­­­­

Ethical, Legal, and Social Implications
Eddie S. Jackson
Kaplan University
IT599: Applied IT Master Project

Rhonda Chicone, Ph.D.
8/4/2015

**Ethical, Legal, and Social Implications**

**Ethical**
 This week’s part 2 assignment is to provide some information about the ethical, legal, and social ramifications of using Bitlocker (or any encryption solution for that matter) on company computers. Due to most company computers containing customer and company data, it would be highly unethical for that data not to be protected at all times. Thus, once Bitlocker has been installed on all computers, encryption compliance will be enforced by using the scripts created for LANDesk. While encrypting data seems like an obvious solution to a serious risk, i.e. unauthorized access to data recovered from stolen or lost hard drives, Bitlocker can be influenced by cultures in other countries. Because Company X employees do occasionally travel outside the country, it is imperative that all company personnel familiarize themselves with the international laws that govern encryption, as it specifically impacts how encryption may and may not be used outside the country. There will be scenarios where encryption must be temporarily disabled why traveling abroad.
**Legal**
 When it comes to encryption legislation on a global scale, numerous countries have laws *against* encryption, this would include having computers imported or exported with the recently implemented Bitlocker. For example, a short list of countries has been compiled with certain countries and what actions must be taken when encryption enters that country. These can be seen in the chart below (Brown University, 2015):

|  |  |
| --- | --- |
| **Country** | **Action** |
| Burma | A license is required |
| Belarus | Restricted initially until license is approved |
| China | A permit is required from the Beijing Office of State Encryption Administrative Bureau |
| Hungary | Has laws that foreigners must adhere to |
| Iran | Has laws that all people must adhere to |
| Israel | You can have encryption, but the password must be provided to officials |
| Morocco | Has strict laws against all encryption |
| Russia | A license is required |
| Saudi Arabia | Encryption is normally banned everywhere |
| Tunisia | Importing encryption is restricted |
| Ukraine | Has strict laws against all encryption |

Note, this is only a small portion of the actual list. To see more, the U.S. State Department’s website may be referenced. Additionally, the Electronic Code of Federal Regulations, or e-CFR, outlines laws and regulation surrounding encryption commodities, software and technology (U.S. Government Publishing Office, 2015).
**Social**
 The social implications of using encryption encompass three primary schools of thought: (1) encryption should be available to everyone, for any kind data that is deemed sensitive; (2) encryption can be employed, but the recovery passwords must be accessible by the government; and (3) no encryption is allowed. In the first approach to encryption, all sensitive, private data should be protected from unauthorized access, this would include encrypting data to protect it against offline attacks. It is important to clarify, even the local and federal government will not have access to view this particular type of encrypted data.
 In the second approach, sensitive, private data can be encrypted, however the local and national authorities must have access to view the content, and in most scenarios, special permits and official documentation must be acquired prior to implementing encryption. Why would this be necessary? Why would law enforcement and government officials need access to encrypted data? In some cases, criminals and terrorists use encryption to hide or secure their criminal activity. Likewise, encryption could be used to steal company data, or commit corporate and government espionage. It is understandable, if everyone is allowed full access and usage to encryption, the social implications could be severe in the hands of a criminal. If the government had the ability to regulate encryption, they could monitor it for criminal-like activity, thus preventing crime.
 The third outlook towards encryption is that encrypted data is a national or state security risk, and that it should be denied completely. As referenced in the legal aspects of encryption on a global scale, not all countries share the ideology that encryption is good, and as such, heavy restrictions may apply. In fact, numerous countries have laws *against* enabling any form of encryption on computers, this includes importing, exporting, and domestic forms of encryption.

 References

Brown University. (2015). Learn about BitLocker (encryption for Windows). Retrieved from http://www.brown.edu/information-technology/knowledge-base/article/1254

U.S. Government Publishing Office. (2015). Electronic Code of Federal Regulations. Retrieved from http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=f69a12e71396cdb0037d 905024c2eca2&rgn=div8&view=text&node=15:2.1.3.4.25.0.1.17&idno=15