Consider the Source: How Weak Whistleblower Protection Outside the United States Threatens to Reduce the Impact of the Dodd-Frank Reward Among Foreign Nationals

By: Patrick Collins, Lee Stein, and Caryn Trombino, Perkins Coie LLP

I. Introduction

In the wake of the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("the Act"), some observers have predicted that, given the attractive financial whistleblower provisions, the Act will generate an influx of Foreign Corrupt Practices Act ("FCPA") allegations to the Securities and Exchange Commission ("SEC"). Early reports from the SEC and various plaintiff's law firms indicate that there has already been an increase in whistleblower tips under the bounty program, although it is not yet clear what percentage of the tips relate to FCPA cases.

Given the unique nature and origin of FCPA cases, there is reason to question whether the Act will open the floodgates to new FCPA cases. Specifically, FCPA whistleblowers tend to be foreign nationals in countries that historically have been hostile to whistleblowers. Given this fact, can the Act's limitations adequately protect foreign nationals in order that the new provisions meet the Act's expectations?

The Act's reward provisions are designed for individuals who have access to "original information."[1] In the FCPA context, the qualifying person is almost necessarily a foreign national residing in the overseas markets where the illegal conduct is taking place. Particularly with DOJ's current geographic FCPA focus, these individuals are often working in countries where the anti-corruption enforcement environment is much more hostile to whistleblowers. Accordingly, until a more global commitment to anti-corruption efforts and whistleblower protection takes hold, the extraordinary potential of the whistleblower reporting mechanism envisioned by the Act likely will not be fully realized, particularly in regions reported to have the most pervasive levels of corruption.

This article analyzes the potential impact of the Dodd-Frank whistleblower provision on FCPA cases involving foreign nationals working at foreign subsidiaries of United States companies. Specifically, it questions whether the Act's current provisions are attractive enough to lure foreign-based whistleblowers in the face of the known risks to known whistleblowers in countries, such as China, India and Russia, where there is heavy FCPA interest. At the end of the day, the success of the Act may depend substantially on perception. Will potential whistleblowers in foreign markets feel confident that the mechanisms created by the Act are, in addition to being potentially profitable, effective and safe as well?

Changing the culture of whistleblowing in foreign countries may prove more difficult than anticipated, particularly in light of the existing global climate. In its 2009 Annual Report, Transparency International reported that, in a worldwide public opinion survey, more than one in ten people interviewed reported having paid a bribe in the previous twelve months, and yet nearly half of bribery victims polled viewed existing complaint mechanisms as ineffective.[2] Even in the United States, despite statutory schemes enacted to protect whistleblowers, it is

widely perceived that such laws often give "the illusion of protection without truly meaningful opportunities or remedies for achieving it."[3]

Regardless of whether a large number of foreign national whistleblowers ultimately participate in, or benefit from, the new provision to advance FCPA allegations, the Act likely will spur United States-based multinational companies to take a closer look at their internal whistleblowing program to make the internal reporting process more attractive. If foreign national whistleblowers access the company's internal process, that could lead to increased internal disclosure of FCPA allegations, which will necessarily lead, over time, to more companies walking into the SEC with voluntary disclosures.

II. Dodd-Frank Whistleblower Provision

A. The Bounty

In the United States, whistleblower legislation that offers financial rewards has proven to be a largely effective method to increase participation in federal whistleblower programs.[4] For example, the federal False Claims Act ("FCA"), after being revised in 1986 to award whistleblowers anywhere from 25% to 30% of judgments, has since resulted in over 4,000 qui tam suits filed, and FCA recoveries have totaled more than $24 billion.[5]

The financial reward, or "bounty," which the Act's whistleblower provision outlines, has the potential to create an extraordinary windfall for successful whistleblowers, particularly in FCPA cases. The Act provision was designed to "amply rewar[d] whistleblower(s)," and thus creates a minimum payout between 10% and 30% of any monetary sanctions that are collected based on the information provided by the whistleblower.[6] In order for the whistleblower provision to be triggered, the SEC must bring a judicial or administrative action under the securities laws resulting in monetary sanctions exceeding $1 million.[7] Because recent FCPA enforcement actions have resulted in settlements exceeding $100 million, observers have noted that the financial incentives posed to a potential whistleblower are anticipated to be dramatic. With such large payouts at stake, a "cottage industry" of law firms is expected to develop to assist whistleblowers through the administrative and legal processes.[8]

B. Eligible Whistleblowers

The Act defines "whistleblower" quite broadly, as any individual who provides information relating to a violation of the securities laws.[9] However, the Act makes certain whistleblowers ineligible for the award, including those who are (or were at the time of acquiring the original information) members, officers or employees of a regulatory agency, the Department of Justice, a self-regulatory organization, the Public Company Accounting Oversight Board, or a law enforcement organization.[10] Although the Act does not explicitly provide that foreign nationals are included among eligible whistleblowers, it contains no language limiting participation to United States citizens.

Under the Act, any whistleblower who is convicted of a criminal violation related to the judicial or administrative action is likewise ineligible for award,[11] as is any whistleblower who gains the disclosed information through the performance of a financial statement audit as required under the securities laws.[12] Any whistleblower who fails to submit information to the SEC, as it may

require by rule, shall not receive an award under the provision,[13] and a whistleblower will not be entitled to an award if he knowingly and willfully makes any false, fictitious, or fraudulent statement or representation, or uses any false writing or document (knowing it to contain false, fictitious, or fraudulent entries).[14]

C. Whistleblower Protections

1. Dodd-Frank Protections

In drafting the Act's whistleblower protections, Congress explicitly acknowledged the "enormous risk" that individuals undertake when blowing the whistle on fraud and corruption.[15] Due to this risk, the Act attempts to prohibit employer retaliation against the employee-whistleblower in a multitude of ways, ranging from discharge to more subtle forms of harassment and discrimination.[16] Aggrieved employee-whistleblowers are provided with a cause of action in federal district court, as well as potential relief in the form of reinstatement (with same seniority status), double the amount of back pay with interest, and compensation for litigation costs, expert witness fees, and reasonable attorneys' fees.[17]

Although the Act does include confidentiality provisions in order to protect the identity of the whistleblower, upon further review, the Act's provisions do not guarantee confidentiality. The Act provides that the SEC shall not disclose any information which could reasonably be expected to reveal the identity of the whistleblower (including information provided by the whistleblower to the SEC), **unless and until required to be disclosed in connection with a public proceeding**.[18] Furthermore, nothing in the Act may be construed to limit the ability of the Attorney General to present evidence to a grand jury, or to share evidence with potential witnesses or defendants, in the course of an ongoing criminal investigation.[19] The SEC may, at its discretion, disclose information provided by the whistleblower to government and regulatory agencies at the federal and state level, as well as to foreign securities authorities and foreign law enforcement authorities, when doing so is necessary to accomplish the purposes of the Act and to protect investors.[20] The law provides that information shared with foreign regulators or law enforcement agents must be maintained with assurances of confidentiality as determined by the SEC.[21]

2. Past and Present Problems with United States Whistleblower Provisions

Before turning our attention to the Act's potential applicability in foreign countries with a history of hostility toward whistleblowers, a brief review of several historical whistleblowing statutes is in order.

On March 29, 2010, just four months prior to the Act's authorization on July 21, 2010, the SEC's Office of the Inspector General ("OIG") released a memorandum assessing the SEC's then-existing "Bounty Program."[22] Among its findings, the OIG noted that although the program had been in place for more than 20 years, the SEC had not received a large number of applications from individuals seeking a bounty, and further that the SEC had made very few payments under the program (seven payouts to five whistleblowers totaling $159,537), largely due to the fact that whistleblowers were only entitled to a reward if the case related to insider trading.[23] The OIG's assessment specifically called for several legislative changes that were ultimately incorporated

into the Act's whistleblower program, and the OIG identified the DOJ and Internal Revenue Service ("IRS") whistleblower programs as being particularly well-defined examples of "best practices."[24]

a) IRS Whistleblower Program

The Senate Committee report indicates that, in drafting the Act, the Committee noted the SEC Inspector General's recommendation, and modeled the new whistleblower program after the IRS program, which features the "critical component' of the minimum payout to successful whistleblowers.[25] However, despite the endorsements offered by the SEC's OIG and Senate Committee, whistleblowers participating in the IRS program have complained that the system does not function as designed by the legislation. In July 2010, just prior to the signing of the Act, attorneys representing IRS whistleblowers described an "institutional resistance to rewarding whistleblowers," despite the fact that the law entitles them to as much as 30% of the proceeds.[26]

Although the IRS Whistleblower Program was revised in 2006 to require a mandatory payout of at least 15% to tipsters, the IRS had yet to pay any bounties under the new scheme, as of June 2010.[27] Nevertheless, the revised program has successfully enticed informants to submit dozens of tips involving purported tax losses of $100 million or more, as well as several hundred "big case" leads above the previous average.[28] It is questionable, however, whether tipsters will continue to submit information if the IRS continues to fail to deliver the bounty as promised.

b) False Claims Act (FCA) Program

Although the FCA whistleblower provision is generally viewed as a success, in practice, participation in the program is similarly fraught with difficulties. Under the FCA, whistleblowers file qui tam cases that remain under seal as the DOJ investigates and determines whether it will join the suit.[29] About 80% of the federal qui tam cases filed are rejected by the United States government, after which point whistleblowers can choose whether to continue with their own lawsuits.[30] While the United States government successfully reaches settlement in 98% of the cases pursued, whistleblowers who continue with their own lawsuits are far more likely to lose, some estimates claiming they lose more than 95% of the time.[31]

A recent study published in the New England Journal of Medicine indicates that, even among whistleblowers who receive the financial reward (ranging from $100,000 to $42 million, with a median of $3 million), "the prevailing sentiment was that the payoff had not been worth the cost."[32] Many whistleblowers complain of social alienation, industry blackballing, loss of employment and stress and tension that is prolonged over the often lengthy period of time it takes to resolve a case.[33]

Even when legislation provides whistleblower protections, the efficacy of these remedies is not borne out by statistics regarding the successful resolution to retaliation complaints. For example, from its enactment in 2002 through May 2006, 499 out of 677 completed Sarbanes-Oxley ("SOX") retaliation complaints were dismissed and 95 were withdrawn.[34] Only 2% of the remaining 286 cases that went to administrative law judge resulted in a decision for the whistleblower employee.[35]

Aside from the statistical gamble that a whistleblower's claim will ultimately be selected and pursued by the United States government, the lack of certainty and administrative difficulties that precede actual recovery of the whistleblower bounty are clearly major issues that persistently surface in practice. Any whistleblower, regardless of national origin, will also face these hurdles when choosing to participate in the Dodd-Frank whistleblower program, as it is entirely untested and still in the early process of formation. However, for the reasons explored below, the task awaiting a foreign national whistleblower is far more daunting, and the stakes to participating can be very high, depending in large part on the country in which the potential whistleblower is based.

3. Unclear Legal Implications for Foreign Whistleblowers

In some respects, the jury is still out as to whether the Act's language will meet the unique challenges of the foreign national whistleblower. That is because, under the Act, the SEC has 270 days from its enactment to issue final regulations implementing the whistleblower provision;[36] until those critical details emerge, there remain several open questions as to the potential efficacy of the Act to foreign whistleblowers.

a) Application of Anti-Retaliation Protection

Under the terms of the Act, it would appear to apply to foreign nationals. However, the Act does not clearly establish **how** the anti-retaliation provisions would be enforced in an instance involving a foreign whistleblower employed by a foreign subsidiary.[37] For example, the cause of action that the Act creates for individuals alleging retaliation requires that the action be brought in a United States district court, and that subpoenas requiring attendance of witnesses at trial or hearing may be served at any place in the United States.[38]

In the preexisting SOX anti-retaliation cause of action, congress failed to establish clear intent for extraterritorial coverage, and as a result the First Circuit and the Department of Labor declined to apply the law's protections to a foreign worker at a foreign subsidiary of a United States corporation.[39] In *Carnero v. Boston Scientific Corp*., 433 F.3d 1 (1st Cir. 2006), the First Circuit held that the SOX provision did not have extraterritorial application and thus did not extend whistleblower protection to foreign employees working abroad. The court in *Carnero* noted the provision's silence as to application abroad, including critical issues such as enforcement mechanisms in foreign settings, potential conflicts with foreign labor laws, extraterritorial investigative powers, venue provisions, and logistical issues such as the provision of interpreters, coordination with the State Department, and a realistic time frame to conduct overseas investigations.[40]

While the Act specifically extends the universe of potential retaliation claimants to include employees of "any subsidiary or affiliate whose financial information is included in the consolidated financial statements of a company,"[41] neither the Act nor its legislative history appears to address the extent to which the right to claim retaliation applies to employees of **foreign** subsidiaries. Despite the lack of specificity in the legislation, employees of foreign subsidiaries would appear to be covered, provided that such entities are included on the company's consolidated financial statements.[42] Nevertheless, the Act fails to address the concerns implicit in foreign enforcement that are outlined by the court in *Carnero*, and it is

unclear whether the SEC's forthcoming implementation regulations will shed any light on these practical considerations.

b) Problems with Local Law

Foreign whistleblowers who are current employees of foreign subsidiaries will likely be providing the United States government with documents and materials that will potentially include information that is proprietary and/or covered by the attorney client privilege.[43] And as multinational companies have already experienced, transmitting information from one country to another implicates serious data privacy issues that often bring to the fore thorny issues regarding conflicts in international laws.[44] It is not clear how, and to what degree, whistleblowers might be held accountable for their actions under local laws, as foreign employees of foreign subsidiaries remain generally governed by the laws of the country where they are employed.[45]

c) Possible Barriers to Recovering the Bounty

In terms of a foreign whistleblower's right to the bounty, while the Act provides that a whistleblower who has been convicted of a criminal violation related to the judicial or administrative action is ineligible for award, it does not clarify what would happen in the instance of a foreign whistleblower who has unclean hands, but for whom there is no jurisdiction for criminal prosecution.[46] Further, while the bounty is to be paid if information provided to the SEC leads to a successful related action by the DOJ (or another state or federal enforcement agency),[47] it is not clear whether a whistleblower will receive an award if the SEC does not have jurisdiction over the foreign subsidiary, but the information provided does lead to monetary sanctions in a related action by the DOJ.[48]

Further, although the Act does provide a minimum recovery of 10% payment of monies obtained by the government, the SEC enjoys a wide breadth of discretion to determine the amount within that range, based on factors such as "significance of the information," "degree of assistance," and the vague catch-all of "additional relevant factors as the SEC may establish by rule or regulation."[49] Given the latitude that the SEC may exercise in awarding the bounty, potential whistleblowers may face similar obstacles to what participants in the IRS Whistleblower Program have confronted. The ability to challenge and litigate these issues is significantly more difficult for a foreign national, who would likely not have the resources to sustain these delays and costs until resolution.

III. Whistleblowing Outside the United States

The problems that United States whistleblowers historically have faced pale in comparison to the potential risks and obstacles facing foreign whistleblowers, particularly in countries with endemic corruption problems. In FCPA cases, low-level foreign employees are often the "gatekeepers" with direct, firsthand knowledge of the company's daily operations.[50] According to the Association of Certified Fraud Examiners, the most common source of reports of corruption is employee tips (42.6%).[51] If the Dodd-Frank program is intended to attract these foreign whistleblowers, it will be essential to provide assurances that the employees will be protected, particularly when they are unlikely to find adequate protection in the whistleblower laws (assuming they exist) in their own countries.

A. Global Patchwork of Anti-Corruption Enforcement

Although the United States has demonstrated a relatively strong commitment to anti-corruption enforcement, its positions have not been adopted by its global counterparts. The Organization for Economic Cooperation and Development's ("OECD") Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, adopted in 1997, now has 38 parties and is administered by the OECD Working Group on Bribery.[52] The Working Group's 2010 Progress Report examined enforcement and steps taken by member countries to implement the Working Group's previous recommendations regarding the passage of implementation laws and institutions, policies and practices for enforcing the prohibition on foreign bribery.[53] Notably, the 2010 Progress Report concluded that only seven of the 38 parties to the Convention were engaged in "active enforcement," with 20 of the remaining parties (among them, Canada) engaged in "little or no enforcement." While the recent increase in the number of "active enforcement" countries from four to seven was viewed as a positive development, the Report found it "deeply disturbing" that almost no change in the "little or no enforcement" category had transpired over the past five years.[54] Moreover, China, India and Russia—countries which are major exporters and are also regions of FCPA focus—are not even member countries to the Convention.[55]

The OECD Working Group Report characterizes the current global enforcement environment as "unstable," citing "danger signals" such as efforts in certain countries to limit the role of investigative magistrates, shorten statutes of limitation, and extend immunities from prosecution.[56] The OECD Convention does not require whistleblower protection,[57] and experts in 24 of the 38 member countries found inadequate complaint systems and/or whistleblower protection.[58] Among the handful of countries that have passed legislation to protect whistleblowers, most laws do not do so effectively, with few recognizing disclosure of information as a protected activity, and most only protecting whistleblowers who testify or serve as witnesses.[59]

Although the United States has created the tools and committed the resources necessary for aggressive anti-corruption efforts, many OECD member countries lack a similar political commitment, both in failing to provide adequate funding and staffing for enforcement, and—in some cases—actively using political obstruction to frustrate anti-corruption investigations.[60]

Cultural Views Regarding Whistleblower Rewards and Anonymity

Throughout the international community, there is disparate treatment and consideration given to whistleblowers, particularly in the context of financial remuneration. Although several countries have adopted laws to encourage whistleblowing, including Australia, Canada, Ireland, Israel, Japan, New Zealand, South Korea, and the United Kingdom ("UK"),[61] it is actually quite rare for whistleblower legislation to offer financial rewards. Indeed, in some countries, such as the UK and Australia, there is reluctance or refusal to reward whistleblowers.[62] Whistleblowers in the UK are protected by the Public Interest Act of 1998, but in order to be protected by the law, the whistleblower must not be acting for personal gain (among other requirements).[63] Also, per the UK's Employment Rights Act, whistleblowers who act for personal gain are explicitly

withheld whistleblower protection.[64] In this way, certain countries outside the United States place higher value on a more "idealistic" whistleblower motive and discourage the financial motivation.[65]

Additionally, many countries outside the United States view with skepticism core concepts such as the protection of whistleblower anonymity. The confidentiality issue has posed significant problems for multinational United States-based corporations attempting to create whistleblower hotlines in compliance with SOX.[66] For example, when McDonald's Corporation and Wal-Mart attempted to establish hotlines in France and Germany, a German labor court ruled that the proposed hotline violated German law, and the French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertes*) refused to approve the proposed whistleblowing programs.[67] For France, in particular, the concept of anonymous reporting carries historical implications related to Nazi informants during World War II, and there remains fear that an anonymous whistleblowing system could give way to an organized system of professional denunciation.[68]

Nevertheless, witnesses living in the most corrupt regions of the world are not likely to report allegations of wrongdoing if they fear reprisals or other negative consequences from the government, or from within their workplace or community; for these individuals, the protection of anonymity may be critical.[69]

B. Threats to the Safety and Freedom of Whistleblowers in China, India and Russia

Although financial incentives historically have proven to be an effective incentive to draw out whistleblowers in the United States, it is not at all clear that the financial motivation incentive would, in itself, be powerful enough to overcome the very human costs whistleblowers in certain countries face when their identity is put at risk. Aside from workplace harassment and loss of employment---the primary concerns among United States whistleblowers---, whistleblowers in countries like China, India and Russia are more likely to fear more severe victimization through physical threats and violence, particularly when exposing acts of public corruption.

1. China

In March 2009, a survey published by Chinese national newspaper *China Youth Daily* reported that, despite national campaigns to reduce corruption, the Chinese public remains hesitant to provide information to authorities regarding official corruption.[70] Fear of retribution is reported to be a major concern for Chinese whistleblowers, with some sources claiming that, in many cases, informants are killed, jailed, or attacked for tipping off authorities.[71] On August 30, 2010, Chinese anti-corruption activist and whistleblower Fang Zhouzi was reportedly sprayed in the face with a chemical and beaten with a hammer, after recently posting an online article that criticizes a controversial medical procedure that is performed by a Chinese hospital.[72] Similarly, a Chinese journalist who had written an article questioning the procedure's efficacy was assaulted in June 2009.[73]

Concerns regarding inadequate whistleblower protection are evident in public survey results which indicate that the Chinese public prefers reporting corruption through the internet, rather than directly to public prosecutors or the police.[74] However, the Chinese government's

surveillance and censorship of the internet seriously comprises the confidentiality of online communications, as highlighted most recently in January 2010 when Google threatened to pull service out of China following targeted cyber attacks on the email accounts of dozens of human rights advocates in China.[75] Indeed, Human Rights Watch reports that the Chinese government devotes massive financial and human resources to internet monitoring and censorship.[76] Google's website does not disclose the number of requests for user data that it receives from the Chinese government because censorship demands are considered state secrets in China.[77] Skype uses local servers in China and has disclosed that chat messages received into and transmitted out of China may be monitored and stored by local authorities.[78]

In 2006, the Chinese government, at a cost of $700 million, implemented a firewall intended to monitor, filter, and block sensitive online content.[79] Internet traffic is routed through the firewall (known as the "Golden Shield" or "Great Firewall") against a blacklist of forbidden internet addresses, including BBC News and Voice of America.[80] The Public Security Bureau also employs human censors to monitor domestic sites and email traffic to identify and target politically sensitive content.[81] Against this backdrop, potential Chinese whistleblowers with information concerning corrupt activities of public officials must determine whether they feel confident that communications with authorities in the United States will remain confidential, should they choose to participate in the Dodd-Frank whistleblower incentive program.

2. India

In late August 2010, India's Union Cabinet approved the Public Interest Disclosure and Protection to Persons Making the Disclosure Bill, which aims to protect the identity of whistleblowers and to prevent disciplinary action from being taken against them.[82] The proposed legislation follows the 2003 murder of whistleblower Satyendra Kumar Dubey, who had reported to the Prime Minister information concerning corruption within the National Highways Authority of India ("NHAI").[83] Although Dubey had requested his identity be kept a secret, his name was exposed and he faced internal reprimand from the NHAI, and later death at the hands of assailants.[84] Similarly, as many as eight Indian whistleblowers have been killed in 2010, each of whom was seeking information from the Indian government through "right to information" or RTI.[85]

Although the draft bill is regarded as a positive development, legal observers note that the proposed legislation does not address measures that would be taken in the event that a whistleblower's identity is revealed, and further express concern that the entity which is empowered to enforce whistleblower protection—the Central Vigilance Commission—is comprised of former government officials and has heretofore failed to enforce its anti-corruption powers.[86] The bill further provides that persons making false allegations will pay a fine of 50,000 rupees (approximately USD $1,000), or could face a jail sentence of up to three years.[87]

Furthermore, in August 2010, after receiving unverified reports that BlackBerry maker Research in Motion ("RIM") agreed to set up a server in China to address the Chinese government's security demands, India's Home Ministry threatened to shut down RIM services in India if the company refuses to create similar security and access for Indian authorities.[88] The Indian government is seeking access to monitor, intercept or decrypt Blackberry messenger, email and Web exchanges, citing national security concerns regarding terrorist communications.[89]

Similarly, on September 2, 2010, Indian authorities announced that—in addition to RIM—they are requesting all companies that provide encrypted communications (among them, Google, Skype, Nokia and MSN Hotmail) to likewise install local servers in the country so that Indian security agencies can more easily decrypt electronic communications and obtain user data.[90]

While Indian authorities maintain that national security demands necessitate surveillance of electronic communications, potential whistleblowers desiring to remain anonymous when disclosing information related to public corruption might question whether the privacy of their communications, and thus their physical safety, has been compromised.

3. Russia

Recent incidents further underscore the fear of retaliation that Russian whistleblowers face when bringing attention to acts of public corruption, particularly given the country's ranking of 146 out of 180 countries on Transparency International's Corruption Perception Index.[91] With Russia's corruption score faring far worse than other major emerging markets, some major multinationals are reportedly questioning whether they can continue having a business presence there.[92]

In May 2010, a wealthy Russian businessman fled to the UK after participating in a sting to expose a corrupt Kremlin official, out of concern that he would be "running a serious risk" if the information and evidence in his possession remained in Russia.[93] The whistleblower, Valery Morozov, reported the corrupt official to the Economic Crimes Department of the Ministry of the Interior, and subsequently worked with police to secure video and audio recordings to serve as evidence against the Kremlin official. Despite the evidence, prosecutors declined to bring charges against the official.[94] Subsequently, Morozov's company lost its contract on a construction bid for the 2014 Winter Olympics, and also had its equipment confiscated from a building site.[95] After Morozov arranged to have a letter of complaint hand-delivered to Russian President Dmitry Medvedev, and further sought publicity through the British press, Medvedev issued a direct order to reopen the case against the Kremlin official.[96]

In November 2009, Russian police officer Alexei Dymovsky recorded a videotaped open letter to Prime Minister Vladimir Putin in which he detailed the widespread corruption and abuse of authority within the Russian police force.[97] In the video, which was later posted to YouTube and generated over a million views, Dymovsky described how police officers collect bribes from citizens and businesses, and how officers routinely bring false charges against innocent civilians.[98] Shortly after the video appeared, Dymovsky was quickly fired from the police force, and he later hired a bodyguard, publicly stating that he feared for his life.[99] In January 2010, Dymovsky was arrested and taken to a police detention center on charges relating to corruption and abuse of office.[100] Dymovsky was later released on his own recognizance on March 7, 2010, and stated that he and his family continued to face pressure from Russian authorities.[101] In late 2009, Sergei Magnitsky, a lawyer involved in a corruption lawsuit against the police died in custody after being denied medical treatment, and in the week prior to Dymovsky's arrest, a Russian journalist died after being beaten while in police custody.[102]

IV. Conclusion

Whether the Act will spur additional FCPA investigations may well be a function of how the Act's provisions are received—and perceived—by foreign nationals. Rather than immediately jump into the fray, foreign nationals may wait to observe the success of the new SEC whistleblower program before deciding to assume the enormous risk that accompanies blowing the whistle on public corruption in certain areas of the world. Until more countries outside the United States improve whistleblower protection enforcement, foreign whistleblowers will likely not be as willing as United States citizens, or citizens from countries with more robust anti-corruption environments, to volunteer information to the United States government. With the new provision entirely untested, whistleblowers face significant uncertainty: 1) will they be able to communicate with United States investigators; 2) will they have access to United States courts; 3) will they be guaranteed anonymity or confidentiality; 4) will they have a realistic likelihood of recovering the highly-anticipated bounty.

Some of these questions may be answered once the SEC issues its regulations implementing the Dodd-Frank whistleblower provision; however, it will likely take time for the nuances of the program to crystallize. In the meantime, multinational companies are well-advised to reexamine the efficacy of corporate internal reporting mechanisms, and to make adjustments where necessary in order to make internal whistleblowing a more attractive avenue for employees who may be reluctant to address their concerns to the United States government. Companies undertaking pre- or post-acquisition due diligence reviews should place greater emphasis on fully debriefing employees who are leaving the company following the merger, as these individuals might be particularly disgruntled and have lost any remaining sense of loyalty to their employer. These individuals might indeed be the most likely candidates to take advantage of the SEC's whistleblower program.

While the financial rewards that the Act has created undoubtedly will attract participants who might otherwise raise their concerns internally, foreign employees may not be willing to assume the risk of whistleblowing, particularly when it is not yet clear how difficult it will be to recover the bounty or to avail themselves of the Act's anti-retaliation protections.

---

[1] The Act states that "original information: (i) must be 'derived from' the independent knowledge or analysis of the whistleblower; (ii) cannot be 'known to the SEC from any other source; ' and (iii) cannot be 'exclusively derived from an allegation made in a judicial or administrative hearing, in a government report, hearing, audit, or investigation, or from the news media.'" Dodd-Frank Act, 111th Cong. § 922a(a)(3) (2010).
[2] *Annual Report 2009* (Transparency International), Jul. 2010, at 50, http://www.transparency.org/publications/publications/annual_reports/ti_ar2009.html.
[3] Terry M. Dworkin, *SOX and Whistleblowing*, 105 MICH. L. REV. 1757, 1764 (2007).
[4] *Id*. at 1769.

[5] *Id*. at 1769; Thomas O'Brien et al., *Recent Changes in Federal Law and Investigative Tactics Signal Heightened Enforcement under the False Claims Act*, Jun. 10, 2010, http://www.paulhastings.com/assets/publications/1636.pdf?wt.mc_ID=1636.html.
[6] S. Rep. No. 111-176, at Subtitle B, (2009-2010).
[7] Dodd-Frank Act, § 922a(a)(1) (2010).
[8] Lisa H. Bebchick et al., *Incentives for Foreign Corrupt Practices Act Whistleblowers: Dodd-Frank Wall Street Reform and Consumer Protection Act*, Jul. 16, 2010, http://www.ffhsj.com/index.cfm?pageID=25&itemID=6223.html.
[9] Dodd-Frank Act, § 922a(a)(6) (2010).
[10] Dodd-Frank Act, § 922a(c)(2)(A) (2010).
[11] Dodd-Frank Act, § 922a(c)(2)(B) (2010).
[12] Dodd-Frank Act, § 922a(c)(2)(C) (2010).
[13] Dodd-Frank Act, § 922a(c)(2)(D) (2010).
[14] Dodd-Frank Act, § 922a(i) (2010).
[15] Sen. Rep. No. 111-176, The Restoring American Financial Stability Act of 2010, (2009-2010), Subtitle B, 181.
[16] Dodd-Frank Act, § 922a(h)(1) (2010).
[17] *Id*.
[18] Dodd-Frank Act, § 922a(h)(2)(A) (2010).
[19] Dodd-Frank Act, § 922a(h)(2)(C) (2010).
[20] Dodd-Frank Act, § 922a(h)(2)(D) (2010).
[21] *Id*.
[22] *Assessment of the SEC's Bounty Program* (U.S. Securities and Exchange Commission, Office of the Inspector General), Mar. 29, 2010 at 2, http://www.sec-oig.gov/Reports/AuditsInspections/2010/474.pdf.
[23] *Id*.
[24] *Id*. at 1
[25] S. Rep. No. 111-176, at Subtitle B, (2009-2010).
[26] David S. Hilzenrath, *Change in IRS Rules Could Block Rewards for Whistleblowers*, WASH. POST, Jul. 1, 2010, at A11.
[27] Janet Novack and William P. Barrett, *Tax Informants Are on the Loose*, Dec. 14, 2009, http://www.forbes.com/forbes/2009/1214/investment-guide-10-ubs-irs-spondello-tax-informants-on-loose.html; Martin Vaughan, *IRS Whistleblower Guidelines Spark Criticism*, Jun. 18, 2010, http://online.wsj.com/article/BT-CO-20100618-711526.html.
[28] *Id*.
[29] David Voreacos and Margaret C. Fisk, *AstraZeneca Case Rewards Two Whistleblowers with $45 Million*, May 13, 2010, http://www.businessweek.com/news/2010-05-13/astrazeneca-case-rewards-two-whistleblowers-with-45-million.html.
[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] Dworkin, *supra* note 3, at 1765.
[35] *Id.*
[36] Dodd-Frank Act, § 924(a) (2010).
[37] *Financial Reform Bill Includes FCPA Whistleblower Provision*, (McKenna Long & Aldridge, LLP), Jul. 26, 2010, http://www.mckennalong.com/news-advisories-2357.html.
[38] Dodd-Frank Act, § 929(h)(1)(B).
[39] Carnero v. Boston Scientific Corp. (*Carnero II*), 433 F.3d 1, 9 (1st Cir. 2006); Dworkin, *supra* note 3, at 1775.
[40] *Carnero II*, 433 F.3d at 15-19.
[41] Dodd-Frank Act, § 929(A).
[42] *Whistleblower Provisions in Dodd-Frank Legislation Provide Further Impetus to Increased FCPA Investigations and Enforcement*, (Steptoe & Johnson LLP), Jul. 26, 2010, http://www.steptoe.com/publications-7066.html.
[43] McKenna, *supra* note 37.
[44] *See* Alan C. Raul et al., *Reconciling European Data Privacy Concerns with United States Discovery Rules: Conflict and Comity*, 3 G.C.L.R. 119 (2009), *available at*: http://www.sidley.com/reconciling-european-data-privacy-concerns-with-us-discovery-rules-conflict-and-comity-07-01-2009/html.

[45] *SOX Applied to Employee Working Overseas*, (Jackson Lewis), Apr. 30, 2008, http://www.jacksonlewis.com/legalupdates/article.cfm?aid=1364.html.
[46] McKenna, *supra* note 37.
[47] Dodd-Frank Act, § 922a(b)(1) (2010).
[48] McKenna, *supra* note 37.
[49] *Id*.; Dodd-Frank Act, § 922a(c).
[50] Matt A. Vega, *The Sarbanes-Oxley Act and the Culture of Bribery: Expanding the Scope of Private Whistleblower Suits to Overseas Employees*, 46 HARV. J. ON LEGIS. 427, 478 (2009).
[51] *Id*. (citing Ass'n of Certified Fraud Examiners, *2008 Report to the Nation on Occupational Fraud & Abuse* (2008)).
[52] *Progress Report 2010: Enforcement of the OECD Anti-Bribery Convention*, (Transparency International), Jul. 2010, at 6, http://www.transparency.org/publications/publications/conventions/oecd_report_2010.html.
[53] *Id*.
[54] *Id*. at 8.
[55] *Id*. at 6.
[56] *Id*. at 8.
[57] *Id*. at 10.
[58] *Id*. at 13.
[59] Vega, *supra* note 50, at 489.
[60] *Progress Report 2009: Enforcement of the OECD Anti-Bribery Convention*, (Transparency International), Jun. 2009, at 9, http://www.transparency.org/publications/publications/conventions/oecd_report_2009.html.
[61] Marcia P. Miceli, Janet P. Near & Terry M. Dworkin, WHISTLEBLOWING IN ORGANIZATIONS 168 (2008).
[62] *Id*.
[63] *Whistleblowers*, (Working Rights), http://www.workingrights.co.uk/Whistleblowers.html.
[64] Elletta S. Callahan, Terry M. Dworkin & David Lewis, *Whistleblowing: Australian, UK, and US Approaches to Disclosure in the Public Interest*, 44 VA. J. INT'L L. 879, 895 (2004).
[65] *Id*.
[66] Miceli, *supra* note 61, at 174.
[67] Stephen Taub, *Multinationals Find SOX is Conflicting with Local Laws*, (Compliance Week), Jul. 19, 2005, http://www.complianceweek.com/article/1881/multinationals-find-sox-is-conflicting-with-local-laws.html.
[68] David Bender, *Whistleblower Debate*, New York Law Journal, Apr. 11, 2006.
[69] *Making Government Anti-Corruption Hotlines Effective*, (Transparency International, Working Paper No. 07/2009, 2009), at 3, http://www.transparency.org/publications/publications/working_papers/wp_07_2009_gov_ac_hotlines_09_dec_2009.html.
[70] Wu Zhong, *Dark Days for China's Whistleblowers*, Mar. 26, 2009, http://www.atimes.com/atimes/China/KC26Ad01.html.
[71] *Id*.
[72] Peter Ford, *Attack on China Whistleblower Shows Risk of Unveiling Corruption, Fraud*, Aug. 30, 2010, http://www.csmonitor.com/World/Asia-Pacific/2010/0830/Attack-on-China-whistleblower-shows-risk-of-unveiling-corruption-fraud.html.
[73] *Id*.
[74] Zhong, *supra* note 70.
[75] *China: Google Challenges Censorship*, (Human Rights Watch), Jan. 12, 2010, http://www.hrw.org/node/87654.html.; *see also*, Alexei Oreskovic, *Google Facing Many Risks in China Standoff*, Feb. 4, 2010, http://www.reuters.com/article/idUSTRE61408520100205.html.
[76] Human Rights Watch, *supra* note 75.
[77] *India Widens Security Crackdown, Providers Like Google and Skype Must Set Up India Server*, Sept. 2, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/09/02/AR2010090201461.html.
[78] *Id*.
[79] Oliver August, *The Great Firewall: China's Misguided and Futile Attempt to Control What Happens Online*, Oct. 23, 2007, http://www.wired.com/politics/security/magazine/15-11/ff_chinafirewall.html.
[80] *Id*.
[81] *Id*.

[82] Shabina Akhtar, *A Safety Net for Crusaders*, Aug. 25, 2010, http://www.telegraphindia.com/1100825/jsp/opinion/story_12852916.jsp.html.
[83] *Id*.
[84] *Id*.
[85] *Id*.; *RTI Activist Who Exposed Corruption in Maharashtra Found Dead*, (The Times of India), Aug. 29, 2010, http://timesofindia.indiatimes.com/india/RTI-activist-who-exposed-corruption-in-Maharashtra-found-dead/articleshow/6456957.cms.html.
[86] Akhtar, *supra* note 82.
[87] *Id*.
[88] Sumon K. Chakrabarti, *Why India May Issue a BlackBerry Ultimatum*, Aug. 10, 2010, http://www.time.com/time/world/article/0,8599,2009585,00.html.
[89] *Id*.
[90] *India Widens Security Crackdown*, *supra* note 77.
[91] Michael Stott, *Russia Corruption May Force Western Firms to Quit*, Mar. 15, 2010, http://www.reuters.com/article/idUSTRE62E1SU20100315.html.
[92] *Id*.
[93] David Leppard and Mark Franchetti, *Kremlin Bribery Whistleblower Flees to UK*, May 30, 2010, http://www.timesonline.co.uk/tol/news/uk/article7140175.ece.html.
[94] *Id*.
[95] *Id*.
[96] *Police Lost $500,000 Bribe Used in Sting, Owner Says*, (The Moscow Times), Aug. 20, 2010, http://www.themoscowtimes.com/news/article/police-lost-500000-bribe-used-in-sting-owner-says/413317.html.
[97] Alexsei Kuznetsov, *Whistleblower Tackles Russian Police Corruption*, Nov. 10, 2009, http://www.cbsnews.com/8301-503543_162-5599082-503543.html.
[98] *Id*.; Fred Weir, *Russian YouTube Whistleblower, A Cop, Arrested on Corruption Charges*, Jan. 25, 2010, http://www.csmonitor.com/World/Global-News/2010/0125/Russian-YouTube-whistleblower-a-cop-arrested-on-corruption-charges.html.
[99] Kuznetsov, *supra* note 97.
[100] Weir, *supra* note 98.
[101] *Russian Police Whistleblower Says Another Video 'Coming Soon'*, (RIA Novosti), Mar. 25, 2010, http://en.rian.ru/russia/20100325/158307403.html.
[102] Weir, *supra* note 98.