This article is debating whether or not backdoors should be used in encryption software. Law enforcement is against encryption and they fear they are “losing access to vital evidence” (Price). They want tech companies to give them access to encrypted data in order to protect our country from threats, such as terrorism. On the other side, people think backdoors would be bad because of the risk of other people having access to the data, too. In the end, the Obama administration decided to not set limits on encryption.

In the lecture, Matt Hottell explained the history behind encryption. He showed specific examples for why companies need to encrypt data. One example was Amazon receiving credit card information form their customers. If the information were not encrypted, criminals would be able to steal their credit card information. He also explained how Public Key Encryption works. Each person has a public and private key that they use to encrypt and decrypt data (Hottell). This lecture connects with the article because they are both looking at the privacy of people and the level of access others have. If the law enforcement is able to decrypt data without using a key, then criminals will be able to decrypt it, too.

I thought the debate about the level of encryption is interesting. Authorities want to be able to access this data, but if they can, other people can, too. Encryption makes things more difficult for law enforcement, but it keeps people’s information more secure. I think it would be too risky to allow authorities access.
In the future, I think encryption is going to allow people to keep their information more secure. Encryption will help lower the risk and make users safer.

In the future, I think the government is going to spend more time and money on encryption. Terrorism threats are becoming more prevalent in this age. The government is going to want to know their plans in order to be able to prevent attacks. Also, the government is going to want to make their encryption software more secure.
