2011

Private Prediction Markets and Insider Trading: Avoiding The Orange Jumpsuit -- A Snapshot Of Status and Proposed Risk Mitigation Strategies

David J Rodziewicz, J.D.

Private Prediction Markets and Insider Trading: Avoiding The Orange Jumpsuit

A Snapshot Of Status and Proposed Risk Mitigation Strategies

By David J. Rodziewicz, J.D.

Table Of Contents

Table Of Contents

Private Prediction Markets and Insider Trading: Avoiding The Orange Jumpsuit

A Snapshot Of Status and Proposed Risk Mitigation Strategies

By David J. Rodziewicz [1]

I. Introduction

John Doe took the long way home after a hard day at work.[2] He really enjoyed how his new Mercedes E350 handled the curvy back roads. The navigation system was great at routing him around the traffic jams on the way into work for the last few weeks, too. John felt this was not bad for a maintenance man with two years of work at the company. He would make it home right before dinner with the wife and kids.

This unexpected bounty was thanks to John's participation in a game at the office where he and his fellow employees all made bets on the future direction of things. Some of the games dealt with world events; one was about the recent Presidential election. Last year, when the game asked about one of the Company's proposed future products, so many people bet that this would be industry changing, John saw the opportunity of a lifetime. John thought, buy the dream car, take a "lifestyles of the rich and famous" vacation, max out the kid's college savings, all with money left over. He said to himself, "Buy in big and cash out early, just like the bigwigs do." In a few months, the new products hit the market and everything in his life changed.

Turning into his side drive, John saw the kid's bikes in the yard, a black Ford sedan in front of the house, and his tearful wife on the front porch. His wife said, "Two men are waiting inside to talk to you. They have badges, FBI badges." Crying, she asked, "What did you *do*?"

The agents said John made an unlawful set of "insider trades" based on information not

[1] David Rodziewicz is the Managing Director of TransformationArts LLC and a former KPMG Consulting Partner, specializing in business operational restructuring and turnarounds. Mr. Rodziewicz was awarded his J.D. from Barry University's Andreas School of Law.

[2] This is a fictional account for illustrative purposes only.

[2] This is a fictional account for illustrative purposes only.

generally available to the public. They showed him records of the stock trades, his banking records, the kid's college fund checks, and even the receipt for the new Mercedes. They wanted to discuss this with him, now. John objected, "Inside information? Isn't that reserved for the President and CEO and not rank-and-file employees? How would I get inside information?" The agents responded, "Good point, we're going to visit the CEO next. We like to call on senior executives after bedtime. But you are still in the soup."

II. Background

The insider information and eventual windfall that attracted the interest of the Department of Justice and FBI resulted from a game played at work by Mr. Doe, called a Prediction Market ("PM"). This article will examine whether a stock trade, based on information garnered in a *Private* Prediction Market ("PPM"), rises to the level of Illegal Insider Trading ("IIT"). The article will also: introduce and define PMs; summarize IIT statutes, regulation, and judicial history; and analyze problems that arise at the nexus of the common business use of PMs and today's IIT environment. Finally, the article will propose changes to business process, regulation, and law in light of emerging technologies like PPMs.

A. Prediction Markets Defined

There is an old adage that hindsight is 20/20. But what if a business could possess "20/20 foresight?[3]" Thriving, successful businesses are constantly looking for breakthrough strategies, solutions, and tools. PMs are one type of these breakthrough tools targeted at looking into the future with greater acuity.

A PM, sometimes called a "game," is a miniature stock market created to trade around a

[3] HUGH COURTNEY, 20/20 FORESIGHT: CRAFTING STRATEGY IN AN UNCERTAIN WORLD 3-4 (2001).

question or set of questions related to a future event.[4] Generally, players trade with tokens or play money, although gambling markets exist. Winnings are also generally token in nature, but having *something* at stake is critical to the design of PMs.[5] PMs are predicated on the theory that a sufficient population of interested individuals, with varied views on a particular question or game, possesses insight on the likely answer to the question or outcome of the game. This notion is sometimes called, "the wisdom of crowds"; James Surowiecki authored a book on PMs by that title.[6]

The University of Iowa ("UI") has been a leader in the study and creation of PMs.[7] UI's PM for the 2008 Presidential election tracked actual results within less than one half a percentage point. UI's PM predicted Obama would receive 53.55% of the popular vote.[8] He received 53.2% of actual results tallied.[9] Public PMs like these have existed for years, addressing a variety of social, political, or entertainment questions like election results, sports contests, or box office tallies.[10]

Conceptually, a PM is not difficult to implement. [11] The designer develops a question with a finite set of outcomes.[12] Players buy a stake in a future outcome for a share price much like a share of stock.[13] At its simplest, a single outcome will win and other alternative outcomes

---

[4] Justin Wolfers & Eric Zitzewitz, *Prediction Markets in Theory and Practice* 2, Nat'l Bureau of Econ. Research Working Paper No. 12083 (2006), *available at* http://www.nber.org/papers/w12083.
[5] Renee Dye, *The Promise of Prediction Markets: A Roundtable*, MCKINSEY QUARTERLY (April 2008), *available at* http://www.mckinseyquarterly.com/The_promise_of_prediction_markets_2114. Winners take great pride in a PPM t-shirt at Google per roundtable quote; more so than nominal cash.
[6] JAMES SUROWIECKI, THE WISDOM OF CROWDS 3 (2004).
[7] University of Iowa Press Release, *IEM Within Less Than Half Percentage Point in Presidential Race Prediction*, *available at* http://tippie.uiowa.edu/news/story.cfm?id=2058.
[8] *Id.*
[9] *Id.*
[10] *Id.* The term Public PMs refers to PMs used in the public domain, generally accessible through special interest websites catering to PMs or the subject matter of the game (i.e., sports, box office, current events).
[11] *Supra* note 5.
[12] *Id.*
[13] *Id.*

will lose, so the winning unit value equals one.[14]

Like the stock market, perception of risk impacts price.[15] In the 2008 Presidential election example above, a PM share in Obama may have garnered twenty cents when he announced his run. Fewer voters, and correspondingly fewer players, were supporting Obama-to-win at that time. Just before the election, when Obama's poll numbers were higher and with competition and other uncertainties resolved, a share of Obama-to-win would have cost nearly three times more. In comparison to the eve of announcement, more open questions were resolved on the eve of election. Many factors influence the perception of risk and share value; these factors have an upward or downward aggregate impact on price.[16] Visibility to this price movement is one of the benefits a PM offers.

When Obama won the election, a player who bought shares of Obama-to-win at the time of his announcement would have earned one dollar for every twenty-cent share. A similar investor in McCain-to-win would have lost his/her investment whatever the purchase price. Winning would result in one dollar for the fractional amount invested, losing would forfeit one's investment.[17]

Corporations implement Private PMs ("PPMs") as a tool to harvest insight on a variety of questions related to operations, future products, or likelihood of success in internal or competitor initiatives.[18] Eli Lilly used PPMs to predict the market success of new drugs.[19] Intel's use of PPMs to allocate manufacturing resources beat traditional forecasting models.[20] GE uses PPMs

---

[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] Michael Abramowicz & M. Todd Henderson, *Prediction Markets for Corporate Governance*, 82 NOTRE DAME L. REV. 1343, 1350 (2007).
[20] *Id.*

in prioritizing new product investment.[21] The big box retailer Best Buy, compared results of gift card sales for a given periodic interval between their internal forecasting unit and an employee PPM asking the same question. [22] Best Buy's professional forecast varied from actual result by 5% while the PPM result was 99.5% accurate. [23]

A PPM in a business setting results in *both* "collective judgment" (i.e., forming a "collectively derived answer or estimate") [24] and information hidden within the minds of PM participants.[25] What if there is no dispersed aggregate information?[26] Alas, PMs are not a panacea. Game or question design is key to harvesting insight. If no "collective knowledge" exists among the participants, the game or question will offer little value. [27]

As noted above, PPMs are superior to mere polls or surveys in a number of ways. [28] Participants in a PM have something at stake, as opposed to a poll or survey where there is virtually no consequence for offering an opinion.[29] This behavioral trigger is foundational to the accuracy of PMs.[30] Moreover, polls and surveys serve as snapshots in time; [31] PMs are like a live camera feed. PMs reflect living, breathing, and evolving market change in real time.[32] As conditions impacting the question or game arise, the share prices adjust to market forces.[33] This quality makes PMs particularly valuable to corporations when PMs are used to predict and

---

[21] *Id.*
[22] *Supra* note 5. Regarding accuracy of PMs, your mileage may vary.
[23] *Id.*
[24] *Id.*
[25] Robin Hanson, Insider Trading and Prediction Markets (November 2007) *available at* hanson.gmu.edu/insiderbet.pdf. This article reminds us that Economics is a behavioral science. Perception of risk is the behavioral trigger impacting value. PMs are a new tool to harvest hidden data locked in the minds of one's staff.
[26] *Supra* note 5. Based on the question asked within a game, there may or may not be a wealth of information spread throughout the minds of the players. Game design matters.
[27] *Id.*
[28] *Supra* note 5.
[29] *Id.*
[30] *Supra* note 25.
[31] *Supra* note 19 at 1346.
[32] *Id.*
[33] *Id.*

manage risk.[34] Lastly, harvesting hidden information (mentioned above) from willing participants is at the core of a given PM's value.[35] Polls and surveys do not offer the same qualitative capacity.[36]

B. Illegal Insider Trading

IIT statutes, regulation, and case law strive to maintain a level playing field in regulated securities trading.[37] Imbalance occurs when one trader uses material nonpublic information to an unfair advantage over others.[38]

Generally, IIT encompasses the knowing, unlawful use of material, non-public information to trade in securities. Under the traditional theory of IIT,[39] the possession and use of insider information in IIT gives an unfair advantage over everyone else not otherwise in possession of that information (i.e., causes an imbalance).[40] Laws and regulations forbidding IIT are focused upon this fundamental unfairness in the flow of insider information and resulting harm to shareholders.[41] Advancing technology, however, presents an ever-present threat for regulating IIT. Periodically since 1929, individuals or enterprises have leveraged (or attempted to leverage) a variety of tools, techniques, or practices to unfair advantage.[42] Technology enabled IIT utilized the telegraph, telephone, and later computer based tools.[43] When technology is used to innovate IIT approaches, the resulting unfair advantage upsets otherwise stable

---

[34] *Id.*
[35] *Supra* note 5.
[36] *Id.*
[37] David M. Brodsky & Daniel J. Kramer, *A Critique of the Misappropriation Theory of Insider Trading,* 20 CARDOZO L. REV. 41, 42-43 (1998).
[38] *Id.* at 43-44.
[39] United States v. O'Hagan, 521 U.S. 642, 652 (1997).
[40] Henry G. Manne, *Insider Trading: Hayek, Virtual Markets, and the Dog That Did Not Bark*, 31 J. CORP. L. 167, 167-70 (2005); Jared L. Kopel & Ira Lee Sorkin, 6-80 *Securities Law Techniques* § 80.01 [1] (LEXIS 2009). The scope of IIT is broad and complex. IIT enforcement encompasses legislative, regulatory and judicial action and related history. This paper is not intended as a treatise on IIT, but rather as a summary of relevant components relating to our given scenario and PPM treatment.
[41] *Id.*
[42] *Id.*
[43] *Id.*

markets and undercuts confidence in investment values.[44]

Congress creates legislation, the Securities and Exchange Commission ("SEC") creates and enforces regulations, and the Court interprets and decides the fairness of both.[45] All three entities attempt to maintain a market balance for traders of securities.[46] Since no one can accurately predict future technology or business practices, one should not expect permanent stability in rules or regulations for securities markets. When technologies, business practices, or shocking lapses in ethics (personal or professional) enable unfair advantage, one or all of these entities react to restore market stability.[47] Sadly, their reaction lags behind, and rarely anticipates, the unlawful use of technology in relation to IIT.

A brief historical summary of IIT related statutes, regulation, and case law demonstrates how Congress, the SEC, and the Court have attempted to restore balance from previous IIT threats. As a direct result of the market crash of 1929, Congress enacted two foundational pieces of legislation.[48] The Securities Act of 1933 ("33 Act") provided baseline protections and guidelines for securities offered to the market.[49] The Securities Exchange Act of 1934 ("34 Act") provided the bases for prosecution of unlawful trades "involving manipulation and fraud in the secondary market."[50]

Section 10b of the 34 Act codified the SEC's authority to develop and deploy rules to maintain fairness. This statute provides the flexible, forward-looking framework for securities enforcement still currently used. Section 10b states:

> It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce or of the mails, or of any facility of

[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] *Supra* note 40.
[49] *Id.*
[50] *Id.*

> any national securities exchange . . . (b) to use or employ, in connection with the purchase or sale of any securities registered on a national securities exchange or any security not so registered, any manipulative or deceptive device or contrivance in contravention of such regulations as the [Securities and Exchange] Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors.[51]

To restore fairness to securities markets, Congress enacted this legislation to: a) make fraudulent securities transactions unlawful, and b) enable an ongoing mechanism to protect investors.[52]

Based upon this authority, the SEC established Rule 10b-5 in 1942.[53] This foundational set of regulations issued by the SEC set the cornerstone of enforcement activities related to IIT.[54] Rule 10b-5 states:

> It shall be unlawful for any person, directly or indirectly, by use of any means or instrumentality of interstate commerce, or of the mails, or of any national securities exchange,
>
> a. to employ any device, scheme, or artifice to defraud,
> b. to make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading, or
> c. to engage in any act, practice, or course of business, which operates as a fraud or deceit upon any person, in connection with the purchase or sale of any security.[55]

Since IIT is within this definition of a prohibited device, this SEC Rule and the previous statute provide the framework for prosecution of securities violations related to IIT.[56]

By the 1980s, advances in computing technology and the increased speed of information flow impacted securities markets internationally. In 1980, the Supreme Court decided *Chiarella v. United States*, articulating "material non-public information" as the core of the traditional theory of IIT.[57] Importantly, this case defined two elements related to the quality of information

---

[51] *Id.*; 15 U.S.C. § 78j(b) (2006).
[52] *Id.*
[53] *Id.*; 17 C.F.R. § 240.10(b)-5 (2009).
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] 445 U.S 222, 231 (1980).

in question: 1) material and 2) nonpublic.[58] The Court held that there is a fiduciary relationship between shareholders of a corporation and those who gain inside knowledge by virtue of their position.[59] For the insider, this relationship begets a "duty to disclose" or to refrain from "taking unfair advantage of uninformed . . . shareholders."[60]

The Supreme Court again clarified an SEC enforcement action in *Dirks v. SEC* in 1983.[61] The Court ruled that outsiders can be insiders.[62] In *Dirks*, the Court defined *outsiders* as temporary fiduciaries when they come into possession of insider information, and placed them under the same duty to disclose or refrain from trading as *insiders* in *Chiarella*.[63]

These two rulings provided clarification on two required elements of an IIT offense: 1) duties of fiduciaries to disclose or refrain from trading with respect to insider information,[64] and 2) the possibility of outsiders becoming insiders (or temporary fiduciaries) when they possess insider information.[65] These rulings restored balance by defining the offense of IIT and the responsibilities of individuals when trading in securities.

In 1984 Congress acted by affirming the Insider Trading Sanctions Act of 1984 ("ITSA").[66] The ITSA imposed more serious civil and criminal consequences for IIT by traditional and non-traditional insiders.[67] Congress acted again by passing the Insider Trading and Securities Fraud Enforcement Act of 1988 ("ITSFEA"), intending to modify penalties enacted in the ITSA.[68] The ITSFEA also specified *possession* of material non-public

---

[58] *Id.*
[59] *Id.* at 228.
[60] *Id.* at 228-29.
[61] Dirks v. SEC, 463 U.S. 646 (1983).
[62] *Id.* (Thanks to Professor Frederick Jonassen for this turn of the phrase.)
[63] *Id.* at 655.
[64] *Chiarella*, 445 U.S 222.
[65] *Dirks*, 463 U.S. 646.
[66] *Supra* note 40, § 80.13 [1]; 15 U.S.C. § 78a (2006).
[67] *Id.*
[68] *Supra* note 40, § 80.13 [1]; 15 U.S.C. § 78u-1 (2006).

information as an actionable violation.[69]

In 1997 the Supreme Court, articulated the misappropriation theory of IIT in *United States v. O'Hagan*.[70] The Court agreed with the Government's contention that, "Under this theory, a fiduciary's undisclosed, self-serving *use* of a principal's information to purchase or sell securities, in breach of a duty of loyalty and confidentiality, defrauds the principal of the exclusive use of that information." [71] This theory further states that "a fiduciary who '[pretends] loyalty to the principal while secretly converting the principal's information for personal gain . . . dupes' or defrauds the principal."[72] In effect, if a fiduciary or temporary fiduciary per *Dirks*, *uses* corporate information to the personal gain of the fiduciary, the *use* of the misappropriated information is fraudulent and actionable.[73]

More recently, the SEC issued Rule 10b-5(1) in 2000, in part responding and adjusting to the Court's ruling in O'Hagan.[74] The new rule states that if an individual makes a purchase or sale of securities, and is *aware* of being in possession of insider info (i.e., aware of possession and use, with scienter), then the purchase or sale is deemed to have been made "on the basis of" material nonpublic information.[75] As of this new regulation, *awareness* is the third element of IIT.[76]

The SEC also issued Rule 10b-5(2) in 2000. [77] The SEC extended its regulatory

---

[69] *Id.* There was some controversy associated with this legislation. The ITSFEA based the presumption of guilt merely upon *possession* of insider information without use or scienter. The Supreme Court corrects this in *O'Hagan*.
[70] *O'Hagan*, 521 U.S. at 652.
[71] *Id.* (emphasis added).
[72] *Id.* at 653-54 (*quoting* Barbara Bader Aldave, *Misappropriation: A General Theory Of Liability For Trading on Nonpublic Information*, 13 HOFSTRA L. REV. 101, 119 (1984)).
[73] *Id.*
[74] *Supra* note 40, § 80.07 [2][d]; 17 C.F.R. § 240.10b-5(1) (2009).
[75] *Id.*
[76] *Id.*
[77] 17 C.F.R. § 240.10b5(2) (2009).

interpretation making virtually any temporary fiduciary an insider.[78] The rule explicitly included family members in addition to professional services subcontractors.[79] These two SEC rules are significant because they extend the definition of fiduciary relationships and prohibited transactions deemed to be IIT.

Like elections, traffic, or even athletic competition, regulated markets require rules to efficiently function.[80] Imbalance of rule sets can emerge when new technology, techniques, or market conditions appear, resulting in an unfair information advantage.[81] To regain balance, a modified rule set must be defined. The evolution of securities law is an attempt on the part of Congress, the SEC and the courts to create and maintain a rule set. These rule sets instill confidence *and* deter chaos in complex systems.[82]

A significant violation of established rule sets was uncovered after the collapse of Enron Corporation in 2000.[83] In reaction to the abuses uncovered after that collapse, Congress enacted the Sarbanes-Oxley Act ("SOX") in 2002.[84] While SOX was not specifically directed at IIT, it increased the criminal penalty for "knowingly [executing or attempting to execute] a scheme or artifice" to twenty-five years in prison.[85] This legislation is significant to IIT balance because of the perceived deterrent effect of large criminal penalties for unlawful behavior. In 2007, SEC Chairman Christopher Cox commented that along with expansion of criminal penalties enumerated in SOX, *senior business executives* now have personal liability for unlawful

---

[78] *Id.*
[79] *Id.*
[80] THOMAS P.M. BARNETT, THE PENTAGON'S NEW MAP 9-10 (2004). Barnett speaks of rule sets as the basis for global homeostasis. Here, by analogy, I apply his logic to the balance (or disruption thereof) of securities markets. In securities markets, Congress, the SEC, or interpretation of the courts define and adjust rule sets.
[81] *Supra* note 40.
[82] *Supra* note 80.
[83] John R. Kroger, *Enron, Fraud, And Securities Reform: An Enron Prosecutor's Perspective*, 76 U. COLO. L. REV. 57, 58-59 (2005).
[84] *Supra* note 40, § 80.10 [4]; 18 U.S.C. § 1348 (2006).
[85] *Id.* In addition, 18 U.S.C. § 1350 (2006) criminalizes false reporting of a company's financials. This is a first for U.S. corporations and their senior executives.

accounting and financial behaviors, saying, "ours is the only country that requires an attestation [from senior executives] along with the independent auditor's report."[86]

III. Problem Statement

The question is whether a PM's output mimics insider information or enables IIT. Todd Henderson articulated the problem eloquently during McKinsey and Company's 2008 Roundtable on PM:

> Take the employee who sees a prediction market price on her dashboard and realizes, with some degree of confidence, that a certain drug is going to be a success. Is it illegal if she trades on this information in the real stock market? Is she an insider because she now has information that only a few top people had before? What kind of disclosure obligations does that put on a US public company?[87]

A. Elements of the PPM Hypothetical

It is important to carefully deconstruct the elements of this hypothetical PPM problem with some additional focus.

1. The principal actor has access to insider information by virtue of PPM participation.

This person is an employee, family member, friend, or professional services contractor. This person may be one of any potential class of temporary fiduciary, like John Doe, our maintenance man from the introduction.

2. The hypothetical PPM creates insider information as a byproduct.

---

[86] *Statement of U.S. Securities & Exchange Commission Chairman*: *Hearing Before the S. Comm. on Banking, Housing and Urban Affairs*, (July 31, 2007) (statement of Christopher Cox, Chairman, Securities and Exchange Commission), *available at* http://www.sec.gov/news/testimony/ts073107cc.htm.

[87] *Supra* note 5. Todd Henderson is a University of Chicago Assistant Professor of Law and former McKinsey and Company manager.

This individual participates in a game, or is associated with someone participating in the game (i.e., a "tippee"). The game is created by and for the exclusive use of a publicly traded enterprise for its internal nonpublic use. The sensitivity of the information revealed by participating in the game may range from facts as trivial as something one could determine from outside analysis or as sensitive as a trade secret.

3. The principal actor sees a compelling opportunity for gain.

The perceived information opportunity is compelling enough to incite this person to act. An expectation of windfall drives this compulsion.

4. The principal actor is fully aware the public does not have access to this information.

His/her stock trade is based upon nonpublic information, because the public has no access to the "game" or its output. The individual might not think beyond, "too bad for everyone else," or "I can make a killing because nobody else knows this." That individual possesses a sufficient awareness of the act but may or may not be aware of the consequences.

5. The principal actor actually buys or sells securities based on that information.

The act is more than mere possession, accidental use, or a simple oops. Instead, this individual makes a willful and significant market move. Also like John Doe, the winnings are significant.

In the hypothetical PPM's set of facts, there are two loci of liability to investigate. An individual may be solely liable for his/her acts. A corporation, however, may also be liable in a variety of ways.

B. Liability for the Individual

Based on this scenario, the SEC could argue that an enforcement action against the individual for IIT is warranted. SEC enforcement considers three elements: 1) materiality of

information, 2) nonpublic nature of information, and 3) awareness of material nonpublic nature of the information used when trading (i.e., scienter).[88]

Regarding the first element, explored in more detail *infra*,[89] the Court has interpreted the term materiality, broadly.[90] Materiality may be related to the simple business value of information or even be evidenced by the winnings.[91] Second, if a given business created an internal PPM with warnings like "company confidential information," "trade secret," or "internal use only," the target information could be more easily judged nonpublic.[92] The third element, awareness, is a given element in our PPM hypothetical. Awareness would need to be proven to satisfy the third element.[93] Bragging to co-workers, perhaps in an email, or voice mail message stating the same could suffice as evidence of awareness. The use of PPM data, then, in this hypothetical could be considered one of the "'manipulative and deceptive devices' prohibited by Section 10(b) of the Act (15 U.S.C. 78j) and § 240.10b-5" by the SEC as an instance if IIT.[94]

C. Liability for the Enterprise

Business liability is a much more complex question and (we hope) will be the topic of a future article. In summary, though, employers control the structure, content, and implementation of PPMs.[95] Publicly traded businesses are required to implement appropriate controls over

[88] *Concerning Insider Trading: Hearing Before the H. Judiciary Comm. On The Judiciary*, (Dec. 5, 2006) (testimony of Linda Chatman Thomsen, Director, Division Of Enforcement, U.S. Securities and Exchange Commission), *available at* http://www.sec.gov/news/testimony/2006/ts120506lct.pdf.
[89] *See* Section 4 *infra*, Analysis of Law.
[90] Colesanti, J. Scott. "Why *Materiality* May Someday Become Immaterial." LexisNexis® Expert Commentary (*visited* May 5, 2009).
[91] *Id.*
[92] 17 C.F.R. § 243.100-243.103 (2009); U.S. Securities and Exchange Commission, *Final Rule: Selective Disclosure and Insider Trading*, *available at* the SEC's website http://www.sec.gov/rules/final/33-7881.htm (SEC's discussion on selective disclosure guidelines under SEC rule FD).
[93] *Id.*
[94] U.S. Securities and Exchange Commission, *Preliminary Note to § 240.10b5-1(a)*, *available at* the SEC's website http://www.sec.gov/rules/final/33-7881.htm.
[95] *Supra* note 4.

sensitive data.[96] In light of these duties, enterprise liability might arise in a variety of ways.[97]

1. Aiding and Abetting

Enterprises may be found liable for aiding and abetting IIT as a secondary party, as explained in 15 U.S.C. § 78t(e) (2006). If, for example, an enterprise's lack of information controls, or management inaction is found to have knowingly provided substantial assistance to the principal violator, liability may attach.[98] Section 78t(e) states:

> Prosecution of persons who aid and abet violations. For purposes of any action brought by the Commission under paragraph (1) or (3) of section 21(d), any person that knowingly provides substantial assistance to another person in violation of a provision of this title, or of any rule or regulation issued under this title, shall be deemed to be in violation of such provision to the same extent as the person to whom such assistance is provided.[99]

2. Controlling Person Liability

A subset of aiding and abetting specific to employers is called "controlling person liability"; employers controlling actions of their employees may be jointly and severally liable for their actions.[100] 15 U.S.C. § 78t(a) (2006) states:

> Every person who, directly or indirectly, controls any person liable under any provision of this title or of any rule or regulation thereunder shall also be liable jointly and severally with and to the same extent as such controlled person to any person to whom such controlled person is liable, unless the controlling person acted in good faith and did not directly or indirectly induce the act or acts constituting the violation or cause of action.[101]

If during the course of assigned duties, participation in a PPM is part of an employee's compensated responsibilities, liability may attach. An innocuous conversation about stock value

---

[96] *Supra* note 86.
[97] This list is intended to be representative rather than exhaustive.
[98] Harold K. Gordon and Tracy V. Schaffer, *Recent SEC Actions Show Employer Liability for Insider Trading*, Special to Law.com (July 30, 2007) *available at* http://www.law.com/jsp/ihc/PubArticleFriendlyIHC.jsp?id=1185527216922 (*citing* Graham v. SEC, 222 F.3d 994, 1000 (D.C. Cir. 2000) (presenting elements of aiding and abetting)); 15 U.S.C. § 78t(e) (2006).
[99] *Id.*
[100] *Supra* note 98.
[101] *Id.*

or company growth with the boss, for example, might be enough to "directly or indirectly induce the act" of IIT.[102] An act demonstrating a lack of good faith would also trigger this type of liability.

3. SEC Regulation FD

The SEC introduced Regulation FD in 2000 to curb disclosure of material nonpublic information made by companies to select third parties.[103] Stated here:

> (a) Whenever an issuer, or any person acting on its behalf, discloses any material nonpublic information regarding that issuer or its securities to any person described in paragraph (b)(1) of this section, the issuer shall make public disclosure of that information as provided in § 243.101(e):
>
> (1) *Simultaneously*, in the case of an *intentional disclosure*; and
>
> (2) *Promptly*, in the case of a *non-intentional disclosure*.[104]

If the SEC regards information revealed through use of a PPM as material and nonpublic, disclosure rules of Regulation FD would apply.[105]

4. The Sarbanes-Oxley Act (SOX)

Finally, SOX holds businesses to a higher account in a variety of ways.[106] The Act states:

> Whoever knowingly executes, or attempts to execute, a scheme or artifice-
>
> (1) to defraud any person in connection with any security of an issuer with a class of securities registered under section 12 of the Securities Exchange Act of 1934 (15 U.S.C. 781) or that is required to file reports under section 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 780(d)); or
>
> (2) to obtain, by means of false or fraudulent pretenses, representations, or promises, any money or property in connection with the purchase or sale of any

[102] *Id.*
[103] 17 C.F.R. § 243.100-103 (2009).
[104] 17 C.F.R. § 243.100(a) (2009) (emphasis added).
[105] *Id.*
[106] *Supra* note 40, § 80.10 [4]; 18 U.S.C. § 1348 (2006).

> security of an issuer with a class of securities registered under section 12 of the Securities Exchange Act of 1934 (15 U.S.C. 781) or that is required to file reports under section l5(d) of the Securities Exchange Act of 1934 (15 U.S.C. 780(d));
>
> shall be fined under this title, or imprisoned not more than 25 years, or both.[107]

An enterprise, its officers, or specific employees, may be held civilly or criminally liable if they are associated with "knowingly [executing or attempting to execute] a scheme or artifice."[108] The statute can be used as an additional tool to deter and enforce IIT violations. If an egregious lack of controls, or facts which indicate management involvement in IIT exist, SOX civil and criminal penalties are possible.

Companies are wise to be cautious concerning SEC enforcement actions. A case is considered "successfully resolved" if it results in a favorable outcome for the SEC, including through litigation, a settlement, or the issuance of a default judgment.[109] In FY 2008, 92% of cases brought were "successfully resolved" in favor of the SEC.[110] Also, in FY 2008, the SEC deployed approximately 9% of their total investigatory resources to IIT related matters.[111]

D. One approach to the problem

Businesses assume a wide variety of risks in attempting to secure benefits from a PPM.[112] To mitigate these risks, Professor Tom W. Bell proposes the following four strategies.[113]

1. Segregating markets for traditional insiders from other markets.[114]

Professor Bell suggests companies should segregate PM by user type, separating

---

[107] 18 U.S.C. § 1348 (2006).
[108] *Id.*
[109] U.S. Securities and Exchange Commission, *In Brief FY 2010 Congressional Justification* (May 2009), *available at* the SEC's website http://www.sec.gov/about/secfy10congbudgjust.pdf
[110] *Id.*
[111] *Id.*
[112] Tom W. Bell, *Private Prediction Markets and the Law*, 3 THE JOURNAL OF PREDICTION MARKETS 89, 100-01 (2009).
[113] *Id.*
[114] *Id.*

executives and insiders from all other employees.[115]

2. Broadening safeguards against illegal insider trading to reach beyond traditional insiders.[116]

He recommends a "click-through" interface to make warnings and admonitions "routine and unavoidable."[117]

3. Treating the market's claims and prices as trade secrets. [118]

Next, he recommends that businesses should advise participants of the PPM via the same "click-through" interface "that claims and prices constitute the corporation's trade secrets."[119]

4. Setting up decoy claims and prices.[120]

Finally, he suggests a corporation might experiment with seeding a finite amount of frivolous claims and prices as a decoy to authentic data.[121]

Professor Bell's first strategy, that companies consider segregating classes of employees, erodes the basic value of a PPM - harvesting hidden information from *all* participating employees.[122] Executives, secretaries, loading dock workers, and janitors all matter in PPM participation.[123] A business could no more lace two employee-segregated games together than turn sausage back into a pig.[124] Depending on the specific question or game design, removal of these potential participants could skew the results so unfavorably that the margin of error would overshadow a reasonable expectation of return for a given PPM implementation. That

---

[115] *Id.*
[116] *Id.*
[117] *Id.*
[118] *Id.*
[119] *Id.*
[120] *Id.*
[121] *Id.*
[122] *Supra* note 5.
[123] *Id.*
[124] *Supra* note 4. Review the mathematical models within this working paper. The result of joining these two distinct PPMs would be akin to a statistical guess.

unintended outcome would defeat the purpose of a PPM, making businesses much less likely to open their wallets in the first place.

For the purpose of analysis, Professor Bell's second and third strategies will be considered together. The baseline intention of a "click-through" system is good, but the implementation is too passive, too easy to defeat. Information technology professionals produce instant added value for their enterprises by enforcing business process and controlling access to information systems. Virtually every corporate information technology department possesses a better solution today than Professor Bell proposes. Organizations routinely deploy information controls through password protection, even encrypting sensitive information. Every day, people logon to email, banking, and shopping sites passing through this familiar gate keeping software. Consider a subscription metaphor to the PPM area of the company's information systems. If invited and verified (i.e., subscribed), one can participate. Unlike a simple "click-through" notification, this alternative can control users by: predefined class, location of access (restricting home, office, or mobile access), training level (perhaps enforcing a business policy requiring an IIT prevention course before participation), trade secret sensitivity, or a mix of key factors. If you skip the training, access is revoked. If you try to participate in a game after you leave the company, access is denied, etc.

Professor Bell's fourth point is simply too risky to attempt. The implantation of decoys is suggested as an experiment. However, trust is implicit when requesting the participation of a group of users in a new system implementation. Disclosure of hidden decoys could destroy trust and user participation in a given firm's PPM. Historically, users react poorly to perceived deceit or a waste of their time. Nurturing participation is an important part of implementing a new system, like a PPM. Without that wide participation, there is no " dispersed aggregate

thinking,"[125] no "collective judgment,"[126] and no hidden information."[127] There is no value in one's information system investment at all. Users vote on the success or failure of an information system by their participation, and using Bell's approach, participation likely diminishes. More effective, less risky alternatives are commonly deployed today.

IV. Analysis of Law

The foregoing sections presented the historical basis in statute, regulation, and case law for the prosecution of IIT. In determining liability related to IIT, however, it is important to apply a fact pattern to *current* application of these bases. The hypothetical PPM defined herein provides a starting point for this discussion.[128]

The SEC's website provides a current[129] snapshot of regulatory, legislative, and judicial benchmarks related to IIT offenses.[130] *O'Hagan* is the most recent Supreme Court decision referenced for enforcement against unlawful activity resulting in IIT.[131] *O'Hagan* provides that the traditional theory of IIT, where the trader breaches "a duty to shareholders with whom the insider transacts," and the misappropriation theory of IIT, where the trader breaches a duty "to the source of the information" (i.e., the company itself), are *complementary*.[132] Either theory may be used in prosecuting IIT.

A. Traditional Theory of IIT

Chiarella defines "material, nonpublic information" as the standard for information used

---

[125] *Supra* note 5.
[126] *Id.*
[127] *Id.*
[128] *Supra* notes 5 & 87 and accompanying text.
[129] As of Summer 2009.
[130] *Supra* note 86.
[131] *O'Hagan*, 521 U.S. 642.
[132] *Id.* at 652-53

in traditional theory of IIT, and is current.[133] The Court in *O'Hagan* wrote that this theory of IIT is based upon a "corporate insider's breach of duty *to the shareholders* with whom the insider transacts."[134]

1. Material Information

The Supreme Court, in *TSC Indus. v. Northway*,[135] wrote a working definition still in use for the materiality of insider information, presenting a totality of the circumstances test:

> The general standard of materiality that we think best comports with the policies of Rule 14a-9 is as follows: An omitted fact is material if there is a substantial likelihood that a reasonable shareholder would consider it important in deciding how to vote. This standard is fully consistent with Mills' general description of materiality as a requirement that "the defect have a significant propensity to affect the voting process." It does not require proof of a substantial likelihood that disclosure of the omitted fact would have caused the reasonable investor to change his vote. What the standard does contemplate is a showing of a *substantial likelihood* that, under all the circumstances, *the omitted fact would have assumed actual significance in the deliberations of the reasonable shareholder*. Put another way, there must be a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the "total mix" of information made available.[136]

Simply stated, if the information in question would spur the average shareholder to buy, or sell, or vote differently on a proxy; the information in question is material.[137]

In our hypothetical PPM, the quality of materiality that elicits action is obvious. The information revealed as a result of PPM participation was *substantive enough to cause the information holder to act*.[138] By the Court's formulation, if the information gleaned from the PPM would, in "substantial likelihood," cause a "reasonable shareholder" to act, the PPM based

---

[133] *O'Hagan*, 521 U.S. at 651 (*quoting Chiarella*, 445 U.S. at 228-29). However, *awareness* that one is using material nonpublic information when trading is still required per Rule 10-5b(2).
[134] *O'Hagan*, 521 U.S. at 652 (emphasis added).
[135] *Supra* note 40, § 80.06 [1][a] (*quoting* TSC Indus. v. Northway, 426 U.S. 438, 449 (1976) (emphasis added)).
[136] *Id.*
[137] *Id.*
[138] *Id.*

information will likely be ruled material information based on case law.[139]

2. Nonpublic Information and Awareness

The Court in *Chiarella* defined nonpublic information as company confidential information (considered company property) not known to the general trading market.[140] Specificity of information, as opposed to mere rumors, seems to impact the Court's interpretation.[141] The Court subsumes nonpublic within the definition of material information.[142] In essence, if information is confidential and not known to the general trading market, then it is material.[143]

In our hypothetical PPM, analysis of whether PPM information is nonpublic depends on the company's implementation of the specific game. If the information is identified as confidential, identified as a trade secret, password protected, and accessed only by staff who have been trained and acknowledge the sensitivity of the information output,[144] courts will likely interpret the information as nonpublic and material. If the information revealed is not subject to even basic business process controls, interpretation as nonpublic may be questionable.

In the Court's interpretation of the traditional theory of IIT, the standard is the use of material *or* nonpublic information rather than material *and* nonpublic information.[145] This is important to the analysis of our scenario since a finding of either, with awareness, attaches liability for IIT.[146]

An interesting defense to a claim of knowing use of material *or* nonpublic information as the basis of IIT exists. One might claim that the output of a PPM is merely a hypothetical

---

[139] *Id.*
[140] *Chiarella*, 445 U.S. at 230-31.
[141] *Supra* note 40, § 80.06 [2].
[142] *Id.*
[143] *Id.*
[144] These factors characterize "strong controls."
[145] *Supra* note 40, § 80.06 [2].
[146] *Id.*, § 80.07 [2][d]; 17 C.F.R. § 240.10b-5(1) (2009).

exercise; neither a strategy, nor a plan, nor a certainty. How would courts then interpret the materiality of a simulation of a possibility? How could such highly speculative information be material? Given this, how would a prosecutor prove knowing use with *awareness*? This logic could be useful for both individuals *and* companies facing liability for use of PPM gleaned information.

B. The Misappropriation Theory of IIT

The misappropriation theory of IIT identifies the fraudulent misuse of corporate information (i.e., a corporation's property) for personal gain by a fiduciary, or temporary fiduciary, as an offense.[147] The corporation has an exclusive right to this property, and is defrauded of that right.[148] This approach is current in the prosecution of IIT.[149] This theory attaches liability to the "fiduciary-turned-trader's deception of those who entrusted him with access to confidential information."[150] Here, the focus is on the fiduciary, temporary fiduciary, or a non-traditional insider' s *duty to the information owner* rather than market participants. [151] The Court likens unlawful self-enriching use of this information to embezzlement.[152] These outsiders have the identical duty as traditional insiders to disclose or refrain from trading.[153]

When the SEC issued Rule 10b5(2), it stated that interpretation of information as protected hinged upon: 1) the type of relationship between an issuer of securities and the restricted fiduciaries, and 2) a "knowing use" standard to resolve conflict in the U.S. Courts of Appeal.[154]

---

[147] *Id*.
[148] *Id.*
[149] *Id.*
[150] *Id.*
[151] *Id. (referencing Dirks*, 463 U.S. at 655).
[152] *Id.* at 654.
[153] *Dirks*, 463 U.S. at 655.
[154] 17 C.F.R. § 240.10b-5(1) (2009); The SEC describes the conflict in footnote 97 of its Final Rule Document for Rule 10b5-1, "*Compare United States v. Teicher*, 987 F.2d 112, 120-21 (2d Cir.), *cert. denied*, 510 U.S. 976 (1993)

An effective evaluation of our hypothetical requires more circumstances and facts surrounding a company's actual PPM implementation. If implemented with strong controls,[155] one could argue an individual's IIT violation more readily. In the absence of strong controls, proving that the information in question was confidential or that a duty was knowingly breached would be less likely.[156] Through use of better controls, corporate liability decreases (in an inverse relationship) as individual liability increases. This is an analogous relationship to assessing more severe penalties to an individual who breaks into a locked business rather than strolling through an open door. Locks decrease risk of business loss yet increase individual penalties.

Hence, the most likely defense to an individual charge of IIT based on the misappropriation theory using information gleaned from this hypothetical PPM would be to: 1) argue the inadequacy of the business process, information system, or other controls and warnings by which the information should have been secured; 2) argue that if the information was not obviously company confidential, an attempt to prove that the information was knowingly used is pointless; and 3) refute an individual's legal duty in the absence of awareness of information sensitivity. As before, another defense (individual or corporate) would question the very nature of the information, framing it as a *simulation rather than a certainty*, hence not material.[157]

C. Corporate liability revisited

(suggesting that "knowing possession" is sufficient) with *SEC v. Adler*, 137 F.3d 1325, 1337 (11th Cir. 1998) ("use" required, but proof of possession provides strong inference of use) and *United States v. Smith*, 155 F.3d 1051, 1069 & n.27 (9th Cir. 1998), *cert. denied*, 525 U.S. 1071 (1999) (requiring that "use" be proven in a criminal case)." The SEC's complete Final Rule Document is *available at* http://www.sec.gov/rules/final/33-7881.htm#P233_90511.

[155] *Supra* note 144.

[156] A paradox lurks here. If a business has inadequate controls over sensitive data, an individual's liability for IIT may be decreased but the company's liability (fiduciary or otherwise) increases. One sure tactic to reduce company liability would be to publish PPM data in the Wall Street journal, again eliminating a source of personal liability for IIT. Unfortunately, disclosure of valuable trade secrets is both a violation of fiduciary duty, and foolish as a matter of common (business) sense.

[157] *See infra*, the last paragraph of Section 4.A.2 of this document.

Based on the PPM hypothetical fact pattern,[158] potential corporate liability arises in two significant ways: 1) cascading liability as the result of an individual's actions, and 2) corporate liability through specific statute and regulation identified herein. This article's PPM hypothetical is intentionally mute as to implementation or management specifics to manifest liability. Liability is fact and situation specific.

Nonetheless, actions of an individual employee can result in liability for the corporation of employment.[159] Hence, efforts that reduce the occurrence of individual IIT liability will also reduce liability to related corporations. Two areas of potential corporate liability that cascade from an individual's unlawful actions are aiding and abetting and controlling person liability.

1. Aiding and Abetting

This liability attaches when any person, including a supervisor or colleague, "knowingly provides substantial assistance to another person in violation," of IIT statues.[160] In the case of a fellow employee or manager, the corporation can be just as liable.[161] The enforcement boundaries of "substantial assistance" may vary. But if an employee secures assistance for potential IIT activity from others within a business, sufficient facts may exist.[162]

2. Controlling Person Liability

Controlling person liability relies on facts uncovered in a specific occurrence of IIT. An implementation, business process, or supervisory act showing less than good faith, or either direct or indirect encouragement of IIT, attaches liability.[163] Did an employee discuss the IIT with the boss, even informally, during working hours? Did the boss suggest using eTrade or

[158] *Supra* notes 5 & 87 and accompanying text.
[159] 15 U.S.C. § 78t(a) (2006); 15 U.S.C. § 78t(e) (2006).
[160] 15 U.S.C. § 78t(e) (2006).
[161] *Id.*
[162] *Id.*
[163] 15 U.S.C. § 78t(a) (2006).

another online broker in furtherance of unlawful act? Did the employee access trading software from his/her workstation without restriction? Does poor information security suggest incompetence with a purpose (i.e., bad faith)? These and many other factors could impact the SEC's and court's interpretation of a company's liability.

Two other types of liability are based upon business behavior solely. This corporate liability might arise based on a violation of SEC Regulation FD or SOX.

3. Regulation FD

An interesting aspect of our hypothetical PPM is its likelihood to generate an intentional or non-intentional disclosure of material information, per definition within Regulation FD.[164] If data revealed during participation in a company's PPM is material, the regulation defines any holder of the company's stock as a person restricted from disclosure.[165] Any employee holding the company's stock in a brokerage, retirement, or other account is a prohibited person.[166] The regulation exempts a disclosure made "to a person who expressly agrees to maintain the disclosed information in confidence."[167] That statement contains a significant business process implication. In order to limit Regulation FD liability in PPM implementation, any holder or prospective holder of the company's stock must expressly agree to maintain information confidentiality.[168]

4. SOX Liability

Within a narrow fact pattern, where a select group of corporate insiders intentionally, willfully attempt to or actually defraud shareholders, SOX's significant civil and criminal

[164] 17 C.F.R. § 243.100-103 (2009).
[165] *Id.,* § 243.100(b)(1)(iv).
[166] *Id.*
[167] *Id.*, § 243.100(b)(2)(ii).
[168] *Id.*

liabilities attach.[169] While not limited to IIT, the penalties under SOX are severe for use of a PPM by a traditionally restricted insider for the purposes of an IIT.[170]

D. Business Risk Remediation

Courts and regulators will likely interpret PPM share price movement and other insight, openly visible to participants, as "material nonpublic information."[171] The quartet of statutory and regulatory requirements discussed[172] combined with this interpretation frames an enterprise's legal risk when considering a PPM implementation.

If it is one's intention to manage this legal risk and maximize benefit when launching a PPM, start with a structured, systemic approach.[173] Implementing a PPM is not like installing spreadsheet software on an office PC. An organization's awareness of potential risks and benefits at the onset of a PPM implementation is key to avoiding problems, frustration, and liability.

Reasonable organizational expectations prevent a common cause of implementation failure: lack of resources in staff or funds. A sudden, unexpected lack of resources is also an implementation risk. It is these resource gaps that can lead companies to under-train users, under-design systems, and miss the pot of gold at the end of the implementation rainbow. A system that is assessed and designed poorly, lacks sufficient training, or misses appropriate controls, increases a company's legal risk in a regulated environment.

1. Risk management starts with a game's creation or objective.

The first issue is to decide whether the objective of the game to train users, to build PPM acceptance, or offer insight on an organizational or competitive question. Based on various PPM

[169] 18 U.S.C. § 1348 (2006).
[170] *Id.*
[171] *Supra* notes 46 & 135 and accompanying text.
[172] Aiding and abetting, controlling person liability, Regulation FD, and SOX
[173] Defining a well-understood set of goals and success criteria is also a wise early effort.

game objectives, a company's Information Systems team would create classifications for each individual PPM game, rating sensitivity of content. The Information Systems team would then design a differing set of user notifications (warnings), user access qualifications, and logon security specific to those objectives. Unless the PPM is merely an introductory non-business, entertainment, or training exercise, for example, assume PPMs to contain material nonpublic information. Defining PPM game classification is the first step in avoiding liability (cascading liability, SOX and Regulation FD) related to unintended disclosure.

2. PPMs require new rule set and business process development.

Companies will create non-optional training for participants, perhaps delivered online. New rule sets developed will require that every user participating in a PPM be required to execute an explicit acceptance, as specified in Regulation FD.[174] This acknowledgment identifies PPM information as confidential or trade secret. Training programs, in concert with screen warnings and affirmative user acknowledgement screens, render explicit the implications of unlawful misuse of corporate information, including IIT. Information system professionals will then develop classifications of users based on training, game experience, and area of responsibility. Well implemented training and rule set definitions limit liability in a few ways. Training deters IIT at the source by informing users of *their* legal liability resulting from use of PPM data for IIT. A rule set requiring explicit acknowledgement of PPM data as company confidential (and penalties for unlawful use) deters individual user acts of IIT and satisfies Regulation FD requirements.

3. Control over participants' information system access is critical.

Based on defined user classifications, a company's information system team has the *capability* (not requirement) to sequence users into PPMs deemed appropriate by the company's

[174] 17 C.F.R. § 243.100(b)(2)(ii) (2009).

rule set. In any individual PPM, all or a subset of employees may participate, based on company objective. Users then access games for which they are approved. A subscription restricts a user's access in a way that is flexible to implement, yet difficult to defeat. Defined levels of participation are more than splash screen and "display and pray" caveats. Instead, they affirmatively limit sensitive games to trained, informed users. If users attempt to access games outside of authorization, exception reporting can be triggered. Differing levels of play could provide a user incentive to participate, increasing acceptance and participation.[175] User access controls (i.e., subscription) lock one door through which confidential information escapes. Access controls limit Regulation FD liability by preventing accidental disclosure of PPM related confidential data. Access controls enforce training and game classification rule sets limiting cascading liability (from aiding and abetting and controlling person liability) and SOX liability (by enforcing strong controls).

4. Use technology tools to freeze and enforce business rule sets.

As mentioned earlier, the planning protocol and logon access restrictions are *de rigueur* for information system professionals. The use of information technology freezes a company's rule set in time, enforcing it daily. An implementation like this demonstrates strong controls[176] within a corporation, limiting liability as above. The skilled implementation of a wise design is the key to mitigating business risk and legal risk.

Although acting on these observations will mitigate risk, it will not provide an iron-clad guarantee of avoiding liability. Until Congress, the SEC, and/or the courts exert a specific opinion on PPM implementations, there will continue to be legal risk.

---

[175] Ask anyone with Facebook access about the drive to reach increasing levels in the Mob Wars game, for example. A site that is fun and rapidly changing brings users back time and time again. PPMs, well designed and implemented, are similarly as attractive.

[176] *Supra* note 144.

E. Proposed Changes to Regulation & Legislation

Consider the legal risks faced by businesses deploying a PPM, discussed herein. Absent clear guidance on potential statutory and/or regulatory PPM pitfalls, many enterprises will sadly regard these legal risks as immovable barriers. Defining explicit procedures to achieve safe harbor using approved business practices would result in a path to benefit from PPMs with acceptable risk. Criminalizing other behaviors (having uncertain criminality today) associated with IIT and PPMs, would deter behaviors that lead to cascading liability for businesses.

Today businesses rely on the foundational securities protection acts of the 1930s, the 33 Act and the 34 Act.[177] The SEC regulations enacted and Congressional modifications and additions have remediated glaring market ills. Though these acts have aged well, the rule sets need an update.

1. SEC's Remarks During the Current (2008 - 2009) Financial Crisis

SEC Chairman Mary Shapiro's remarks to a Congressional oversight committee regarding the current financial crisis included a variety of proposed legislative changes.[178] Of interest, Chairman Shapiro suggested establishing criminal penalties for "aider and abettor" claims in the Securities Act.[179] This is a fine start and needed change.

2. Components of the Next Generation of Securities Legislation

It is, however, well past time to enact the *next* generation of foundational securities legislation that contemplates realities of a computerized, highly networked world. Observing the frenetic pace of technological change may be regarded as a cliché. But enforcement realties,

---

[177] *Supra* note 40.
[178] *SEC Oversight - Current State and Agenda*: *Hearing Before the H. Comm. on Fin. Serv. Subcomm. on Capital Mkts., Ins. and Gov't-Sponsored Enters*., (July 14, 2009) (testimony of Mary L. Schapiro, Chairman, U.S. Securities and Exchange Commission) *available at* the SEC's website http://www.sec.gov/news/testimony/2009/ts071409mls.htm).
[179] *Id.*

enabled by process and technology innovations, are all too real. Gregory Moore of Intel Corporation opined that best-in-class processing capacity would double every two years (sometimes called Moore's Law), perhaps for the foreseeable future.[180] An increase in computing power begets an increase in software and raw data processing capacity; those increases beget the capability to harvest gems of insight from vast amounts of previously useless data. Further combined with widely available high-speed data connections from wired[181] or wireless[182] sources, information travels from origin to handheld in a virtually instantaneous manner. These evolving factors stretch existing definitions of materiality of information, the boundaries of nonpublic information,[183] and what constitutes awareness.[184]

If legislation could be created in as flexible and forward thinking a manner, perhaps the legislative enforcement platform of the future would be as enduring as the 33 & 34 Acts. Consider these components of that new breed of securities legislation:

a. New Language

This article advocates targeted changes to legislation and regulation. Industry leaders or regulators need to create forward-looking, inclusive language (i.e., terms, words) to describe emerging data harvesting processes and technologies, like PPMs. Based upon those new terms, Congress should enact prohibitions against specific IIT behaviors that use a company's own harvested data, perhaps from a PPM, rising to the standard of "material non-public information."

---

[180] Intel Corporation © 2005, *Excerpts from A Conversation with Gordon Moore: Moore's Law*, *available at* Intel's download website ftp://download.intel.com/museum/Moores_Law/Video-Transcripts/Excepts_A_Conversation_with_Gordon_Moore.pdf ; Michael Kanellos, *New Life For Moore's Law, available at* http://news.cnet.com/New-life-for-Moores-Law/2009-1006_3-5672485.html. I jokingly say that I started my career when computers were made of wood. In the span of my career, the first data center in which I worked had less storage, memory, and processing capacity than the iPhone I carry on my hip today. The cheapest laptop today exceeds the processing and storage capacity of most data centers of the early 1980s.

[181] Like broadband or DSL connections, for example

[182] Like WiFi, WiMax, or cellular 3G networks, for example

[183] If information appears on a blog, is it then public, or opinion, or analysis? What about an email distribution list? How wide a readership of either is required to trigger a disclosure that becomes "public?"

[184] How does a world of twenty-four hour a day news, blogs, instant messaging, and email impact what constitutes public awareness versus nonpublic information?

Since a wealth of legislation, regulation, and case law defines "material non-public information," these new terms will simply adjust the scope of protected data.

b. New Supervisory Business Process Requirements

Congress or the SEC should consider adding a supervisory business process requirement for data harvesting processes and technologies, like PPMs. Implemented like Section 15f of the 34 Act[185] or SOX provisions,[186] a process requirement would hold businesses to (at least) minimum data security standards. In exchange for approval to garner value from new technical modalities, like PPMs, comes the data security responsibility to shareholders and the markets.

c. New Safe Harbor Provisions for Businesses in Compliance

In the spirit of fairness, Congress or the SEC should then define some harbor provisions for businesses that install the required data security controls, including PPM implementations. If a business meets a set of process standards that include specific elements (to be defined), then it would be granted safe harbor from statutory or regulatory liability as a result of IIT. Consider by analogy the safe harbor provisions Congress created for forward-looking statements in 15 U.S.C. § 78u-5 (2006).

A safe harbor for individuals trading securities exists today. An individual must have "awareness" of using material nonpublic information when trading securities to be culpable of IIT. "Awareness" functions as an individual's safe harbor under SEC regulations.[187]

d. Enhance Wire Fraud Statutes

Finally, Congress should consider extending the existing wire fraud definition in 18 U.S.C. § 1343 (2006) with language creating greater flexibility for emerging technologies.

---

[185] 15 U.S.C. § 78o(f) (2006).
[186] *Supra* note 105 and accompanying text.
[187] 17 C.F.R. § 240.10b-5(1) (2009); 17 C.F.R. § 240.10b5(2) (2009).

Today the statute states: "Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of *wire, radio, or television communication* in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both." The inclusion of "internet, wired, wireless, satellite, or any other electronic communication modality owned, regulated, managed or auctioned by the Federal government," would suffice.[188] The deterrent effect of this legislation could prevent acts of IIT, perhaps using PPM data, from occurring.

Legislation adapts more quickly than the courts. Legislation, however, requires broad consensus. If a comprehensive approach is not possible, any of these proposed changes could be achieved via add-on legislation like Insider Trading and Securities Enforcement Act of 1988.

[188] The current U.S. Attorney's Manual (USAM 9-43.100) uses a variety of US Circuit case law to define elements of wire fraud. These elements are focused on the transfer of funds through wire, a back end process. I propose criminalization of use of telecommunications for IIT earlier in the process.

V. Conclusion

A perfect world, void of risk, doesn't exist for businesses contemplating information system implementations, like PPMs. Businesses have no absolute answers when legislators, regulators, and the courts are silent on questions of importance like those discussed in this article. As technological innovation impacts securities markets, Congress, the SEC, and the courts will continue to adjust as they have since the 1930s.

So how can business leaders and others avoid the orange jumpsuit? They can succeed by doing what they do best; managing risk and reward in such a way that shareholders receive a reasonable return within a reasonable timeframe. When considering implementing new tools in their portfolios, wise enterprises assess, design, and implement risk mitigation strategies. Successful firms budget for risks, including legal risks, at the onset of projects.

This article is intended to provide a starting point for discussion since Congress, the SEC, and the courts have not spoken directly on the matter of PPMs and IIT. The potential liability discussed herein, however, is *not* a reason to avoid PPM implementation. Instead, it is a call to action to implement PPMs with careful planning and skill.

