**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 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 scripts from LANDesk. While encrypting data seems like an obvious solution to a serious risk, i.e. 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 international law, as it specifically relates to encryption. There will be scenarios where the encryption will need to 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; (2) encryption can be used, but the government must have access to it; 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. 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 evident, if everyone is allowed full access and usage to encryption, the social implications could be severe. If the government had the ability to view this secured data, they could monitor it for criminal-like activity, thus preventing crime.
 The third approach to encryption is to deny it completely. As referenced in the legal aspects of encryption on a global scale, not all countries share the ideology that encryption is a good thing, 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-based encryption.