CASE REPORT 1

Name:	Jenet Baribeau, Crissy Rogers, David Humphrey
Case Study:	Case 2.7 Veil of Censorship
Course:	CIS150-01
Date:	9/23/2012

Part 1: Ethical Dilemma

Websense specializes in content filtering software. The primary issue is whether Websense should supply the Saudi Arabian Government the Internet filtering software. Websense has a potential lucrative contract that the client, Saudi Arabia, would bring to their company. Websense has already begun a product trial with the government to censor the Internet country-wide. Websense is competing against the incumbent company, Secure Computing, as well as other filtering companies for the account. Does Websense contribute to the human rights violation in Saudi Arabia by providing the tools to prolong the government censorship? Or simply, does Websense merely have an obligation to create a product to be used by customers wherever and for whoever purchases the product? The case asks a simple question, "What should Websense do?"

Part 2: Role of IT

Specific technologies necessary to create a successful filtering system are various hardware, ISP connection, firewall, and filtering software. This would be rolled out through the capital Riyadh countrywide.

Part 3: Stakeholders

Critical Stakeholders of the ethical dilemma in "Veil of Censorship" include:

1. The Saudi Arabian People (who cannot access Web content that is deemed lawfully unacceptable): They have the right to fair treatment and security from their government.
2. The Saudi Arabian Government (who is, at the time of this case, actively soliciting bids from the software development industry for the contract to provide statewide content-filtering software): They have the right to expect the best possible product from whomever they award the content-filtering contract and to abide by their filtering requests.
3. Secure Computing (who currently has the contract with the Saudis, with their contract due to expire soon): They have the right to vie for contract renewal, and to be fairly evaluated for it.
4. Websense (who are competing with Secure Computing for the Saudi contract): They have the right to actively bid for the lucrative Saudi contract.

Part 4: Analysis of Possible Actions and Outcomes

1. *Do Nothing:* We have several paths that can be taken; for instance, we (that is, Websense) can say "No" to bidding (in effect, do nothing), in which case, presumably, Secure Computing re-secures the contract (or someone else entirely wins it.) By doing so, we remove ourselves from the equation, both teleologically and deontologically, and the status quo is preserved. There is no *direct* effect on any of the other stakeholders-- although, opportunities to ethically influence may have been lost. If we happened to make software that was superior to Secure Computing's, the Saudi government would face a less desirable outcome than if we *had* stayed in the bidding war for the Saudi contract. The people of Saudi Arabia are presumably not affected by the outcome of this decision, in that their access to Internet content will still be restricted by the government (although it may be now possible for a hacker to exploit the fact that the blocking system will be in a compromised condition as its being switched over). If we decide that being involved with what could be considered a political "hot potato" could cause damage to our own well-being, this may be the most rational choice available.
2. *Compete for the contact:* We could, alternatively, actively vie for the Saudi contract, providing the content-blocking tools in accordance with the specifications in the Saudi government's contract, enjoying the ensuing financial windfall. Secure Computing maintains that its transactions have always been entirely in good faith and that it is beyond their power if a customer chooses to use its technology to produce a harmful situation[9], and we could do exactly the same thing. The net result of this action is the continued restriction of the flow of information to the Saudi people, though it may now be possible for someone to exploit the content-blocking system while it's being switched over. But if this is the route we choose to go, we could very well become center-stage in a controversy and marginalized by our association with a government's attempt to keep its citizens powerless, regardless of what either our or the Saudi government's real intentions.
3. *Compete, but with ulterior motives:* We could also vie for the contract with subversive intentions--a possible example of which might be that they design the software to be circumvented easily by hackers by making known, through some avenue or another, that a

security breach in the code can be accessed. This would also, essentially, be ignoring the duty of a legal contract they have with the Saudi government, but perhaps fulfilling a social contract they perceive to have with the disadvantaged Saudi people. This would be exceptionally risky for us--if, somehow, this strategy were effective, some of this disadvantage might be transferred back to the Saudi government itself; but it also, in all likelihood, would spell the end of our business. By breaking an explicit contract with a client, we would broadcast to our market that we value our own idealism over trustworthiness.

4. *Expose the situation:* The last strategy for us might to act as a highly vocal, human rights advocate; exposing to the rest of the world the evil intentions of the Saudi Arabian government to solicit cutting-edge technologies from the world's best minds in order to strengthen the enterprise of suppression and prevent the erosive effect of outside influence on their base of power (if that is, indeed, how we happen to interpret their actions.) This could conceivably make the stigma associated with vending software to highly questionable regimes so undesirable that it would dissuade those prospecting this market from entering it; it would thereby prevent the Saudi government from (legally, at least) getting the tools they need to suppress their people. But is this what the people of Saudi Arabia want? It is very possibly not. So while we think we might be doing the right thing for the right reasons, are we doing it based on the right *facts*? After all, it is our business to provide tools like content-filtering software because *that is what we do as a business*--and so arguably it is our duty. Where do we draw the line for what we consider "unacceptable"?

Part 5: Deontological Perspective

From a deontological perspective, Websense should expose the situation and take action to affect change for Saudi Arabia and other countries in similar situations. Being an advocate, Websense should combine efforts from competing software filter companies to improve the Saudi people's human rights. They will take the necessary steps to create a universal law for the Internet. Technology they could use the social networks as platforms to initiate uprisings and the need for change. Ultimately, even if the outcry is unsuccessful, it would bring attention to

the injustices that run throughout the Middle East and more than 40 countries [12] that utilize the statewide filtering software to inhibit its people from free knowledge.

If Websense were to do nothing and maintain the status quo, they will affect no change. As IT professionals, it's their duty to perform and promote a fair Internet environment in addition to take the moral higher ground for the Saudi People, not necessarily their customer, the Saudi Arabian Government. Secure Computing wins the contract and everything stays status quo.

If Websense were to use the ruse of #3, it breaks all moral duties and obvious contracts. Websense provides the software with support but builds a backend to allow information through to the Saudi People. Websense would be ignoring their contract with the Saudi Arabian Government discrediting their corporation and perhaps even doing the Saudi people harm. If the Saudi Arabian Government is only filtering certain information that goes directly against their religion which is also their constitution[5] then Websense is violating Saudi Government laws as well as numbers 3 and 7 of W.D. Ross' Basic Moral Duties[2] distribute goods justly and avoid injury to others, respectively.

Part 6: Teleological Perspective

From a teleological perspective, Websense should take the action that creates the greatest net benefits for all the shareholders listed in Part 3. As such, Websense should take Action 2 with the modifications mentioned in Part 5, Websense should, however, create stipulations in the contract that prevent the Saudi Arabian Government from abusing the service. If a violation occurs, all service is stopped immediately. This has the highest likelihood of generating positive outcomes for Websense, Secure Computing, the Saudi Government, and the people of Saudi Arabia. However, the benefits to the many will far outweigh the costs to the few. The net result of this action is the contract would be secured and the Saudi's would get their content filtering software.

Option 1, do nothing, would not benefit anyone, other than the company who picks up the contract, except the Saudi people temporarily. Any competitor, such as Secure Computing, would pick up the contract from Saudi Arabia and continue in aiding the suppressive reign.

Websense would miss out on a lucrative contract, the Saudi's would still have their Internet content filtered through another company's software, and the Saudi Government would not be affected because they would get the software from someone else.

Option 3, to complete the contract with subversive intentions, would not benefit the shareholders listed in Part 3. I also would not be the ethically correct thing to do.

Option 4, Expose the situation, would bring unwanted negative attention from the Saudi Government. Teleologically speaking, this option is not the best route, because the Saudi Arabian people may agree with the limited availability of Internet access in accordance with their religious beliefs.

Part 7: My Recommendation

Websense should compete for the contract with true intentions as in #2 listed in Part 4 with both of the recommendations from the deontological and teleological perspectives.

In the U.S., we balk at the idea of our government attempting to control what information we can and cannot see and what of what could be considered the "individual rights" of each *human being*? Does every person on the planet have a right to free, unfiltered access to any information he or she wants? In the U.S., we consider the law of the land to be a human institution that exists to ensure that our freedoms remain intact. But those living in an Islamic culture do not make a distinction between legal framework and heavenly edicts; they believe their laws are of divine origin. Saudi Arabia, a monarchy and citizens of Muslim countries generally make no distinction between religion and state--their social, religious and legal frameworks are all unified [5]. In this context, it is difficult to define "suppression".

Islamic culture regards pornography as a serious threat to this well-being, and the Saudi people, for the most part, support the government's efforts to prevent its entrance into their daily lives. Saudi Internet-governance institution, The Information Security Center at King Abdul Aziz City for Science and Technology, the Saudi Arabian national science agency and research laboratory [8], maintains that its content-blocking procedures are largely the product of a consensus from the Saudi people, and that they strive to maintain as much flexibility as possible in their blacklisting policies [9].

With this background information on Saudi Arabia, the combination of actions is the only way to resolve this for all stakeholders. The Saudi people and government are using the filtering for a religious purpose. With no separation of church and state, any blacklist items would filter not necessarily the "Western" accessed information (CNN, BBC, etc.). Websense can give the government the best product necessary but keep provisos then periodically monitor the access. If the Saudi Government shows to be violating the agreement that moves towards suppression of the freedom of knowledge, then Websense terminates all services. Of course, Saudi Arabia can seek alternate services from competitors but if Websense is successful in banding together the competitors then they too will refuse service.

[1] Paul, Richard, and Linda Elder. *The Miniature Guide to Critical Thinking: Concepts and Tools*. 6th ed. Tomales, CA: Foundation for Critical Thinking, 2009. Print.

[2] Spinello, Richard. *Case Studies in Information Technology Ethics*. Second Edition ed. Upper Saddle River, New Jersey: Prentice Hall, 2003. 50-52. Print.

[3] Baase, Sara. *A Gift of Fire: Social, Legal and Ethical Issues for Computing and the Internet*. Third Edition ed. Upper Saddle River, NJ: Pearson Prentice Hall, 2008. 144-188. Print.

[4] Websense. "Websense Data Sheets." *Datasheets at Websense.com*. N.p., n.d. Web. 18 Sept. 2012. <http://www.Websense.com/content/Datasheets.aspx>.

[5] U.S. State Department. "Saudi Arabia." *U.S. Department of State*. U.S. Department of State, 25 Feb. 2004. Web. 20 Sept. 2012. <http://www.state.gov/j/drl/rls/hrrpt/2003/27937.htm>.

[6] Central Intelligence Agency, *The World Factbook*. 1st Public Ed. Washington, D.C. November, 2001

[7] "Crown Prince Abdullah's address to the United Nations" New York, United Nations, 6 September, 2000.
<http://www.saudinf.com/main/x007.htm>

[8] King Abdulaziz City for Science & Technology. "Internet Services Unit." KACST, 2012.
<https://www.kacst.edu.sa/en/services/pages/Internetservices.aspx>

[9] Lee, Jennifer. "TECHNOLOGY; Companies Compete to Provide Internet Veil for the Saudis." *The New York Times*. 19 November, 2001. New York, NY
<http://www.nytimes.com/2001/11/19/business/technology-companies-compete-to-provide-Internet-veil-for-the-saudis.html>

[10] Newman, Michael. "Websense statement on improper use of technology for suppression of rights and in violation of trade sanctions." Websense, Inc. 11 Nov., 2011.
<http://community.Websense.com/blogs/Websense-insights/archive/2011/11/01/Websense-statement-on-improper-use-of-technology-for-suppression-of-rights-and-in-violation-of-trade-sanctions.aspx>

[11] Shakespeare, William. *Hamlet* (The New Folger Library Shakespeare). Simon & Schuster; New Folger Edition, 2003.

[12] York, Jillian. "More than Half a Billion Internet Users Are Being Filtered Worldwide." *OpenNet Initiative*. N.p., 19 Jan. 2010. Web. 23 Sept. 2012.
<http://opennet.net/blog/2010/01/more-half-a-billion-Internet-users-are-being-filtered-worldwide>.