9-2011

# Nokia Siemens Networks: Just Doing Business – or Supporting an Oppressive Regime?

Judith Schrempf-Stirling
*University of Richmond*, judith.stirling@richmond.edu

# Nokia Siemens Networks: Just doing business — or supporting an oppressive regime?

**Judith Schrempf-Stirling**

University of Richmond, Robins School of Business, 28 Westhampton Way, 23173
Richmond, VA 23173, USA
Judith.schrempf@gmail.com
001 804 929 8194

## Abstract

This case study examines the relevance of taking social and political factors into consideration when a corporation is making a key business decision. In September 2009, Simon Beresford-Wylie, the outgoing CEO of Nokia Siemens Networks (NSN), was reviewing the company's achievements — while acknowledging the latest public criticism regarding NSN's business relationship with the Iranian government. In the summer of 2009, NSN was accused of complicity in human rights violations linked to Iran's presidential election. The company sold network infrastructure and software solutions to the Iranian government, which then used this technology to observe, block, and control domestic communications. Should NSN have acted differently?

Students are asked to examine the economic and moral arguments for and against selling products to an oppressive regime that might then use those products to violate human rights. In such a case, does the corporation bear co-responsibility for human rights violations committed by an oppressive regime?

**Keywords**: censorship, complicity, human rights, corporate social responsibility, Nokia Siemens Networks

**September 2009**

For more than two years, Simon Beresford-Wylie had served as Chief Executive Officer (CEO) of Nokia Siemens Networks (NSN). In October, Rajeev Suri was poised to replace Beresford-Wylie as NSN's new CEO. During his final working days at NSN, Beresford-Wylie reflected on the company's achievements during his stint as CEO, but also acknowledged the latest public criticism concerning NSN's business relationship with the Iranian government (Lake, 2009).

Beresford-Wylie recalled the *Wall Street Journal* article titled "Iran's Web Spying Aided By Western Technology" (Rhoads and Chao, 2009). The article gave details about the company's 2008 transaction with the Iranian government involving the sale of so-called "monitoring centers" that enabled the Iranian government to observe, block, and control communications such as telephone calls and short messages.

Following the *Wall Street Journal* article, several other articles and publications reported on NSN's business with Iran, alleging that the company had sold a spy system (Lake, 2009). Non-governmental organizations (NGOs) and activists subsequently criticized NSN's dealings with the Iranian government and argued that the company was an accomplice to the regime's human rights violations. In particular, NGOs and activists claimed that "Neda's[1] blood sticks on Nokia products" (Tomik, 2009) and referred to NSN as "a handyman of dictatorship" (Hartmann et al., 2009). Boycotts of Nokia and Siemens products followed (Kamali Dehghan, 2009).

Beresford-Wylie recalled the transaction in detail. The decision had been made. But now that he saw the consequences, the outgoing CEO wondered whether his company — or he — should have done things differently.

**Simon Beresford-Wylie[2]**

Beresford-Wylie studied economic geography and history at the Australian National University and completed an Executive Development Program offered jointly by Stanford University and the National University of Singapore. Before joining private industry, he worked for the Australian government on taxation and industry policy. In 1989, Beresford-Wylie joined the private sector and had worked there since, holding various senior management positions.

Before joining Nokia in 1998, Beresford-Wylie served as CEO of Indian mobile operator Modi Telstra. At Nokia, he held various senior positions, such as Managing Director of Nokia Networks in India, the head of Nokia's infrastructure business group, and Senior Vice President of Customer Operations for Nokia Networks. Overall, his positions, both in Asia and Europe, involved close customer contact.

In 2007, Beresford-Wylie was promoted to CEO of NSN. On the company's Web site, the new CEO was described as follows: "Simon is a results-oriented business leader with a passion for the industry, the customer and execution excellence. He has built a reputation as a strong leader, people manager and communicator. He holds the Nokia Siemens Networks values dearly and is committed to steering the company and its people towards the goal of becoming the world's most visionary and customer-dedicated enabler of communications services."

**Nokia Siemens Networks (NSN)**

A 50:50 joint venture between mobile communications equipment manufacturer Nokia and electrical equipment giant Siemens, NSN started operations in April 2007. Nokia was a world leader in the mobile communications sector. The corporation's product and service portfolio included mobile phones, equipment, and solutions for businesses and consumers, plus imaging, game, and media applications. It sold equipment, solutions, and services to network operators and corporations alike (Nokia Homepage, n.d.).

Meanwhile, Siemens' product offers spanned information and communications, automation and control, power, transportation, medical devices, and lighting. The German company was a global powerhouse in electrical engineering and electronics (Siemens Homepage, n.d.). NSN combined Nokia's network business group with Siemens' communications carrier-related expertise. Siemens retained a non-controlling financial interest while Nokia handled day-to-day business operations.

The joint venture produced one of the world's biggest telecommunications infrastructure companies. Headquartered in Espoo, Finland, in 2008 NSN's net sales totalled 15.3 billion euros (Nokia Siemens Networks, n.d.). Over 1.5 billion people connected through NSN networks: the company boasted the number two position worldwide in wireless networks and operator services. NSN operated in more than 150 countries with some 60,000 employees serving 600 customers.

NSN clients included communications service providers (CSPs), governments, and businesses. CSPs are public or private corporations that deliver information electronically. Examples include wireless telecommunications operators and Internet service providers such as Orange, T-Mobile, and Vodafone. NSN provided CSPs with technology and infrastructure that enable data transport and communication, including microwave antennas, repeater stations, and satellite links. In short, NSN furnished the infrastructure that made Internet and mobile communications possible.

NSN offered a comprehensive service and product portfolio, including mobile, fixed, and hybrid network infrastructure solutions. The company provided hardware and software components for voice, data, and mobile network communications.

Specifically, it provided CSPs with infrastructure that enables wireless and mobile telecommunication transfers. Its software solutions encompassed products that inspect, analyze, and manage mobile voice and data traffic. The software packages allowed service

operators to observe, control, and manage data flow and improve network efficiency. The software could also be used for Web censorship, Internet filtering, and data inspection.

Because the Internet can be used as a vehicle for criminal activities such as child pornography or terrorism, certain legal regulations and standards allow "lawful interception." Software with control capabilities can be used to prohibit child pornography, locate terrorists, or fight corruption and money laundering. Several standards bodies, such as the European Telecommunications Standards Institute (ETSI), the 3rd Generation Partnership Project, and the Communications Assistance for Law Enforcement Act (CALEA)[3] provide guidelines regarding lawful interception. In the European Union, lawful interception capabilities are required, forcing corporations such as NSN to provide relevant technology to network operators when selling network products and services. NSN's term for its lawful interception software is "monitoring center." NSN's monitoring centers can enable Internet service providers to monitor voice and/or data transmissions, depending on how the system is set up.

**Market Competition**

The telecommunications market had two noteworthy characteristics: First, the mobile and Internet communications sectors were highly promising. Emerging markets and rapid broadband Internet and mobile network diffusion were key drivers of this growth (Business Insights Ltd., 2008a). Demand for sophisticated networks was high not only in Western nations but in emerging countries as well. Latin America, India, and Iran held special growth potential, as all wanted to improve wireless and mobile connectivity (Business Insights Ltd., 2008a).

Second, in recent years telecommunications sector competition had intensified due to rapid technological changes. NSN's competitors included Alcatel-Lucent, Ericsson, Cisco Systems, and Huawei. Competition was particularly severe from Chinese vendors such as Huawei (Business Insights Ltd., 2008b). Asian and Chinese vendors enjoyed government

funding and could therefore undercut average industry prices. Due to fierce price competition, each competitor was eager to win new business. This was the case for NSN, too, when in 2008 it closed its deal with the Iranian government to expand the country's mobile network.

**Nokia Siemens Networks and the Iranian Government**

Since NSN's founding, the company had enjoyed business relationships with many governments, including Iran's. The Iranian government wanted to expand the nation's wireless and mobile networks, and approached NSN with a request to provide the necessary equipment, infrastructure components, and upgrades. In the course of the transaction, NSN provided TCI, a state-controlled Iranian communications operator, with lawful intercept software that enabled TCI to monitor conversations conducted with both mobile and landline telephones.

Telecommunication suppliers were legally obliged to provide CSPs with lawful intercept capability. These legal regulations were in force in most Western countries as well as in Iran. Moreover, such requirements were described in internationally recognized standards such as ETSI and CALEA. Such control and monitoring devices enabled government customers fight crime: The voice and data monitoring capability, for instance, could help identify and capture terrorists, drug dealers, and other criminals, such as providers of child pornography. The monitoring center could therefore be used for socially desirable purposes.

NSN's provision of lawful intercept capability to the state-controlled operator TCI drew public attention in the summer of 2009 following the controversial Iranian presidential election. Critics claimed the technology supported government censorship and illicit control over citizen communications.

*Iran's Political Regime*

In 1979, the Iranian Revolution ended the monarchy of Shah Mohammad Reza Pahlavi, who had long been criticized by the Iranian clergy for his pro-Western policies and warm relationship with the United States. The conservative spiritual leader Ayatollah Ruhollah Khomeini, who had led the revolution, proclaimed the nation the Islamic Republic of Iran, and became its Supreme Leader. As Supreme Leader, Khomeini wielded ultimate political and religious power within Iran. The Supreme Leader, for example, made key political and judicial appointments including military commanders, National Security Council members, the chief judge, and half the members of the Guardian Council, who had legislative as well as executive powers. The Guardian Council approved not only laws but presidential election candidates. While the president of Iran was the highest publicly elected political official, he remained subordinate to the Supreme Leader. The president's primary responsibility was to implement Iran's constitution. As head of the executive branch, he was, for example, in charge of signing treaties, budget planning, and national employment affairs. But he lacked complete control over foreign policy, the military, and other issues (BBC News, n.d.). The Supreme Leader was the final decision maker in areas of security, defense, and foreign policy (Amnesty International, 2009).

The post-revolution era was marked by international tension (BBC News, 2005a), conflicts (Iran-Iraq war) (BBC News, 2005b), and anti-Western (largely anti-U.S.) policies (CBC News, 2009). The cleric Ali Hoseini Khamenei succeeded Khomeini following Khomeini's death in 1989, and was serving as Iran's Supreme Leader by the time NSN started doing business in Iran. He continued Khomeini's opposition to the West and to the United States in particular.

After a conservative presidency lasting nearly twenty years, the reformist Mohammad Khatami became Iran's president in 1997. During his governance, Khatami tended to support freedom of expression, tolerance, and civil society, which led to tensions between his government and the conservative clergy. Anti-government protests resulted, and in the 2005

presidential election, many reformist candidates were banned and the conservative hard-line candidate Mahmoud Ahmadinejad won.

Despite the reformist interlude, Iranian policy has remained largely dominated by the clergy and conservatives. The Supreme Leader's power was undeniable. The U.S.-based Committee to Protect Journalists referred to Khamenei as one of the "ten worst enemies of the press and freedom of expression" (Committee to Protect Journalists, 2000). Khamenei was considered the driving force behind media censorship and control in Iran.

*Censorship and Control in Iran*

Censorship, anchored in Iran's constitution and the 1989 Press Law and its amendments, had a long tradition in Iran. According to the country's constitution, publications must not "violate Islamic principles or the civil code" (Mackey, 2009). The 1986 Press Law provided further publication guidelines. The press had to "advance the objectives of Iran, counteract internal division among citizens, propagate Islamic culture and principles, and reject manifestations or imperialistic culture as well as foreign politics and economic politics" (OpenNet Initiative, 2005, p. 8). Publishers were required to acquire licenses from the Ministry of Islamic Culture and Guidance. Government control extended to regulating publication names and publishing timetables. The overarching mantra was that publications needed to serve the best interests of the community and never "violate Islamic principles and codes and public rights" (OpenNet Initiative, 2005, p. 9).

Media content was monitored by the Supreme National Security Council. Regulatory restrictions applied to topics such as religion, morals, national security, politics, and anti-revolutionary activity. The Council furnished publishers with a list of banned subjects (Feuilherade, 2002; Reporters Sans Frontières, 2004). While some independent newspapers continued to operate, their numbers were diminishing. Many newspapers applied self-censorship to avoid sanctions. Violations were reported and referred to a special press court.

The Iranian government sought to control television broadcasts as well. Satellite dishes, for instance, were officially forbidden. The government frequently blocked foreign television broadcasts, as in 2003 when U.S. television channels were blocked (Carter, 2003). While the Press Law had initially applied to print media, radio transmissions, and television broadcasts, the surging use — and importance — of Internet communications caused the Iranian government's censorship to gradually extend to this media channel as well.

*Internet Censorship*

The Middle East, and Iran in particular, was experiencing a tremendous increase in Internet usage. In 2001, Iran had approximately one million Internet users, but by 2009 this number had swelled to over 30 million, representing nearly half of Iran's population (Internet World Stats, n.d.). In 2009, the OpenNet Initiative estimated Iran's annual Internet user growth rate at 48 percent, and nearly 2,000 cybercafés were operating in Tehran alone, the nation's capital (OpenNet Initiative, 2009). The Internet had become a crucial information resource and communication channel, and the most trusted media platform, for Iran's population. Blogs were frequently used and growing tremendously in both number and credibility.

When Internet access first became available in Iran, the Internet was essentially an uncontrolled communication medium. This had enabled independent, uncensored publications and opposing viewpoints to spread. Iranian expatriates, for example, had used the Internet to publish their views on the Iranian government and its politics. The Internet's growing popularity, however, did not go unnoticed by the Iranian government. In 2001, the government started censoring online dissension, including bloggers, Web sites, and other online media. The government's Internet censorship efforts ran the gamut from establishing new government agencies and regulations to technical control mechanisms and punishment, including imprisonment and even torture (Human Rights Watch, 2005).

All commercial Internet Service Providers (ISPs) were required to connect to the Internet via the state-controlled Telecommunication Company of Iran (TCI). All Internet traffic, therefore, ran through a government-controlled gateway. This centralization facilitated both censorship and control. In general, all ISPs needed to be approved by TCI and the Ministry of Culture and Islamic Guidance. In 2001, TCI established guidelines requiring that all ISPs had to filter any material that might be considered immoral or threatening to state security. This included filtering the Web pages of opposition groups (OpenNet Initiative, 2005). Since 2001, Internet providers have been required to install filtering software (Proschofsky, 2009).

The main targets of the filtering efforts were Web sites dealing with national issues, particularly those critical of the Iranian state, and especially those featuring local language (Persian and Farsi) content. The filtering software monitored both Web sites and e-mail messages. To sum up the government's filtering program, all politically sensitive sites (including blogs) as well as sites including gay and lesbian content or information about women's rights, were blocked. Iran had one of the "most sophisticated state-mandated filtering systems" (OpenNet Initiative, 2005, p. 3).

Initially, Iran relied on SmartFilter, a commercial software product from the United States. SmartFilter blocked not only English language Web pages hosted overseas but also Web pages with local language content. Web pages hosted within Iran were also shut down, suspended, or filtered. But later Iran tried to eliminate its dependence on Western Web-filtering technology. The government considered use of Western technologies a weakness, and even a potential threat to the Iranian Internet.

A number of Iranian technology corporations therefore started developing filtering software (Rooz, 2008). Iranian technology enabled the government to search the Internet for specific keywords and questionable content it had defined internally. "With the emergence of this domestic technical capacity, Iran joins China as the only countries that aggressively filter

the Internet using their own technology" (OpenNet Initiative, 2009, p. 4). In addition to implementing sophisticated filtering mechanisms, the government established a blacklist of Web sites featuring questionable content (BBC News, 2003). Between 2004 and 2009, five million Web pages were reportedly blocked (Proschofsky, 2009).

The Iranian government established various new agencies to administer its regulations and undertake its censorship efforts. The Supreme Council of the Cultural Revolution (SCRC) passed filtering system decrees in 2001. The Committee in Charge of Determining Unauthorized Sites (CCDUS) outlined criteria for identifying unauthorized Web pages and blocking them when appropriate. The Information Technology Company of Iran (ITC) was responsible for filtering decisions. Finally, the Communication Infrastructure Company unified filtering policies nationwide (OpenNet Initiative, 2009).

Governmental censorship for all media forms (online and offline) intensified just before the 2004 parliamentary elections. Reformist newspapers were closed, journalists were arrested, and several Web pages (including pro-reformist sites) were blocked. With the election of President Mahmoud Ahmadinejad, censorship increased markedly. Reporters Without Frontiers (RSF) labeled Iran "an enemy of the Internet" (Reporters Sans Frontières, 2009) and the OpenNet Initiative called Iran's Internet censorship policies "pervasive" (OpenNet Initiative, 2005).

In 2006, for example, the government set limits on Internet access speeds. According to this regulation, ISPs were prohibited from providing households and public Internet access points (cybercafes) with access speeds exceeding 128 kilobytes per second. This made downloading multimedia content cumbersome. While this measure may have helped prevent the viewing of criminal content such as child pornography, it naturally thwarted the viewing of neutral content such as international news as well. Only universities and private businesses were allowed to enjoy high-speed broadband Internet service. Both censorship efforts and civil opposition to those efforts escalated during and after the 2009 presidential election.

*Iran's 2009 Presidential Election*

Mahmoud Ahmadinejad, the incumbent president, faced several opponents in the presidential election that took place on June 12, 2009. Mir-Hossein Mousavi, the reformist candidate, was the strongest opponent. Ahmadinejad won with 62.6 percent of the vote compared to Mousavi's 33.8%.

Mousavi and his followers challenged the results and accused the government of election fraud. Several censorship measures taken immediately before the election fueled the fraud allegations. Prior to the election, the Ahmadinejad government had issued an amendment to the Press Law aimed at applying Press Law rules to domestic news sites and Web pages. Personal Web pages and blogs fell under this ruling, thereby undermining freedom of speech on the Internet. Essentially, the amendment made it mandatory to obtain a license to produce Web pages. The result of this amendment was that "bloggers and online media sources would also be subject to the regulatory authority of the Press Supervisory Board under Ministry of Islamic Culture and Guidance, which has the power to revoke licenses, ban publications, and refer complaints to a special Press Court" (OpenNet Initiative, 2009, p. 5).

Critics charged that Ahmadinejad had tried to diminish the online influence of political competitors (OpenNet Initiative, 2009). Online and mobile communication traffic was frequently blocked and monitored during this time, and several sites, including Google and Yahoo, were blocked, making e-mail service through them inaccessible. Additionally, several social networking platforms such as Facebook and Twitter were blocked in the spring of 2009 (Bozorgmehr, 2009; The Guardian, 2009). These services were particularly favored by reformists as platforms for political organizing and campaigning (Amnesty International, 2009). Ahmadinejad and his government, however, denied blocking these sites. Yet other social networking Web sites, too, such as MySpace.com, Flickr.com, YouTube.com, and

Orkut.com, had reportedly been frequently blocked prior to the election (OpenNet Initiative, 2009).

In addition to Internet traffic blocking, the Iranian government increasingly monitored online text and e-mail communications before and after the election. The OpenNet Initiative reported that following their arrest, female activists were confronted with transcripts of their instant messaging communications (OpenNet Initiative, 2009). This indicated that the Iranian authorities possessed comprehensive monitoring tools that enabled comprehensive inspection of multiple forms of online communications. Observers have suggested that these monitoring activities might have been the reason for decreased Internet speeds prior to, during, and after the elections (Cellan-Jones, 2009).

*Civil Society's Response: The Twitter Revolution*

Demonstrations, riots, and street battles between Mousavi followers and military groups followed the controversial election results. Mousavi followers used social media platforms such as Facebook and Twitter to organize demonstrations, mobilize protests against the government, and appeal to the public. In the Facebook group "Where is my vote," some 17,000 participants exchanged their views on the dubious Iranian presidential election.[4] In addition to organizing demonstrations, university students used Twitter and the video platform YouTube to provide minute-by-minute updates on the latest developments in Tehran (Washington Times, 2009). Real-time Twitter messages and YouTube video clips enabled people around the world to view the riots and gain a basic understanding of the political situation in Iran. International interest was so intense that Twitter postponed its regular maintenance work to ensure that information flowed from Iran to the outside world (The Washington Post, 2009).

The Iranian government reacted to the increased use of Twitter and other social media platforms by slowing Internet speeds and temporarily blocking Web sites (Rhoads et al.,

2009). Along with Internet traffic blocking and monitoring, mobile communications traffic was constrained following the election. The Committee to Protect Journalists reported that both mobile phone services and short message services (BBC News, 2009) had been intermittently interrupted in Iran (Committee to Protect Journalists, 2009).

Despite governmental censorship efforts, the election protests continued into the summer of 2009. But the Iranian government's monitoring capabilities enabled its representatives to interfere, block communications, and even identify and locate senders of specific messages. For example, several women rights activists were reportedly arrested at a secretly agreed-upon meeting place, indicating that their private communications had been intercepted (Lake, 2009).

In short, monitoring capabilities made it possible for the government to locate and arrest dissidents. Once arrested, dissidents often became victims of torture and/or threats, including beatings, mistreatment, and forced confessions, according to Amnesty International reports (Amnesty International, 2009). Violent government action against dissidents, including harassment and persecution, had a noticeable effect: online activity by anti-government activists declined in the late summer of 2009. Bloggers with national audiences who posted views critical of the government and the election results were arrested and beaten and their blogs vanished (Gross, 2009). Amnesty International reported that some of its former Iranian informants ceased all communications with them due to threats by military groups.

As a result, the question of how the Iranian government managed to create such a sophisticated communications monitoring and censorship system drew increasingly sharp public attention.

**Worldwide Civil Reaction to NSN's Transaction with Iran**

The controversial election results, escalating protests and violence, and growing reports of Iranian censorship triggered speculation about how the Iranian government acquired such sophisticated monitoring capability. Shortly after the election, the media reported that NSN had assisted the Iranian government in setting up a highly robust monitoring and censorship system. In particular, reports claimed that NSN's technology enabled the Iranian government not only to monitor local voice telephone traffic, but also mobile data and Internet traffic, including so-called deep packet inspection.

Deep packet inspection allows authorities to scan and search e-mail messages, Internet phone calls, and instant messaging traffic for specific keywords. The technology allows such data to be examined for keywords within milliseconds (Rhoads and Chao, 2009). According to media reports, the Iranian government had experimented with the technology in early 2009, but implemented it in full force following the election. In a *Wall Street Journal* article a network engineer stated that monitoring technology such as that provided by NSN enabled the Iranian government "to do very complex tracking on the network" (Rhoads and Chao, 2009).

While news reports could not confirm that the Iranian government had in fact used NSN's technology to monitor its citizens, civil and human rights groups consistently linked NSN to the oppressive Iranian regime. Human rights groups condemned business deals such as the one struck between NSN and the Iranian government as undermining freedom of speech and contributing to the suppression of dissent. Representatives of a number of civil groups called for boycotts of Nokia and Siemens products (Kamali Dehghan, 2009), and drove home their criticisms with techniques including "adbusting."[5]

For example, they mocked Nokia's slogan of "connecting people" by promoting alternatives such as "Connecting Dictators," "Disconnecting people," or "Spying on People," "Jailing People," and "Shooting People." Figure 1 provides examples of adbusting. Appendix A provides a brief overview of key events related to the 2009 Iranian presidential election.

---

Insert Figure 1 here

---

**September, 2009: Nokia Siemens Networks Headquarters in Espoo, Finland**

Recalling the heated debate over NSN's business dealings with the Iranian state, Beresford-Wylie wondered whether there had been any acceptable alternatives to his company's decision to sell products and services to Iran's government. True, filtering mechanisms in the wrong hands could have negative social consequences, but wasn't it better to provide people with communication capabilities than with nothing at all? Besides, NSN was simply carrying out its business and obeying the law. Competition was tough.

What's more, in March of 2009 NSN had sold its Intelligent Solutions division — which handled monitoring centers and related software solutions — to German holding company Perusa Partners Fund LLP. Therefore the monitoring center business was no longer part of its business. Even though the decision had been made, Beresford-Wylie wondered whether NSN — or he — could have done things differently.

**Notes**

[1] On June 20, 2009 a student named Neda Agha-Soltan participated in protests in Tehran. During the demonstration Neda was shot and her death filmed by co-protesters. The film was soon uploaded on the video platform YouTube (www.youtube.com). As a result, Neda became known as a "symbol of rebellion in Iran" (Weissenstein and Johnson, 2009).

[2] The original text of the biography can be found online here: http://web.archive.org/web/20080502141916/http://www.nokia.com/A4126338 (accessed Nov 2, 2010).

[3] More information about the standard bodies can be found on their respective Web sites: http://www.etsi.org; http://www.3gpp.org; and http://www.askcalea.net.

[4] The Facebook group can be viewed here: http://www.facebook.com/group.php?gid=84334119822 (accessed Nov 3, 2009).

[5] Adbusting (also known as "subvertising" or "cultural jamming") refers to the spoofing or parodying of corporate or political advertisements in order to present audiences with alternative views of the issue to which the original advertisement refers. For some more information on adbusting and its origins, see Chapter 12 in "No logo" by N. Klein.

**Appendix A:** Selected events surrounding the 2009 Iranian presidential election and post-election riots

| Month | Day | Event |
|---|---|---|
| **June** | 12 | Presidential election takes place. |
| | 13 | Protests begin and continue throughout June. Riots between protestors and police officers escalate. Protesters are beaten and arrested. |
| | 14 | Mousavi asks the Guardian Council to annul election. |
| | 14-17 | Worldwide protests against the allegedly fraudulent election, erupt in London, New York, and elsewhere. |
| | 16 | Mousavi demands new election.<br>The Iranian government restricts foreign media reports about riots. |
| | 19 | Supreme Leader Khamenei warns protesters and urges them to stop. |
| | 20 | Video of Neda's death circulates worldwide. |
| | 21 | *Newsweek* reporter arrested in Iran. |
| | 23 | The Guardian Council rejects opposition demand for election annulment.<br>U.S. President Obama condemns violence against protesters. |
| | 24 | Supreme leader Khamenei insists that election results are final. |
| | 26 | The Guardian Council states that the 2009 presidential elections were "the healthiest since the revolution." Senior cleric Khatami expects protestors to be punished "ruthlessly and savagely". |
| | 28 | Members of U.K. embassy in Iran are arrested for their involvement in |

post-election riots.

29 The Guardian Council certifies election results.

**July** 4 Some religious leaders call the election and the new government illegitimate. The split within the country deepens.

9 Protests resume after an 11-day quiet period.

17 Former president Rafsanjani criticizes the government's handling of post-election unrest in the country.

25 Human rights organizations urge worldwide peaceful protests against the elections.

30 Riots erupt on the day of Neda's funeral when hundreds of Mousavi supporters gather to mourn. Police officers force Mousavi to leave.

**August** 5 President Mahmoud Ahmadinejad is sworn into office.

**Appendix B: Teaching guidance**

*Suggested questions and brief answers*

1. What might have been Beresford-Wylie's perception of the business deal at the time the transaction took place in 2008?

   Please note that the case study takes a retrospective view. NSN concluded its transaction with the Iranian government in the summer of 2008. In 2009, as he prepared to leave the company, Beresford-Wylie was reflecting on his time as NSN's CEO and reviewing the company's dealings with the Iranian government.

   For this question, anything that happened in 2009 (elections, riots etc) should be ignored. Beresford-Wylie (and NSN generally) would not have known, or could not have reasonably been expected to know, that the company's business relationship with Iran would be eventually criticized. For this question, focus student attention on managerial issues and on Beresford-Wylie personally, and how he might have perceived the business opportunity in 2008.

   Who is Beresford-Wylie?

   Beresford-Wylie is an experienced manager who held various senior positions at Nokia and other companies before becoming CEO of NSN. His background is likely to have exerted significant influence on how he perceived the situation in 2008. Beresford-Wylie might have looked at NSN's business dealings with the Iranian government from the following perspectives/mindsets:

      1. **Economic mindset:** As the CEO of a multinational company, Beresford-Wylie surely considers the economics of any transaction, especially considering the fierce competition NSN faced. Could competition have

justified the deal but narrowed Beresford-Wylie's perception? The intensity of the competition might have led to a "get the deal whatever it takes" mentality.

**2. Compliance-mindset:** As with a general analysis of economic conditions (such as competition), corporations routinely check to ensure their business activities are legal. As explained in the text, NSN regularly served government customers. Therefore Beresford-Wylie might not have given any additional thought to the decision as to whether or not to do business with the Iranian government (especially if we consider that Beresford-Wylie worked for governmental agencies himself before joining the private sector).

**3. Customer oriented mindset:** As noted at the beginning of the case, Beresford-Wylie had worked closely and directly with customers. Hence, he was strongly oriented toward satisfying customer requests. This becomes clear if we look at NSN's description of Beresford-Wylie (p. 4): he has a passion for customers and strives to make NSN a customer-centric enabler of communications services. This customer-oriented mindset may have been particularly strong considering that Beresford-Wylie had worked in the public sector (Australian government) before joining private industry. He therefore was likely to have perceived government agencies as ordinary customers rather than as entities to be regarded with some suspicion.

Considering the above-mentioned mindsets, we might conclude that in 2008 Beresford-Wylie viewed the transaction through a utilitarian lens. As mentioned in his biography (p. 4), Beresford-Wylie was a results-oriented business leader whose goal was to make NSN the world's most visionary, customer-centric enabler of communication services. Doing business with the Iranian government had positive results: Strengthening NSN's competitive position and satisfying a demanding

customer (with good prospects for further business). This brought NSN closer to its goal of becoming number one in its industry.

2. What might have been Beresford-Wylie's perception of the business deal *in September 2009, after the Iranian election*?

   This question requires considering the 2009 elections and riots, events that might have changed Beresford-Wylie's previous perceptions. How might the 2009 riots and civil unrest have changed Beresford-Wylie's (utilitarian) view of the business deal?

   Beresford-Wylie might have continued supporting the business transaction by focusing on economics: after all, NSN was an economic, not a political actor. According to this view, it could ignore political issues when doing business.

   Yet Beresford-Wylie might also have asked himself whether good results always justify the means by which those results were obtained. Besides viewing the situation through a utilitarian lens, he might at least acknowledge a Kantian perspective of the situation, as the end of the case illustrates. The case demonstrates the limitations of utilitarianism (utility distribution, subjectivity, and problems of quantification). A Kantian approach, in contrast, stresses that results do not justify means.

   As indicated by the brief answers, the first two questions allow a detailed comparison of consequentialist and non-consequentialist ethical theories.

3. What does stakeholder analysis tell you about the stakeholders and their interests?

   Stakeholder analysis is a useful tool for acquiring a reasonable overview of the interests of all parties involved. A stakeholder is any actor who affects or is affected by a company's activity. Depending on what was previously discussed about

stakeholder theory in class, this analysis could be a brief discussion or a detailed debate. Following are some suggestions for guiding the discussion:

**Customer (Iranian government):** As the customer, the Iranian government was a key stakeholder that wanted to expand its wireless and mobile networks. Iran is a growth market and satisfying this customer might lead to future business opportunities.

**NSN shareholders:** NSN shareholders expect the company to execute profitable business deals. They expect NSN and its senior management to make efficient economic decisions.

**Nokia and Siemens**: NSN is a joint venture between mobile telephone manufacturer Nokia and electrical equipment giant Siemens. These two prominent companies are naturally interested in NSN doing well. Also, Nokia and Siemens want to avoid negative publicity surrounding their involvement in NSN. The adbusting examples in Figure 1 illustrate Nokia's (and Siemens') vulnerability. Hence, the two companies bear economic as well as reputational risk.

**Competitors**: As mentioned in the text, the competition is fierce and NSN's competitors were keen to win business.

**NSN employees**: NSN's employees are primarily interested in continued employment. This means that employees want NSN to perform well and earn a profit. For some employees, though, it might also be important that the company respect human rights. These employees may sense a dilemma between earning profits and remaining ethical.

**Iranian population**: The Iranian population is also a stakeholder group which must be mentioned in the stakeholder analysis. Iranians are interested in access to the Internet and the latest communications technology (especially given the Iranian government's censorship efforts). For Iranian citizens, communications technology can be a

blessing, but its misuse can also have negative effects, as illustrated by the riots and violence which followed the presidential election. A good tool in the wrong hands might not be good after all.

**Non-governmental organisations (Amnesty International etc**.): The case briefly mentions that several human rights groups such as Amnesty International educated the public about censorship and human rights violations in Iran. These organisations were active before NSN started doing business in Iran. NGOs might be considered key stakeholders as they are sometimes the only public voice of minority groups or victims of human rights violations. Also, these groups can put considerable pressure on corporations and affect corporate reputations and even profits over the long run (examples include 1990s anti-Nike sentiment arising from conditions in Asian sweatshops).

Besides identifying the stakeholders and their respective interests, students could also be asked to assess each stakeholder's importance (in terms of legitimacy, power, and urgency).

4. What are the arguments for and against doing business with the Iranian government?

   Key conflicts/dilemma addressed by the case:

   - Being profitable versus being moral
   - Responsibility for one's own activities versus responsibility for what others do with one's products
   - Being an economic versus political actor

| **For the deal** | **Against the deal** |
|---|---|
| Focus on the end result: Providing Internet access is a good thing from a utilitarian perspective. The Iranian population has | Focus on the means: Following Kant's duty ethics argues against the deal. The ends do not justify the means. |

| | |
|---|---|
| communication access, the Iranian government is a satisfied customer, and NSN makes a profit. | |
| Tool of democratization: In the long term, the technology might be advantageous for everyone. Despite censorship, people in Iran are better off with some Internet access. The power of communication technology is illustrated by the Green Twitter Revolution. It can foster communication. | Tool of oppression: A good tool in the wrong hands might not be good after all. In the wrong hands, the tool can cause considerable harm: Dissidents were arrested, beaten and suppressed. Such technology can suppress rather than foster communication. |
| Good product, bad use: It is not the product that is problematic but how it is used. The use or misuse of a product is not the responsibility of the seller. It is the user who is responsible. | Corporate complicity: In recent years, corporations have increasingly been accused of complicity in human rights violations (e.g. Shell and the Ogoni crisis). Is a corporation responsible for ensuring proper use of the products it sells? |
| Someone will do it: NSN could not have changed the situation. If NSN had not sold the technology, some Chinese company would have. | Moral responsibility: This argument does not release NSN from moral responsibility. Iran was known for human rights violations and censorship. |
| Legality: Lawful interception is legal and mandatory. This technology's intention is good: protect society from illegal activities (terror, child pornography, etc). | Legal does not mean moral: Business ethics deals with a grey area: just because an act is legal does not mean it is morally legitimate (examples are Apartheid or Yahoo in China). Classic work in business ethics argues for going beyond legal compliance. |
| We could not have known: NSN did not know and could not have reasonably foreseen the risk of riots and civil unrest following the presidential elections. | Duty to know: NSN failed to conduct a geopolitical risk analysis (no due diligence). The key question is: Could NSN truly not have understood the risks? Or did it simply fail to obtain all possible information? Human rights organizations have regularly reported on censorship and human rights violations in Iran. |
| No political role: Corporations are economic actors. They do not have the standing or authority to evaluate governmental activities. | Silent complicity: Operating with or under an oppressive regime can be interpreted as passively approving of the regime. |
| Discrimination and negative business consequences: If NSN does not sell its product to Iran, it might trigger a debate about discrimination. If NSN does not do business with Iran, what would this mean for other potential customers? Can NSN do business with Nigeria? Myanmar? Iraq? Russia? China? The USA? | Negative reputation consequences: There is growing pressure on companies that work with or under oppressive regimes (review cases filed under the Alien Torts Claims Act, for example). Also look at adbusting activities. |
| Western imperialism. Why should the principles and norms of Western countries take precedence over those of other nations? | Universality of human rights. The international community, including corporations, cannot ignore violations of |

| | |
|---|---|
| | fundamental human rights. |

5. Does Nokia Siemens Networks bear responsibility for the events in Iran following the 2009 election? What lessons can be learnt?

   This question builds on the previous one and asks students for their opinions. Is NSN responsible for the unintended side effects of its business operations?

   Yes, NSN bears responsibility for the events in Iran following the 2009 election:

   - NSN violated its duty to be informed
   - The political context of business transactions must not be ignored. Corporate activities are always embedded in a political context. Therefore, in contrast to what general management theory still assumes, economic and political aspects of a situation cannot be considered separately. NSN is an accomplice to Iran's human rights violations.

   No, NSN is not responsible for human rights violations. This perspective can be supported by relying on an economic mindset. NSN itself did not hurt any activists. The Iranian regime committed the violations. We can also take a slightly different perspective here and argue that NSN was not responsible for the recent human rights violations following the 2009 election. The company might, however, be responsible for the *efficiency* of the violence. Iranian agencies might have punished dissidents and activists sooner or later anyway, but NSN's technology facilitated the identification of dissidents and enabled the Iranian regime to punish them more quickly. Perhaps this is where NSN's responsibility lay.

Lessons learnt:

- Do not violate the duty to be informed. Thorough geopolitical risk analysis can enable companies to assess the potential side effects and consequences of their business activities.
- Consult home governments, international institutions, and NGOs as part of this risk analysis.

*Courses*

The case study was written primarily for business ethics courses at all levels, undergraduate and graduate. The case has also been successfully used in executive MBA classes. In addition to business ethics classes, the case can be used in corporate social responsibility or decision-making courses. Even though the case is not a classical decision-making exercise (the decision has already been made), discussing the protagonist's reflections on his decision can create sensitivity among students regarding the various dimensions involved in making a decision.

*Case Objectives*

- Analyze the relevance of due diligence in corporate decision-making
- Examine corporate complicity in human rights violations
    - The relevance of due diligence and corporate complicity in human rights violations is prevalent in practice and in theory. First of all, in recent years corporations have increasingly been accused of complicity in human rights violations (Shell in Nigeria, Coca-Cola in Colombia, Google and others in China, and so forth). Second, in 2005 the UN Human Rights Council appointed Professor Ruggie to propose a framework for measuring corporate human rights performance. In his reports, Ruggie examines the concept of

complicity and due diligence. For example, he elaborates on the corporation's duty to become aware of human rights violations, prevent them, and mitigate related adverse effects. His proposed framework and suggestions will be reviewed in 2011 by the UN Human Rights Council. Third, scholars in business ethics and other disciplines increasingly include the complicity concept in their work (Clapham, 2006; Brenkert, 2009). Hence, the first two case objectives address issues in both practice and theory.

- To examine the increasingly political role of corporations
    - This objective takes note of the growing literature on corporate political responsibility, which, in contrast to the economic paradigms presented by traditional management theory, asserts that economic and political domains cannot be cleanly separated (Sundaram et al., 2004). Some of the most influential contributions regarding corporate political responsibility have been advanced by Matten and Crane (2005) and Scherer and Palazzo (2007). As explained by Matten and Crane (2005), multinational corporations are increasingly taking on tasks that were traditionally performed by national governments. Multinational corporations, for example, are engaging in fighting injustice, repression, corruption, and other adverse social conditions (Misangyi et al., 2008), advocating for peace (Fort et al., 2004), or promoting public health (Margolis et al., 2003). This recent stream of corporate social responsibility-related research is promising and can add insights to the case discussion.
- To analyze corporate challenges inherent in operating in or with oppressive regimes
    - This objective can be linked to classic ethical theories such as consequentialism and non-consequentialism. If we consider the discussion of complicity and due diligence, for instance, we can see parallels to non-

consequentialist theories such as Kantian duty ethics (duty to know, be informed, treat people as ends in themselves ….). At the same time, corporate challenges related to operating in or with oppressive regimes can be analyzed from a consequentialist standpoint: aiming to achieve the greatest good for the greatest number (utilitarianism). Other classic ethical theories such as virtue ethics can also be used to analyze the case. In this case, the focus might be on the decision maker (Beresford-Wylie). Applying different ethical theories may lead to different results (legitimization or delegitimization of the business transaction). This should foster considerable discussion among students.

*Teaching the case*

The case can be discussed in one class period lasting 60 to 90 minutes. It is suggested that students read and prepare the case prior to class. Students could be asked to prepare a short, two-to-three page reflection paper summarizing the case and responding to the questions. If students are required to send the paper to the instructor before class, the instructor can include submitted material during class discussion. A suggested class outline is provided below:

Introduction (10-15 minutes)

The instructor might begin the class by asking students what they know about the 2009 Iranian presidential election. This question launches the discussion and provides a review of some key facts about the election (events listed in Appendix A).

Group discussion (30 minutes)

Following this short introduction, the instructor could divide the class into several groups of four to six students each, depending on class size. Each group is then asked to discuss the case questions and select a spokesperson to summarize the group's answers and present them to

the class. This format allows the students to exchange ideas and discuss the questions in detail. The instructor might go from group to group, listening to the debates and answering any questions that arise.

Class discussion (30 minutes)

Coming together again as a class, the instructor could ask group spokespersons to respond to the case questions in order, with teammates/classmates assisting/commenting as per the instructor's preference. To facilitate the discussion, the instructor might summarize key points for each question on a whiteboard or blackboard as the students speak. This is especially useful for Question Four (moral arguments for and against the deal). Question Four and Question Five are the most provocative questions and considerable time should be allowed for their discussion. To stimulate the discussion, the instructor may want to cite phrases from student papers where appropriate.

After discussing responses to Question Five, the instructor may want to cite similar cases of alleged corporate complicity in human rights violations, such as Shell's Nigeria operations (Human Rights Watch, 1995), Google's market presence in China (Brenkert, 2009), or the Killer Coke case (www.killercoke.org). The instructor may want to consider this option in light of student background or experience with relevant courses. The following is a brief discussion of parallels between the NSN case, the Shell/Ogoni case, and the Killer Coke case.

Shell and the Ogoni Case

In the 1990s, the Ogoni people in Nigeria fought for greater control over the natural resources on their lands, leading to violent conflict between their community and national armed security forces (Amnesty International, 2005). Because Shell was operating in the Nigerian region at the time, and some of its facilities were protected by national security forces, it soon found itself confronted with demands to investigate its possible complicity with human rights

violations in the Delta region (Amnesty International, 2005). When some key Ogoni activists were arrested, international organizations called on Shell to use its power (corporate presence in Nigeria) to intervene.

Coca-Cola in Colombia (Killer Coke Case)

Over the last 15 years, local and international NGOs have reported extreme violence against union activists in Colombia. Coca-Cola and some of its bottlers have been accused of hiring paramilitary forces to torture (and kill) union activists in Colombia. In 2001, NGOs and relatives of some victims filed a lawsuit against Coca-Cola under the Alien Torts Claims Act. This action was dismissed in 2006.

Brief discussion

While the NSN case deals with the side effects of product consumption, the Shell and Coca-Cola cases deal instead with the side effects of production (conflicts with local communities and union rights). One interesting question to ask students might be whether corporations have more responsibility for the side effects of production or for the side effects of consumption. How far does corporate responsibility extend? Despite the slight difference (consumption versus production-related side effects) the three cases share a fundamental question: Is it legitimate to do business with or under an oppressive regime?

The Shell Ogoni case is similar to the NSN case: Shell was doing business with an oppressive regime and did not engage in human rights violations itself, but was accused of complicity in such violations. Moreover, Shell may not have conducted a sufficient geopolitical risk analysis before starting to operate in Nigeria (failing in its duty to be informed).

The Shell Ogoni case is particularly interesting because relatives of the executed activists filed a lawsuit under the Alien Torts Claims Act. This suit was settled in 2009. Coca-Cola was also sued under the Alien Torts Claims Act, but its case was dismissed in 2006. This raises a

question for NSN: Would a lawsuit under the Alien Torts Claims Act have led to a similar result? At the time the NSN case study was written, an Iranian activist was about to sue NSN (Nokia and Siemens) for complicity in his torture (Dehghan, 2010). How likely is it that a lawsuit against NSN (Nokia, Siemens) would be successful given the results of the Shell and Coca-Cola cases (one settled, one dismissed)?

Figure 1: Adbusting examples


Source (from left to right):
http://s3.causes.com/photos/RZ/Uf/HM/H1/x3/8T/Eh/0wJ.jpg
http://islamtxt.files.wordpress.com/2009/06/nokia_jailing_09_11.jpg
http://niacblog.files.wordpress.com/2009/08/nokia.jpg

**References**


Amnesty International. 2005. Nigeria: Ten years on: injustice and violence haunt the oil Delta. http://www.amnesty.org/en/library/asset/AFR44/022/2005/en/63b716d6-d49d-11dd-8a23-d58a49c0d652/afr440222005en.pdf. Accessed 23 December 2009).

Amnesty International: 2009, Iran. Election contested, repression compounded. http://www.amnesty.org/en/library/asset/MDE13/123/2009/en/1e69a8fb-dcf1-4165-a7fc-a94369e364bf/mde131232009en.pdf. Accessed 20 January 2010

Amnesty International: 2009, Iran's presidential election amid unrest and ongoing human rights violations. http://www.amnesty.org/en/news-and-updates/news/iran-presidential-election-amid-unrest-and-ongoing-human-rights-violations-20090605, Accessed 15 January 2010

BBC News: 2003, Iran steps up net censorship. http://news.bbc.co.uk/2/hi/technology/3019695.stm. Accessed 12 January 2010

BBC News: 2005a, 1979: Militants storm US embassy in Tehran. http://news.bbc.co.uk/onthisday/hi/dates/stories/november/4/newsid_3910000/3910627.stm. Accessed 15 January 2010

BBC News: 2005b, The Iran-Iraq war: 25 years on. http://news.bbc.co.uk/2/hi/4260420.stm. Accessed 15 January 2010

BBC News: 2009, Iran 'lifts block on SMS texting'. http://news.bbc.co.uk/2/hi/middle_east/8131095.stm. Access 15 January 2010

BBC News: n.d., Iran: Who holds the power? http://news.bbc.co.uk/2/shared/spl/hi/middle_east/03/iran_power/html/. Accessed 20 January 2010

Bharatbook: 2009, Analysis of 3G Mobile Market Potential in the Indian Telecom Market. http://www.prlog.org/10212661-bharatbookcom-analysis-of-3g-mobile-market-potential-in-the-indian-telecom-market.pdf. Accessed 17 January 2010

Brenkert, G. G.: 2009, 'Google, human rights, and moral compromise', *Journal of Business Ethics* 85 (4), 453-478.

Bozorgmehr, N.: 2009, Facebook sets tone in Iran's electoral contest. *Financial Times*, May 13. http://www.ft.com/cms/s/0/da46ad4e-3f19-11de-ae4f-00144feabdc0.html?nclick_check=1. Accessed 12 January 2010

Business Insights Ltd: 2008a, The Top Ten Telecom Service Providers. Positioning, performance and SWOT analyses.

Business Insights Ltd.: 2008b, The Top 10 Hardware Vendors. Positioning, performance and SWOT analyses.

Carter, T.: 2003, Castro regime jamming U.S. broadcasts into Iran. *Washington Times* http://www.washingtontimes.com/news/2003/jul/15/20030715-114937-2635r/. Accessed 10 January 2010

CBC News: 2009, History of Iran: From Persia to present. http://www.cbc.ca/world/story/2009/05/29/f-iran.html. Accessed 15 January 2010

Cellan-Jones, R. : 2009, Hi-tech helps Iranian monitoring. *BBC News*, http://news.bbc.co.uk/2/hi/technology/8112550.stm. Accessed 15 January 2010

Clapham, A. 2006. Human rights obligations of non-state actors. Oxford: Oxford University Press.

Committee to Protect Journalists: 2000, Spotlight on Press Tyrants: CPJ Names Ten Worst Enemies of the Press. http://cpj.org/reports/2000/05/enemies-00.php. Accessed 15 January 2010

Committee to Protect Journalists: 2009, Iran censors newspapers amid unrest. http://cpj.org/2009/06/iran-censors-newspapers-amid-unrest.php. Accessed 15 January 2010

Dehghan, S. K. (2010). Iranian activist sues telecoms firm over "spying system". The Guardian. http://www.guardian.co.uk/world/2010/aug/24/iranian-sues-nokia-siemens-networks. Accessed 24 September 2010

Feuilherade, P.: 2002, Iran's banned press turns to the net. *BBC News*, http://news.bbc.co.uk/2/hi/not_in_website/syndication/monitoring/media_reports/2183573.stm. Accessed 10 January 2010

Fort, T. L., & Schipani, C. A. 2004. The role of business in fostering peaceful societies. Cambridge: Cambridge University Press.

Gross, D.: 2009, Attacks, arrests slowing online news from Iran, http://www.cnn.com/2009/WORLD/meast/07/02/iran.information/index.html. Accessed 20 January 2010.

Hartmann, J., J. Hildebrand und P. Jürgens: 2009, Mobilfunk-Lieferung. Nokia Siemens soll Iran bei Zensur geholfen haben. *Welt Online*, http://www.welt.de/webwelt/article3975137/Nokia-Siemens-soll-Iran-bei-Zensur-geholfen-haben.html. Accessed 22 April 2010

Human Rights Watch: 1995, 'Nigeria, the Ogoni Crisis: a case study of military repression in Southeastern Nigeria' (New York).

Human Rights Watch: 2005, False freedom: Online censorship in the Middle East and Africa, http://www.hrw.org/en/reports/2005/11/14/false-freedom-0. Accessed 10 January 2010

Internet World Stats: Iran. http://www.internetworldstats.com/me/ir.htm. Accessed 10 January 2010

Kamali Dehghan, S.: 2009, Iranian consumers boycott Nokia for 'collaboration'. *The Guardian*, http://www.guardian.co.uk/world/2009/jul/14/nokia-boycott-iran-election-protests. Accessed 13 January 2010

Klein, N.: 2000, *No logo* (Picador, New York), pp. 279-309.

Lake, E.: 2009, Fed contractor, cell phone maker sold spy system to Iran. *The Washington Times*, http://www.washingtontimes.com/news/2009/apr/13/europe39s-telecoms-aid-with-spy-tech/print/. Accessed 20 January 2010

Mackey, B.: 2009, A green revolution for Iran? *The New York Times*, http://thelede.blogs.nytimes.com/2009/06/10/a-green-revolution-for-iran/. Accessed 10 January, 2010

Margolis, J. D., & Walsh, J. P. 2003. Misery Loves Companies: Rethinking Social Initiatives by Business. Administrative Science Quarterly, 48(2): 268-305.

Matten, D., & Crane, A. (2005). Corporate citizenship: toward an extended theoretical conceptualization. Academy of Management Review, 30(1), 166-179.

Misangyi, V. F., Weaver, G. R., & Elms, H. 2008. Ending corruption: The interplay among institutional logics, resources, and institutional entrepreneurs. Academy of Management Executive Review, 33(3): 750-770.

Nokia Homepage.: n.d., http://www.nokia.com. Accessed 22 April 2010

Nokia Siemens Networks Homepage: n.d., http://www.nokiasiemensnetworks.com. Accessed 10 March 2010

OpenNet Initiative: 2005, Country study: Internet Filtering in Iran in 2004-2005: A Country Study. http://opennet.net/sites/opennet.net/files/ONI_Country_Study_Iran.pdf. Accessed 10 January 2010

OpenNet Initiative: 2009, Internet Filtering in Iran. http://opennet.net/sites/opennet.net/files/ONI_Iran_2009.pdf. Accessed 10 January 2010

Proschofsky, A.: 2009, Iranische Internet Zensur: Powered by Nokia Siemens? *derStandard.at*, http://derstandard.at/1244461146648/Iranische-Internet-Zensur-Powered-by-Nokia-Siemens. Accessed 12 January 2010

Reporters Sans Frontières: 2004, Iran - Annual Report 2004. http://www.rsf.org/IMG/article_PDF/Iran-Annual-Report-2004.pdf. Accessed 10 January 2010

Reporters Sans Frontières: 2009, Internet enemies. http://www.rsf.org/IMG/pdf/Internet_enemies_2009_2_-3.pdf. Accessed 10 January 2010

Rhoads, C. and Chao, L.: 2009, Iran's Web Spying Aided By Western Technology. *The Wall Street Journal*, http://online.wsj.com/article/SB124562668777335653.html. Accessed 12 January, 2010

Rhoads, C.; Fowler, G. A. and Cummins, C.: 2009, Iran Cracks Down on Internet Use, Foreign Media. *The Wall Street Journal*, http://online.wsj.com/article/SB124519888117821213.html. Accessed 10 January 2010

Rooz, A.: 2008, The big companies blocking the internet in Iran. http://www.akhbar-rooz.com/news.jsp?essayId=16978. Accessed 12 January 2010.

Scherer, A. G., & Palazzo, G. (2007). Toward a political conception of corporate responsibility: business and society seen from a Habermasian perspective. Academy of Management Review, 32(4), 1096-1120.

Siemens Homepage: n.d., http://www.siemens.com. Accessed 12 January 2010

Sundaram, A. K., & Inkpen, A. C. 2004. The corporate objective revisited. Organization Science, 15: 350-363.

Taylor, K. M.: 2004, 'Thicker than blood: Holding Exxon Mobil liable for human rights violations committed abroad', Syracuse Journal of International Law and Commerce 31 (2), 274-297

Tomik, S.: 2009, Deutsch-finnische Überwachungshilfe. *FAZ NET*, http://www.faz.net/s/Rub868F8FFABF0341D8AFA05047D112D93F/Doc~E79B3BF

405841494AA53BA0C7235B6950~ATpl~Ecommon~Scontent.html. April 22. Accessed 20 April 2010

The Guardian: 2009, Iranian government blocks Facebook access. http://www.guardian.co.uk/world/2009/may/24/facebook-banned-iran. Accessed 12 January 2010

The Washington Post: 2009, Iran Elections: A Twitter Revolution? http://www.washingtonpost.com/wp-dyn/content/discussion/2009/06/17/DI2009061702232.html. Accessed 10 January 2010

Washington Times: 2009, Editorial: Iran's Twitter revolution. Witnessing a new chapter in the quest for freedom. http://www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution/. Accessed 10 January 2010

Weissenstein, M. and A. Johnson: 2009, 'Iranian Girl Shot: Neda Becomes Symbol Of Rebellion in Iran', *The Huffington Post*. http://www.huffingtonpost.com/2009/06/22/neda-becomes-symbol-of-re_n_218804.html. Accessed 24 April, 2010