.pdf?sequence=1 (concluding that “the Brazilian equity market made impressive gains in market capitalization and liquidity over the past decade” compared to other Latin American countries); INTERNATIONAL MONETARY FUND, JAPAN: IOSCO OBJECTIVES AND PRINCIPLES OF SECURITIES REGULATION: DETAILED ASSESSMENT OF IMPLEMENTATION (2012), available at http://www.imf.org/external/pubs/ft/scr/2012/cr12230.pdf (stating that the legal and regulatory framework for the securities market in Japan exhibits a high level of implementation of international standards for securities regulation).


32. 15 U.S.C. § 77b(a)(1); see also § 78c(a)(10) (containing substantially identical language).

33. SEC v. W. J. Howey Co., 328 U.S. 293, 299–300 (1946) (holding that an investment in the cultivation, harvesting, and marketing of fruit from citrus trees is an
is: (1) an investment of money, (2) in a common enterprise, which is (3) expected to produce profits, due to (4) the efforts of others.\textsuperscript{34}

The four elements of the \textit{Howey} test have been developed through case law. First, the "common enterprise" element has been subject to two differing jurisdictional approaches.\textsuperscript{35} Under a horizontal commonality approach, courts have held that the "common enterprise" element is satisfied if the transaction involves a joint participation of investors sharing in the profits.\textsuperscript{36} Therefore, this approach involves a "tying" of each individual investor's fortune to the fortunes of other investors.\textsuperscript{37} Under a vertical commonality approach, a court need only find that the fortunes of an investor are tied to the expertise of the promoter, not to the fortunes of other investors.\textsuperscript{38}

Second, the "expectation of profits" element is only satisfied in situations where an investor is looking for a financial return, not a commodity or service.\textsuperscript{39} Thus, the "expectation of profits" must be the principal motivation for the investment of money.\textsuperscript{40} As the Court concluded in \textit{United Housing Foundation, Inc. v. Forman}, "profits" refer to "either capital appreciation resulting from the development of the initial investment . . . or a participation in earnings resulting from the use of investors' funds . . . ."\textsuperscript{41} For this reason, an investor must be "attracted

\textsuperscript{34.} \textit{Id.} at 298–99.


\textsuperscript{36.} \textit{E.g.}, \textit{Wals v. Fox Hills Dev. Corp.}, 24 F.3d 1016, 1018 (7th Cir. 1994) (explaining that the horizontal commonality approach requires that the fortunes of two or more investors be joined in a pooling of interests).

\textsuperscript{37.} \textit{Revak v. SEC Realty Corp.}, 18 F.3d 81, 87 (2d Cir. 1994); \textit{see Salcer v. Merrill Lynch, Pierce, Fenner & Smith, Inc.}, 682 F.2d 459, 460 (3rd Cir. 1982) (stating that the investment must be "part of a pooled group of funds"); \textit{see also Milnarik v. M-S Commodities, Inc.}, 457 F.2d 274, 276 (7th Cir. 1972) (emphasizing that the success or failure of contracts by other investors must have a "direct impact on the profitability of the plaintiffs' contract").

\textsuperscript{38.} \textit{E.g.}, \textit{SEC v. Cont'l Commodities Corp.}, 497 F.2d 516, 522 (5th Cir. 1974) (ruling that the critical inquiry in determining whether the common enterprise element is satisfied is whether the fortuity of the investments made with a particular promoter depend on the promoter's expertise).

\textsuperscript{39.} \textit{See United Hous. Found., Inc. v. Forman}, 421 U.S. 837, 856–57 (1975) (concluding that rental reductions and tax deductions resulting in savings do not qualify as an expectation of profits).

\textsuperscript{40.} \textit{Id.} at 852.

\textsuperscript{41.} \textit{Id.} (quoting \textit{SEC v. W. J. Howey Co.}, 328 U.S. 293, 300 (1946)).
solely by the prospects of a return on his investment."42

Third, the “efforts of others” element of the Howey test has also been subject to differing views. Various lower courts have concluded that investor participation in the generation of profits does not automatically foreclose the finding of an investment contract, even though the original Howey test required that profits result solely from the efforts of others.43 Courts have concluded that investors may be able to make small contributions to the generation of profits; yet, such contributions must be passive, and the efforts of others must predominate.44 Therefore, one important factor in the satisfaction of the “efforts of others” element is the amount of control that investors retain under their investment agreements.45

Finally, courts have applied the Howey test to a wide range of varying contexts like pyramid schemes.46 Using the Howey test, courts have concluded that investments in pyramid schemes constitute securities because they seek to attract monetary investments in a common enterprise, involving a promoter who organizes the entire scheme with the promise of future returns arising from the efforts of the promoter in attracting new investors.47 Although it would seem that pyramid schemes defy the horizontal commonality approach to the “common enterprise” element because the continued success of the scheme depends mostly on investors who end up luring more investors through favorable pronouncements regarding the scheme’s high returns, courts have applied the “common enterprise” element quite loosely in such circumstances.48

Given the broad, “investment contract” category and its liberal application, the remaining question is whether the SEC can regulate Bitcoin under existing securities regulations. So far, it appears that the SEC may regulate instruments based on the value of bitcoins under federal securities laws.49 But, can a bitcoin itself constitute a security? In other words, when

42. Id.
43. See, e.g., Robinson v. Glynn, 349 F.3d 166, 170 (4th Cir. 2003) (stating that, in addition to the Fourth Circuit, the Supreme Court has relaxed the “efforts requirement by omitting the necessity of the word “solely”).
44. See, e.g., SEC v. Galaxy Foods, Inc., 417 F. Supp. 1225, 1239 (E.D.N.Y. 1976) (explaining that the existence of an investment contract turns upon an analysis of the nature and extent of an investor’s participation and therefore, the efforts of others should be undeniably significant ones which affect failure or success of the enterprise).
47. See id. at 55.
48. See, e.g., SEC v. SG Ltd., 265 F.3d 42, 50 (1st Cir. 2001) (finding a security in an online investment game that depended on the ability of players to lure new players).
you buy a bitcoin, are you buying an investment in the hope of acquiring a future return?

Although the "investment of money" prong under the Howey test is easily satisfied because users buy bitcoins on exchanges using traditional forms of money, the other three elements require further analysis. First, one could argue that the "common enterprise" element of the Howey test is satisfied because users enter a network composed of like-minded users who all have a common desire to continue the block chain and add to Bitcoin’s value. Bitcoin may have “horizontal” commonality because the fortunes of all individual users are tied together; each individual user is better off when the value of Bitcoin rises and worse off when the value of Bitcoin drops. Bitcoin may not have “vertical commonality,” on the other hand, because the fortune of each individual user is not tied to the expertise of a sole “promoter,” especially since no single entity manages the entire Bitcoin community.

The last two prongs of Howey are also in dispute. With regards to an “expectation of profits,” most Bitcoin movement involves investors, speculators, and traders reacting to price fluctuations, seeking a return on their investment. Yet, despite this fact, the “expectation of profits” element may not be satisfied because the primary purpose for Bitcoin is the facilitation of commercial exchange. Moreover, “the efforts of others” prong may also point in either direction. On the one hand, Bitcoin’s profitability does not depend on the efforts of others because private users control every aspect of a transfer; but, on the other hand, Bitcoin users

(E.D. Tex. Aug. 6, 2013) (establishing that a Bitcoin-based fund is a security, subject to the SEC’s rules and regulations).

50. Grinberg, supra note 5, at 196–97. But see Dion, supra note 3, at 183-84 (suggesting that Bitcoins involve investments of CPU power for solving block chains, more so than investments of money).

51. See Grinberg, supra note 5, at 197 (indicating that Bitcoin has horizontal commonality because everyone is proportionally better off when the value of Bitcoin increases).

52. Id.; see Kaplanov, supra note 6, at 160 (stating that there is a “common enterprise of software developers who maintain bitcoin’s value”).

53. Grinberg, supra note 5, at 197. But see Jose Pagliary, Bitcoin Flaw Could Let Group Take Control of Currency, CNN MONEY (Nov. 4, 2013), http://money.cnn.com/2013/11/04/technology/bitcoin-flaw/ (reporting that according to a Cornell study, a single group may be able to control Bitcoin).


55. Grinberg, supra note 5, at 162–63.
play no active role in the system’s management or overall viability.\footnote{56}

Lastly, the SEC may choose to classify Bitcoin as a security due to its similarity to pyramid schemes.\footnote{57} Since its inception, Bitcoin has sought to lure new users into a “common enterprise,” involving both Bitcoin users and developers. The entire Bitcoin system lacks intrinsic value because its value depends only on the willingness of users to accept it.\footnote{58} Therefore, like a pyramid scheme, the more users that are brought into the system, the more likely it is that original users receive greater returns because the demand for bitcoins will rise, leading to an increased value for each individual bitcoin.

\textbf{B. Compared to the United States, the U.K., Brazil, and Japan Represent Varying Degrees of Flexibility for Securities Regulation.}

The U.K.’s approach to securities regulation is quite exclusive, and the “securities” concept under U.S. laws is most akin to the “investment” concept in the U.K.’s Financial Services and Markets Act (“FSMA”).\footnote{59} Although the FSMA provides a general definition for “investment,” whether a particular instrument constitutes an “investment” depends on a two-part analysis.\footnote{60} First, the activity must fall into the categories of investments enumerated in Part II of Schedule 2 of the FSMA; and second, the activity associated with the investment must be a “regulated activity.”\footnote{61}

The first step in the “investment” analysis is whether an instrument falls within the “specified” categories of investment in Part II of Schedule 2 of the FSMA.\footnote{62} This section includes “specified” categories including, but

---

\footnote{56. Grinberg, supra note 5, 197–99 (noting that it is up to the developers of Bitcoin to ultimately keep the system going).}

\footnote{57. Cf. VIRTUAL CURRENCY SCHEMES, EUROPEAN CENTRAL BANK (2012), available at http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf ("Therefore, although the current knowledge base does not make it easy to assess whether or not the Bitcoin system actually works like a pyramid or Ponzi scheme, it can justifiably be stated that Bitcoin is a high-risk system for its users from a financial perspective, and that it could collapse if people try to get out of the system and are not able to do so because of its illiquidity.")}
not limited to, stocks, deposits, electronic money, and options. Under the FSMA, "specified" is defined as "specified in an order made by the Treasury." Therefore, a "security" may include any instrument falling within the definitions of these enumerated categories, or any other instrument that the Treasury defines as an investment.

The second step in the "investment" analysis is whether an activity is a "regulated activity." In order to constitute a "regulated activity," two requirements must be satisfied: (1) the activity must be geographically linked to the U.K. "by way of business," and (2) the activity must relate to an investment of a "specified" kind. Overall, the FSMA considers the following activities to be "regulated activities," among others: dealing in investments, arranging deals or managing investments, and establishing collective investment schemes.

Brazil, on the other hand, adopts a fairly liberal approach compared to both the U.K. and the United States. Essentially, Brazil's definition for "security" is more inclusive because its category for "investment contracts" has fewer requirements than the Howey test. In 2001, Brazil codified the Howey test language into its Capital Market Law, rather than developing the test through litigation. Article 2 of The Brazilian Capital Market Law provides the following category: "(i) when publicly offered, any other collective investment instrument or contract that creates the right of participation on profits or remuneration, including those resulting from the rendering of services, and whose profits derive from the efforts of the entrepreneur or from the efforts of any third parties."

---

63. Id.; see Mazando, supra note 54, at 152 (listing the classes and categories of "specified" investments in Part II Schedule 2 of the FSMA); see also Robert C. Rosen & Gordon R. Walker, INTERNATIONAL SECURITIES REGULATION 8: UK-1-18—1-19 (Thomas Reuters/West, 10/2012).
64. § 22(5).
65. See Mazando, supra note 54, at 152 (explaining that “enumerated category” applies to all those categories in Part II of Schedule 2 of the FSMA or categories specified in secondary legislation).
67. § 22(1).
68. §§ 19, 22(1); see Mazando, supra note 54, at 151 (describing the first requirement as both a geographic test and a business test).
69. § 22(1)(a)—(b).
70. See § 22(2), sch. 2, arts. 2-9(A); see Mazando, supra note 54, at 151 (providing a list of regulated activities barred without prior FSMA authorization).
71. Law No. 10,303 of 2001 (Braz.).
73. Law No. 10,303, art. 2.
Like the Howey test, this category requires an investment instrument or contract that creates: (1) a right to share in the profits from (2) the efforts of an entrepreneur or any third parties. These two elements are similar to the last two elements of the Howey test: (1) an expectation of profits from (2) the efforts of others; yet, unlike the Howey test, this broad category does not require an investment of money, nor does it require the presence of a “common enterprise.”

Lastly, although Japanese financial regulations have been primarily modeled after U.S. laws, the Japanese definition for “security” is the most inclusive. According to the Japanese Financial Instruments and Exchange Act (“FIEA”), the term “security” means any “right” with economic characteristics or features. The FIEA provides a long list of equity and debt instruments, which are commonly known as securities. The FIEA also includes a broad category that may allow for Bitcoin regulation. This category suggests that, when taking into account various factors such as liquidity and the extent to which a particular novel instrument has similar economic characteristics to those securities listed within the FIEA, the Japanese Cabinet may choose to regulate a “right” as a security if it deems that such regulation is “necessary to secure the public interest or the protection of investors.”

C. Despite Such Differing Jurisdictional Approaches, Bitcoin Does Not Fit Squarely within the Laws of the U.K., Brazil, or Japan.

Bitcoin is unlikely to fall within the scope of the U.K. definition because

74. Id.; Robert C. Rosen & Gordon R. Walker, International Securities Regulation 4: JP-4—JP-5 (Thomson Reuters/West, 10/2012) (explaining that although various Japanese laws in the 19th and 20th century were modeled after European laws, the end of World War II created a shift for securities regulation and now most Japanese financial laws are substantially influenced by Anglo-American law).


76. Law No. 10,303.

77. See Rosen & Walker, supra note 74, at 4: JP 4–5 (explaining that although various Japanese laws in the 19th and 20th century were modeled after European laws, the end of World War II created a shift for securities regulation and now most Japanese financial laws are substantially influenced by Anglo-American law).


79. Id. art. 2; see generally Rosen & Walker, supra note 74 (giving a broad overview of the Japanese statutory definition for securities).

80. FIEA, art. 1; see Rosen & Walker, supra note 74, at 4: JP-19—JP-20 (listing and discussing all of the enumerated categories of securities that fall under Article 1 of the FIEA).

81. FIEA, art. 1, para. 1, xxi.

securities are confined to those instruments specifically enumerated within the FSMA, depriving regulators of the opportunity to interpret a broad category, like that of “investment contracts” under the U.S. regulatory regime. The FSMA’s list includes instruments that are commonly held to be securities by most jurisdictions, and Bitcoin is so novel that it is not yet commonly recognized as a security. The FSMA does, however, include one potential category under which Bitcoin may fall: the FSMA lists “electronic money” as a specified category within its investment definition. Because Bitcoin has been regarded as a form of digital currency used to buy goods and services online, it may easily fit within this specified category of investments; however, the particular scope of Bitcoin’s regulation under the FSMA will ultimately depend on the type of Bitcoin activity that is conducted.

In order to qualify as a “regulated activity” under the FSMA, an activity must be geographically linked to the U.K. “by way of business.” Many factors determine whether an activity is carried on “by way of business.” Some of these factors include the activity’s degree of continuity and the existence of a commercial element. Generally, it is difficult to argue that one’s activities do not satisfy the business element of the “regulated activity” test, as most companies dealing with the specified categories of investments discussed in the FSMA are carrying on some sort of business; however, the FSMA specifically lists “issuing electronic money” as the only type of “regulated activity” associated with the “specified” category of electronic money. For this reason, under the FSMA’s definition, regulating Bitcoin may be limited only to those individuals who partake in the issuance of individual bitcoins, that is, large Bitcoin exchanges.

In contrast, Bitcoin has a better chance of falling within the scope of the Brazilian definition for security. As previously mentioned, in order to fall within the scope of Brazil’s definition, Bitcoin must constitute an investment agreement that (1) creates a right for its users to share in the profits, depending on (2) the efforts of a third party. This second element

83. Mazando, supra note 54, at 156-57 (describing the FSMA’s limited scope when defining a “security”).
85. FSMA, §§ 19, 22(1).
86. Mazando, supra note 54, at 151.
87. Id.
88. See Rosen & Walker, supra note 58, at UK-1-17 (arguing that it is generally hard for anyone to argue that their activities relating to specified instruments are not by way of business).
89. FSMA, § 22(2), sch. 2; Rosen & Walker, supra note 58, at UK-1-17.
90. Law No. 10,303 of 2001 (Braz.).
is similar to the fourth element of the \textit{Howey} test, and therefore, a similar analysis may be used: although private users control every aspect of a Bitcoin transfer, Bitcoin’s management, profitability, and viability depend solely on the program’s developers, which ultimately satisfies the “efforts of a third party” element in the Brazilian regulatory system.

Contrastingly, the first element of the Brazilian definition is not easily satisfied with regards to Bitcoin. The Brazilian definition of security requires a \textit{right} to share in the profits, not just an \textit{expectation}, as stated under the \textit{Howey} test. This difference in language suggests that there may be a contractual component involved. As such, the Bitcoin system does not contractually guarantee a right to its users; Bitcoin users enter the system at their own risk without any guarantees from Bitcoin’s developers. Despite this disputed element, however, the Brazilian definition still does away with the “common enterprise” element—the hardest element to satisfy under the \textit{Howey} test—which shows that Bitcoin is, nonetheless, more likely to fall within the scope of Brazilian securities regulations, than U.S. securities regulations.

Lastly, Bitcoin regulation may be easiest in Japan. The \textit{FIEA} ultimately allows the Japanese Cabinet to regulate any “right” as a security if, after taking into account factors such as the liquidity and the extent to which a particular novel instrument has similar economic characteristics to those securities listed within the \textit{FIEA}, the Cabinet deems such regulation “necessary to secure the public interest or the protection of investors.”

First, bitcoins have similar economic characteristics to typical securities. Most securities, like stocks and bonds, have no intrinsic value because their value is derived from some other underlying valuable asset. Likewise, bitcoins do not have intrinsic value because their value is based entirely on supply and demand. Second, bitcoins resemble investments because the vast majority of activity in the Bitcoin market involves the movement of bitcoins through investors and traders on Bitcoin exchanges, and this activity is based on speculation regarding Bitcoin’s fluctuating market price.

Additionally, Bitcoin liquidity is quite limited because the entire system

\footnotesize
91. \textit{Id.}
94. See Carter Dougherty, \textit{Wall Street Bitcoin Fans Try to Make Real Money from Virtual}, BLOOMBERG (Jan. 6, 2014 10:52 AM), http://www.bloomberg.com/news/2014-01-06/wall-street-bitcoin-fans-see-to-make-real-money-from-virtual.html (stating that most Bitcoin enthusiasts are buying and holding the currency, betting that it will rise in value, while others are engaging in other types of investment activities such as trading, exchanging or storing bitcoins).
is designed so that there will only ever be a total of 21 million bitcoins in circulation.\textsuperscript{95} This limited liquidity means that Bitcoin merchants cannot comfortably sell their orders at a known or predictable price, and therefore, a sizable sell order itself could have the potential to drive down the entire market price for bitcoins.\textsuperscript{96} Due to Bitcoin’s illiquid nature, which may give rise to large price fluctuations, the Japanese Cabinet may deem Bitcoin regulation necessary for the protection of investors.

That being said, if one were to adhere to a strict interpretation of the FIEA, Bitcoin may actually fall outside the scope of the Japanese definition, as well. Like the Brazilian definition of a “security,” the FEIA uses the term “right”—not expectation—when defining a “security.”\textsuperscript{97} This suggests that there is a contractual component involved, and the Bitcoin system does not contractually guarantee any rights to its users, but rather bitcoin users enter the system at their own risk without any guarantees from the system’s developers. Therefore, Bitcoin may also fall outside the Japanese definition.

With such uncertainties for Bitcoin, the next Part provides a solution to domestic Bitcoin regulation. It recommends that the SEC regulate Bitcoin as a “quasi-security,” subjecting it to some reporting requirements, but not others.

III. SOLUTION: BITCOIN AS A “QUASI-SECURITY”

Despite the varying approaches to securities regulation analyzed in Part III, there is no existing definition that easily incorporates Bitcoin into existing laws. Although the United States has created a broad definition for securities, Brazil’s definition eliminates two key requirements. Contrastingly, the U.K. definition is the most exclusive, as it contains no broad category and allows regulation only of those instruments specifically enumerated within the FSMA. Finally, the Japanese definition adopts the most inclusive approach, allowing the regulation of any economic right that the Japanese Cabinet deems necessary to protect the public interest; yet, as previously mentioned, even this inclusive approach may give rise to uncertainties for Bitcoin regulation.

Generally speaking, amending the Howey test to mirror any of the definitions analyzed in this Note would prove particularly unhelpful as a proper regulatory solution to Bitcoin regulation, especially since bitcoins

\textsuperscript{95} See Robert MacGregor, Bitcoin is Money... It’s Just Terrible At It, YAHOO FINANCE (Jul. 29, 2013 4:57 PM), http://finance.yahoo.com/blogs/the-exchange/bitcoin-money-just-terrible-205752180.html (explaining that due to Bitcoin’s illiquid nature, the very act of disposing or selling Bitcoins may devalue them).

\textsuperscript{96} Id.

\textsuperscript{97} FIEA, art. 1.
themselves do not fall squarely within any approach. The Howey test has become a useful guide for courts when determining whether unorthodox investments fall within the scope of existing federal securities legislation. Therefore, amending Howey to facilitate the inclusion of digital financial instruments like Bitcoin may not only retroactively affect the status of other unorthodox instruments, but also, it may burden various agencies that have relied on this test for so long.

If amending existing securities regulations is not the proper approach to Bitcoin regulation, then what is? I argue that the United States and other jurisdictions should create new laws to successfully regulate Bitcoin as a "quasi-security." As an agency whose primary mission is to protect investors from risky investments that are not fully understood by the general public, the SEC should study the various risks associated with Bitcoin and decide whether it should extend certain requirements to bitcoin transactions and bitcoin-based products.

Ideally, the SEC should extend regulations to key actors in the Bitcoin community, requiring such entities to either register themselves or disclose material information. For example, the SEC could require large bitcoin wallet holders to register themselves, especially if they are in the business of buying and selling bitcoins. Similarly, the SEC could compel exchanges to periodically report large transactions, especially those transactions that are large enough to substantially alter the market value of bitcoins and create devastating losses for bitcoin users. It could require exchanges to disclose material facts regarding the amount of Bitcoin traffic in a day as well as any attacks or attempted attacks on the entire network. Lastly, the SEC could also resort to indirect control over Bitcoin by imposing amount limitations on individuals and/or entities that invest using bitcoins, as well as, establishing capital requirements on trading houses, banks, and other entities that hold bitcoins.

CONCLUSION

If not properly regulated, Bitcoin has the potential to create a disruptive and risky new global monetary system. Bitcoin not only poses grave money-laundering dangers, but also, it has the tendency to result in drastic price fluctuations, which may create various risks for users and investors in bitcoin-based financial products. Notably, regulators should seek a solution that will provide proper oversight and investor protection, without discouraging economic growth and investment.
As the global economy recovers from the 2008 financial crisis, it has become paramount for companies to protect their intellectual property assets abroad. This is especially true in countries that are notorious for lackluster statutory protection and inefficient policing and enforcement. This Note seeks to advise practitioners on the domestic trade secret regimes of Brazil, Russia, India, and China—collectively the BRICs. In this difficult economic climate, both the importance of trade secrets and the threat of misappropriation increase. In addition to outlining relevant domestic trade secret statutory provisions, this Note expounds on the most dangerous aspects inside each BRIC country. Finally, this Note explains which of the four BRIC countries is the safest and which represents the largest risk to American multinational enterprises that export their trade secrets and other intellectual property.

Introduction ..........................................................................................504

I. The Scope of the Current Domestic Trade Secret Laws of
   Brazil, Russia, India, and China ..........................................................506
   A. Domestic Trade Secret Law of Brazil .............................................507
   B. Domestic Trade Secret Law of Russia ...........................................508
   C. Domestic Trade Secret Law of India ..............................................509
   D. Domestic Trade Secret Law of China ............................................509
II. Analysis of the Domestic BRIC Trade Secret Regimes: The Positive and Negative Elements ..............................................................510
A. Analysis of Brazilian Trade Secret Law: An Adequate Law with Inadequate Penalties ..............................................................510
C. Analysis of Indian Trade Secret Law: The Absence of Statutory Regime Leaves Protection Lacking ..........................513

III. General Recommendations to American MNEs Intent on Expanding into the BRICs ........................................................................515

Conclusion ..................................................................................517

INTRODUCTION

In late 2003, the large investment bank Goldman Sachs released a paper entitled “Dreaming With BRICs: The Path to 2050.”1 The authors forecasted – quite optimistically – the rise of the “BRIC economies,” an acronym that refers to Brazil, Russia, India, and China.2 Using a number of projection factors, such as gross domestic product (GDP), GDP per capita, and GDP averages, the authors predicted that the BRICs would become a much more powerful, if not the most powerful, global economic force by 2050.3

To an extent, these predictions are on point – as of 2012, all of the BRICs have secured their positions as four of the top ten international economies.4 Despite this monumental growth, not even the BRIC

2. See id. at 4 (forecasting that by 2040, the BRIC nations could be worth more in dollar terms than the G6, which is comprised of the United States, the United Kingdom, Italy, France, Germany, and Japan).
3. See id. at 9 (predicting collective BRIC GDP to top the economic scales at US$ 84,201 billion in 2050); see also Six Global Trends Shaping the Business World: Emerging Markets Increase Their Global Power, ERNST & YOUNG, http://www.ey.com/GL/en/Issues/Business-environment/Six-global-trends-shaping-the-business-world—Emerging-markets-increase-their-global-power (last visited Oct. 6, 2013) (“By 2020, the BRICs are expected to account for nearly 50% of all global GDP growth. Securing a strong base in these countries will be critical for investors seeking growth beyond them.”).
economies were shielded from the economic recession of 2008.\textsuperscript{5} One resounding effect of the global recession on the BRIC countries was a loss of foreign direct investment (FDI); all four countries saw a dramatic drop from 2008 to 2009.\textsuperscript{6} Regardless of this temporary stagnation, FDI into some of the BRICs has picked up since 2009, and the four countries remain prominent targets for companies wishing to take advantage of the emerging markets.\textsuperscript{7}

Expansion into these countries can be a risky endeavor on many fronts, and this Note seeks to expound on one of them: the threat of trade secret misappropriation abroad. Companies inside of the United States have grown comfortable utilizing the extensive legal protections afforded to trade secrets by both state and federal law.\textsuperscript{8} Unfortunately, this level of protection is not available in the BRIC countries—in fact, each country ranks among the worst for intellectual property protection.\textsuperscript{9} American multinational enterprises (MNEs) must tread carefully when exporting their

\begin{itemize}
\item \textsuperscript{5} See GDP Growth (Annual %), THE WORLD BANK, http://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG (last visited Dec. 20, 2013) (presenting the differences in GDP growth rate for the BRICs before and after the global recession).
\item \textsuperscript{7} See id. (showing large increases in FDI for China and Brazil and small decreases for Russia and India); see also Merrill Matthews, Companies “Outsource” Because That’s Where the Sales Are, FORBES (July 20, 2012, 3:20 PM), http://www.forbes.com/sites/merrillmatthews/2012/07/20/companies-outsource-because-thats-where-the-sales-are/ (arguing that the reason why companies like Caterpillar and GE conduct almost fifty percent of their business abroad is because many expanding countries are experiencing a blooming middle class, creating new, profitable markets for U.S. companies).
\item \textsuperscript{8} See, e.g., ROBERT P. MERGES ET AL., INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 35 (Vicki Been et al. eds., 5th ed. 2010) (noting that every state has adopted some form of trade secret protection, most of which were modeled after the Uniform Trade Secrets Act, the origin being common law tort); see generally Theft of Trade Secrets 18 U.S.C.A. § 1832 (West 2012) (“Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly . . . steals . . . such information”); UNIF. TRADE SECRETS ACT § 1 (1985).
\item \textsuperscript{9} See Measuring Momentum: Global Intellectual Property Center International IP Index, UNITED STATES CHAMBER OF COMMERCE 24 (Dec. 2012), available at http://www.theglobalcenter.com/measuring-momentum-the-gipc-international-ip-index/ [hereinafter GIPC International IP Index] (ranking the United States as the most effective protector of IP rights, while listing Russia, Brazil, China, and India as the least effective in a report that examined different factors such as patent and related rights, copyright and related rights, and membership to international intellectual property treaties).
\end{itemize}
trade secrets into these lucrative markets.10

This Note acts as a practitioner’s guide to navigating the complex, and often times threadbare, trade secret regimes of the BRIC nations. Part II introduces the applicable laws and statutory provisions that provide protection to trade secrets in each country. Part III analyzes the BRIC trade secret regimes by presenting the best and worst aspects of each country’s laws. Furthermore, it identifies both signs of improvement in each BRIC country, and diagnoses what each country must do if it wishes to become a safe, viable target for expanding foreign businesses. Part IV provides advice for American MNEs that wish to expand into the BRICs by determining which, out of the four, is the safest in regards to trade secret and intellectual property protection. Finally, this Note concludes that it is an economic reality that the BRIC countries have reached a level of prominence that used to be reserved for Western, capitalist systems – it falls on the shoulders of each BRIC country to establish trade secret protection worthy of their new, preeminent position in the global arena.

I. THE SCOPE OF THE CURRENT DOMESTIC TRADE SECRET LAWS OF BRAZIL, RUSSIA, INDIA, AND CHINA

With the exception of India, each BRIC country has promulgated domestic trade secret protection in one form or another – largely holding to three common factors present in many trade secret definitions: (1) the information is not known to the public, (2) the subject confers economic benefit through its secrecy and confidentiality, and (3) the information is subject to reasonable efforts to maintain secrecy.11 In Brazil, trade secrets receive minor protection under Article Five, Section XXIX of the Federal Constitution and Article 195 of the country’s Industrial Property Law, which was passed in 1996.12 In Russia, Article 1465 of Part Four of the Russian Civil Code and the Federal Law on Commercial Secrecy protect


trade secrets to an extent. India proves to be the outlier, and does not provide any statutory protection for trade secrets. In China, trade secrets enjoy fairly thorough protection under the Anti-Unfair Competition Law of the People's Republic of China. This Part lays out the applicable statutory provisions for each country, and identifies what kinds of trade secrets are afforded protection.

A. Domestic Trade Secret Law of Brazil

Article Five, Section XXII of Brazil’s Federal Constitution guarantees the right to property. Further, Section XXIX of the same Article provides in part that, “the law shall ensure... protection of industrial creations...” This is augmented by the Industrial Property Law, which criminalizes the misappropriation of trade secrets – the text of Title V, Chapter VI, Article 195, Section XI states, in part, that a crime of unfair competition has been perpetrated by anyone who “divulges, exploits, or utilizes, without authorization... confidential knowledge,” if that knowledge can be used in industry and is not publically known. Section XII extends this protection to information that is obtained by illicit means or fraud.

Sections XI and XII provide protection to any “knowledge, information, or data” which has a use in industry or commerce, so long as it is not known to the public and would not be readily ascertainable by someone


17. Law No. 9,279, of May 14, 1996 (Industrial Property Law) at Title V, Chapter VI, art. 195, § XI.

18. Id. at art. 195, § XII.
well versed in the field, which sets an obviousness standard not seen in the other BRIC countries or the United States. This sweeping definition does not limit the scope of the law by enumerating a list of eligible subjects. In this respect, it is similar to the protection offered in the United States. Brazilian law is implicated in the event of misappropriation through breach of a contractual relationship, illicit means, or fraud, which closely mimics U.S. law.

B. Domestic Trade Secret Law of Russia

In Russia, trade secret protection derives its authority in part from Chapter 75, Part Four of Russia's Civil Code – outlining the subject matter as, "[I]nformation of any type ... including ... methods ... having real or potential commercial value because it is unknown to third persons, to which such persons have no legal open access and with respect to which the owner ... has introduced a regime of trade secret." Article 1472 of the same chapter defines misappropriation, stating that infringement of the exclusive right to a secret of production occurs when "a person who has illegally received information constituting a secret of production ... disclose[s] or use[s] this information ..." Article 1472 extends liability to those who have breached a commitment to maintain confidentiality, and halfheartedly describes the penalty for a breach. The inclusive definitions of both subject matter and scope of misappropriation are similar to those in the Uniform Trade Secrets Act in the United States.

The Federal Law on Commercial Secrecy expands on the trade secret protection outlined in Part Four of the Russian Civil Code. It regulates the establishment, amendment, and termination of the regime of commercial secrecy – a set of requirements that must be met before a piece of information can qualify as a trade secret. In order for a piece of information to qualify as a trade secret, it must meet the definition included in Chapter 75, Part Four of the Civil Code, and have the regime of

19. Id. at art. 195, § XI.
20. See, e.g., Merges et al., supra note 8, at 37 (explaining that the Uniform Trade Secret Act protects any information, so long as that information adds value to its owner and is not publically known).
22. Civil Code of the Russian Federation art. 1465 (Russ.).
23. Id. at art. 1472.
24. See id. (requiring those guilty of infringement to pay damages to the owner of the exclusive right to the secret of production, but omitting a method to calculate an amount).
commercial secrecy introduced, a process described in Article 10 of the Federal Law on Commercial Secrecy.\footnote{7} Once the process is complete, the information will fall within the purview of Russian trade secret law and gain protection.

**C. Domestic Trade Secret Law of India**

India is unique in the BRIC context because it is the only country out of the four that does not provide specific statutory protection for trade secrets, instead, it relies on its British common law tradition of tort and contract law.\footnote{28} Understandably, this dearth of trade secret protection presents a dangerous environment for American MNEs, the intricacies of which will be analyzed in Part III of this Note.

**D. Domestic Trade Secret Law of China**

Unlike India, China has passed an array of laws that protect proprietary information and trade secrets. In 1993, China passed the Anti-Unfair Competition Law of the People’s Republic of China, which is the keystone of the country’s trade secret protection.\footnote{29} While it is accompanied by a number of different laws that touch on trade secrecy to a lesser degree,\footnote{30} Article 10 of the Anti-Unfair Competition Law provides definitions for both trade secrets and misappropriation. Referred to as “Business Secrecy” by the Anti-Unfair Competition Law, trade secrets are defined as, “utilized technical information and business information which is unknown to the public, which may create business interests or profit for its legal owners, and also is [kept secret] by its legal owners.”\footnote{31}

\footnote{27. See id. (describing that an owner must provide a list of the information, establish a procedure to limit access to the information, keep a record of people allowed access to the commercial secret, regulate employee use, and affix an official “Commercial Secret” stamp upon material media and documents).}

\footnote{28. See, e.g., Baldia, supra note 14 (detailing that the absence of statutory protections can place US firm’s IP at risk if it does not carefully employ contractual mechanisms or rely on the common law tort of breach of confidence in the absence of a contract); see also Nomani and Rahman, supra note 11, at 345 (“There are no specific laws in India to protect trade secrets and confidential information. Nevertheless, Indian courts have upheld trade secret protection on [the] basis of principles of equity, and common law action of breach of confidence and contractual obligation”).}

\footnote{29. Anti-Unfair Competition Law of the People’s Republic of China, art. 10, 1993 STANDING COMM. NAT’L PEOPLE’S CONG. GAZ. (China).}

\footnote{30. See J. Benjamin Bai and Guoping Da, Strategies for Trade Secret Protection in China, 9 NW J. TECH. & INTELL. PROP. 351, 356–57 (2011) (detailing the relevant provisions of Chinese Contract Law, Company Law, Labor Law, and Labor Contract Law that allow an owner of a trade secret to impose confidentiality agreements upon employees).}

\footnote{31. Anti-Unfair Competition Law of the People’s Republic of China, art. 10, 1993 STANDING COMM. NAT’L PEOPLE’S CONG. GAZ. (China).}
Article 10 also provides a comprehensive three-part misappropriation provision. The first sentence prohibits theft, coercion, and the use of any other unfair method to obtain another’s business secrets; the second sentence makes it illegal to disclose or permit others to use the business secret without authorization; and the third sentence incorporates the breach of contract into China’s definition of trade secret misappropriation. Accordingly, in order to prevail in a Chinese trade secret action, the elements that must be proven are extremely similar to those in the United States.

II. ANALYSIS OF THE DOMESTIC BRIC TRADE SECRET REGIMES: THE POSITIVE AND NEGATIVE ELEMENTS

This Part examines the pros and cons of each BRIC country’s domestic trade secret regimes, paying especially close attention to the intricacies of each system and the facts that savvy MNEs should consider before exporting their trade secrets abroad.

A. Analysis of Brazilian Trade Secret Law: An Adequate Law with Inadequate Penalties

Despite the fact that the Brazilian Industrial Property Law does not expressly define trade secrets under that name, the law criminalizes the theft of confidential business information. While Brazil’s law does provide a large scope of subject matter eligible for protection, there are a number of glaring shortcomings associated with Brazilian intellectual property and trade secret protection, earning the country a poor reputation.

32. Id.
33. See e.g., Bai and Da, supra note 30, at 356 (outlining the elements as: (1) the trade secret is not publically known, (2) the trade secret provides economic benefit, (3) the trade secret is subject to reasonable measures to maintain secrecy, and (4) there is misappropriation by a “wrongdoer or third party”); see also UNIF. TRADE SECRETS ACT § 1 (1985).


35. See GIPC International IP Index, supra note 9, at 5, 24 (ranking Brazil third from last on overall IP protection); see also The Two Faces of Intellectual Property in Brazil, KNOWLEDGE@WHARTON (March 1, 2006) http://knowledge.wharton.upenn.edu/article.cfm?articleid=1339 (last visited Sept. 16, 2013) (quoting Kenneth Adelman, former U.S. Ambassador to the United Nations, saying “Brazil is a prominent member of the IP axis of evil”).
The first and most obvious problem associated with Brazilian trade secret law is its statutory penalty. Article 195 of the Industrial Property Law states that one guilty of trade secret misappropriation faces between three months to one year in prison, or a fine of an undisclosed amount. This minor penalty pales in comparison to those mandated under United States law, raising questions of the law’s deterrent efficacy. Moreover, the law does not specify the availability of either civil damages or injunctive relief, which adds more uncertainty as to which remedies can be sought.

Another noteworthy factor involves varying reports as to who can be charged with a crime of unfair competition. While the law itself says that anyone who “divulges, exploits, or utilizes, without authorization, confidential knowledge . . .” perpetrates a crime of unfair competition, existing literature claims that Article 195 of the Industrial Property Law simply added parties that can be found liable. If the literature is correct, limiting those who can be held liable for trade secret misappropriation reduces the law’s effectiveness.

Finally, the Brazilian judicial system itself can be an impediment to effective trade secret protection. The system is plagued with dysfunction caused by undue delays and the high cost of litigation. Corruption is present in some areas, and decisions regarding trade secret protection can be of poor quality due to the fact that very few cases have been brought.

36. Law No. 9,279, of May 14, 1996 (Industrial Property Law), at Title V, Chapter VI, art. 195.
37. See Theft of Trade Secrets 18 U.S.C. § 1832 (2012) (setting the penalty for trade secret misappropriation at ten years imprisonment or up to $5 million in fines).
38. See e.g., Trade Secret Theft: Managing the Growing Threat in Supply Chains, CENTER FOR RESPONSIBLE ENTERPRISE AND TRADE 1, 17 (2012), available at http://www.create.org/news-resources/resources/trade-secret-theft-supply-chains [hereinafter CREATE.ORG] (lamenting the uncertain nature of remedies in Brazilian law and reporting that trade secret protection is poorly established).
39. Compare Law No. 9,279, of May 14, 1996 (Industrial Property Law), at Title V, Chapter VI, art. 195, with Protection of trade secrets through IPR and unfair competition law, INT’L ASS’N FOR THE PROTECTION OF INTELL. PROP. 1 (Mar. 31, 2010) available at https://www.aiippi.org/download/commitees/215/GR215brazil.pdf (answering that one bringing a case in Brazil may hold the contractual partner, employee or ex-employee, employer, or the partner or administrator of another company who accessed the information through fraud liable for an unfair competition charge).
40. See, e.g., GIPC International IP Index, supra note 9, at 39 (reporting that it can take up to four years for a case to reach trial and often times a decade before litigation is complete).
41. See Robert M. Sherwood, Intellectual Property Systems and Investment Stimulation: The Rating of Systems in Eighteen Developing Countries, 37 IDEA 261, 295-99 (1997) (explaining in two parts that judicial integrity has been an issue in many highly-publicized cases and that the lack of trade secret jurisprudence leaves many
So, while Brazil does have an adequate trade secret law in place, the country needs to increase the penalties and remedies available, clarify who can be indicted, and overhaul its slow judiciary.

B. Analysis of Russian Trade Secret Law: A Trade Secret Regime with Questionable Government Intentions

Like Brazil, Russia's trade secret laws appear to be inclusive -- Part Four of the Civil Code provides a sweeping scope of covered subject matter and a solid definition of misappropriation. Yet, the country is still notorious for poor trade secret protection.

To begin with, there are a number of statutory issues that should be taken into account by any MNE expanding into Russia. First, is the lack of remedies available -- the statute provides for damages, but is silent when it comes to injunctive relief or criminal charges. Unlike other countries, the Federal Law on Commercial Secrecy requires trade secret owners to affirmatively "introduce the regime of commercial secrecy" -- a list of steps that must be taken in order to achieve statutory protection. In addition to these steps, the Federal Law on Commercial Secrecy includes another troubling measure -- Article 6 gives the Russian government carte blanche authority to demand access to a company's trade secrets, with criminal sanctions and court actions for those who do not comply.

Certain realities outside the country's statutory regime are also extremely troubling. Along with the provision allowing the Russian government to demand a privately held trade secret, it is widely believed that Russia's government is engaged in extensive cyber espionage. The clandestine

42. CIVIL CODE OF THE RUSSIAN FEDERATION art. 1465, 1472 (Russ.) (qualifying "any [type of] information" as a trade secret and illegal use or disclosure as misappropriation).  
43. See, e.g., CREATE.ORG, supra note 38, at 7 (blaming Russia's high threat level on poor police work, weak data privacy, and cybercrime).  
44. CIVIL CODE OF THE RUSSIAN FEDERATION art. 1465, 1472 (Russ.).  
46. See id. at art. 6.  
attitudes of the Russian government present a risk to American MNEs uncommon in other countries.\textsuperscript{48} If this were not enough, the Russian police force is infamous for failing to pursue reports of corporate data theft.\textsuperscript{49} Regardless of the seemingly comprehensive law, American MNEs that expand into Russia face the possibility that their valuable trade secrets will fall into the wrong hands or end up the property of the state.

\textbf{C. Analysis of Indian Trade Secret Law: The Absence of Statutory Regime Leaves Protection Lacking}

Out of the four BRIC countries, India is the only one that does not have some form of statutory trade secret protection.\textsuperscript{50} This is not to say that one cannot protect trade secrets in India – just that the protection available is limited in so far as the parties who can be held liable.\textsuperscript{51} Although there is not a codified definition of trade secrets in India, the Delhi High Court recently recognized the concept in the case \textit{American Express Bank, Ltd. v. Priya Puri}.\textsuperscript{52}

The problem in India is not that it lacks a statutory definition; instead the judicially recognized definition can only be used in cases involving the violation of contractual obligations or breach of confidence – both of which require a preexisting relationship between the parties.\textsuperscript{53} Herein lies the

\textit{Economic Secrets} (asserting that because the United States is the leading global economic innovator, foreign governments, including Russia, have a large incentive to try and pilfer economic and trade secrets).

\textsuperscript{48} See GIPC \textit{International IP Index}, supra note 9, at 67 (attributing weak trade secret protection, in part, to widespread industrial espionage).

\textsuperscript{49} See e.g., CREATE.ORG, supra note 38, at 19 (revealing corruption and poor skills among law enforcement to be the reasons behind the inefficient enforcement).

\textsuperscript{50} See, e.g., Baldia, supra note 14 (warning US businesses that the non-legal environment for trade secrets in India provides a substantial risk if the proper contractual mechanisms are not employed).

\textsuperscript{51} See, e.g., Nomani and Rahman, supra note 11, at 345 (recognizing that Indian courts will protect trade secrets on the basis of equity, common law breach of confidence, and violation of contractual obligation); see also Baldia, supra note 14 (explaining that the tort of breach of confidence only applies to fiduciaries and contractual obligation only applies to those who have agreed not to misappropriate trade secrets).

\textsuperscript{52} \textit{American Express Bank, Ltd. v. Priya Puri}, (2006) III LLJ 540, at page 2129, available at http://indiankanoon.org/doc/445135/ (“A trade secret can be a formulae, technical know-how or a peculiar mode or method of business adopted by an employer which is unknown to others.”).

\textsuperscript{53} See Baldia, supra note 14 (posing a hypothetical scenario in which an American company has its trade secrets misappropriated by an Indian subcontractor who has not entered into a contractual or fiduciary relationship with the American company as an example of a situation where recovery would be impossible).
danger of India's lack of trade secret regime: if an individual or entity that has no prior relationship to the company misappropriates an American MNE's trade secrets, there may be no route to recovery.\textsuperscript{54}

Considering this, it is important to utilize extensive contractual protections when exporting trade secrets into India.\textsuperscript{55} But, even if every contract is perfect, the risk of misappropriation by unknown third parties who have no prior relationship still exists, in addition to the burdens associated with a slow and archaic judicial system.\textsuperscript{56} These factors make India an inhospitable environment for trade secret exportation.


Out of all the BRIC countries, China's trade secret regime may be closest to the protection offered in the United States – both in scope and definition of misappropriation.\textsuperscript{57} Despite this comprehensive regime, a recent report found that, "China's growth has far outpaced its ability to create and enforce legislation or – even more importantly – cultural attitudes towards protecting digital privacy . . . ."\textsuperscript{58}

China's system, like Russia's, is rife with cyber espionage and questionable government attempts at extracting trade secrets from foreign companies.\textsuperscript{59} According to a 2011 US counterintelligence report, China's trade secret theft is motivated by the need for economic growth and a desire to compete with American firms.\textsuperscript{60} This is a risk that lies outside of the

\textsuperscript{54} Id.

\textsuperscript{55} See id. (imploring US companies to insist on contractual provisions that bind both Indian contractors and any subcontractors that are hired by them, making it clear that the US company has a right to enforce any violation of these provisions).

\textsuperscript{56} See CREATE.ORG, supra note 38, at 18-19 (attributing Indian judicial inefficiency to backlogged cases, hand kept court records, misplaced filings, and cycling presiding judges); See generally Baldia, supra note 14.

\textsuperscript{57} Anti-Unfair Competition Law of the People's Republic of China, art. 10, 1993 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. (China), with UNIF. TRADE SECRETS ACT § 1 (1985).


\textsuperscript{59} See Teplinsky, supra note 47, at 263 (explaining that proof has become public that the Chinese government has engaged in cyberespionage against the United States, including Coca Cola who owns one of the most famous trade secrets in the world); see also CREATE.ORG, supra note 38, at 19 (relaying an experience that General Motors had with the Chinese government where, in order to qualify for extensive government subsidies, demands were made that the car maker transfer a number of engineering and electronic trade secrets to Chinese officials; GM refused).

\textsuperscript{60} See Foreign Spies Stealing U.S. Economic Secrets, supra note 47, at 4-5 (expounding on the fact that Chinese intelligence services and private entities often use employees of US firms to steal confidential information using portable devices or
country’s statutory regime, and unfortunately, is difficult to mitigate.

Government corruption aside, there have been recent signs of hope from the Chinese judiciary regarding the protection of American MNE’s trade secrets. Shanghai’s No.1 Intermediate Court recently ruled for American pharmaceutical company Eli Lilly in an action against a former employee from one of its Chinese subsidiaries. Judge Liu Junhua ruled in favor of the plaintiff, using newly amended Article 100 of the PRC Civil Procedure Law, which provides injunctive relief for trade secret cases. This anecdotal evidence reinforces the importance of contractual provisions that mandate confidentiality. In addition, the United States and China continue to hold talks regarding cyber espionage practices. One can hope that the Eli Lilly case, along with the ongoing diplomacy, are signs of things to come – a China where trade secrets are afforded the protection they are due.

III. GENERAL RECOMMENDATIONS TO AMERICAN MNES INTENT ON EXPANDING INTO THE BRICS

Each BRIC country carries a unique set of risks that must be balanced against potential rewards. Every BRIC trade secret regime leaves much to be desired, although many of the problems fall outside of the substantive boundaries of the statutory structure. After a detailed side-by-side analysis of the four BRIC countries and their respective trade secret laws, it is difficult to say which country provides the best protection to foreign MNEs.


62. Id.


64. See Teplinsky, supra note 47, at 263 (explaining that diplomatic talks were prompted after evidence of cyber espionage became public).

65. See generally GIPC International IP Index, supra note 9 (noting that each BRIC country has difficulty enforcing the laws that are in place).

66. See id. at 5 (using the scoring method adopted by the study to show that because each of the BRICs are ranked so low in IP protection, it is hard to pinpoint an
For example, while China has the most promising and comprehensive
trade secret laws, it, nonetheless, suffers from abysmal enforcement
methods. Brazil’s laws seem to protect trade secrets as well, but the
available damages and penalties are insufficient to justify a large risk. Russia’s laws are adequate, but available damages are unclear and the
intentions of the nation’s government are, at times, questionable. India’s
lack of trade secret law is troublesome, and relying on the traditional
contract or tort laws leaves companies vulnerable.

This is an inexact science. Nevertheless, this Note seeks to make a
recommendation to practitioners. Even with all of its faults and failures,
China seems to be the best choice for overseas expansion. It has
enforcement issues, but the availability of civil damages, possible
injunctive relief, and even criminal punishment, gives American MNEs a
range of options to pursue if their trade secrets are misappropriated.
China also extends liability to third parties, even if their actions are
tangential to the initial wrongdoer. This increases possible routes to
equitable recovery. As China’s economy draws closer to the size of the
U.S. economy, its legal and judicial system will have to mature as well. Of
course, this would be welcome news to any MNE doing business there.

In regards to trade secret protection, India falls behind compared to the
other BRIC countries. This is not simply because the nation does not have
a codified trade secret regime, as one can attempt to protect oneself using
contract and tort law. What makes India a frightening place to export one’s

67. See Anti-Unfair Competition Law of the People’s Republic of China, art. 10,
1993 STANDING COMM. NAT’L PEOPLE’S CONG. GAZ. (China). But see Unsecured
Economies: Protecting Vital Information, supra note 58, at 13 (explaining that China,
along with Russia, have the worst reputations for pursuing security related incidents).
68. See Law No. 9,279, of May 14, 1996 (Industrial Property Law), art. 195 XIV,
DIÁRIO OFICIAL DA UNIÃO [D.O.U.] (Braz.) (displaying penalties ranging from three
months to a year in prison, or a fine).
69. See, e.g., Foreign Spies Stealing U.S. Economic Secrets, supra note 47, at 4
(claiming that because Russia views itself as one of the strategic competitors of the
United States, it has become one of the most aggressive consumers of U.S. economic
information).
70. See, e.g., Baldia, supra note 14 (explaining that the traditional “breach of
confidence” tort is applicable only to the fiduciaries of the company and that breach of
contract can only apply to parties with which the US company is doing business).
71. See Bai and Da, supra note 30, at 361 (listing the possible damage calculations
available in China as either plaintiff’s lost profits, defendants realized profits, or
reasonable royalty and explaining that once a plaintiff prevails on a claim, permanent
injunctions are possible).
72. See id. at 364 (noting that criminal liability can be extended to third parties
who either acquired or disclosed the protected information when the third party knew
or should have known that the information was acquired wrongfully).
trade secrets is the fact that even with contract and tort law, a company can only protect itself from half of the possible threats.\footnote{73}{See Baldia, supra note 14 (warning that tort law only applies to fiduciaries of the US company and that contract law only applies to those that the company has a contractual relationship with).} Contract law can hold employees accountable,\footnote{74}{See id. (emphasizing the need for strong contractual provisions).} and tort law can punish fiduciaries for breaches of confidence,\footnote{75}{See id. (acknowledging that India does recognize the common law tort "breach of confidence").} but consider the anonymous hacker who has no relationship with the company – India's existing system does not provide a clear route to recovery against such a person.\footnote{76}{See Nomani and Rahman, supra note 11, at 345 (detailing that the Indian courts have upheld protection of trade secrets based on breach of confidence, contractual obligation, and equity, but not explaining the implications of unknown third party thefts).} For these reasons, India is the riskiest destination when it comes to exporting one's trade secrets.

CONCLUSION

The global economy is here to stay. Business will continue to cross borders, oceans, and hemispheres. Technology will continue to increase efficiency, processes, and unfortunately, risks. MNEs must be wary of the legal systems of countries whose economic growth has outpaced their institutional sophistication – of which the BRICs are the poster children. The trade secret regimes in the BRICs are not adequate and severely need improvement. Until that happens, companies who export their trade secrets in the interest of tapping into new markets must use the utmost caution if they wish to keep them safe and retain their economic edge.