**Lecture 3. Public policies on surveillance and cryptography; introduction to cryptography**

Read for Lecture 4 (Debate #1):

1. Abelson, et. al. *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*. MIT-CSAIL-TR-2015-026 July 6, 2015, 31pp.

2. Vance, Cyrus. *Report Of The Manhattan District Attorney’s Office On Smartphone Encryption And Public Safety*, November 2015. pp. 1-23.

3. Landau, Susan. Making Sense of Snowden. *IEEE Security & Privacy Magazine, July/Aug. 2013*, pp. 66-75. [Although this article was motivated by the Snowden revelations, I’m including it because it provides a good history/background on the wiretapping and surveillance laws that I’ll present in Lecture 3, and it’s germane to the debate.]

All three articles are available on Canvas (Files/Debate Materials/Resolution 1.../All must read)

**Exercise:**

The resolution for this week’s debate is:

*Resolved: The U.S. government should mandate that communications and storage technology providers include a mechanism by which protected data can be obtained under lawful court order***.**

Pay close attention to the wording of the resolution. Note that the required reading papers are not specifically aimed at our resolution but they all address related topics. Study the papers and consider how they relate specifically to our resolution. Please be concise in your answers and provide references (page number) to specific locations in the papers that back up the view. Your answer to the first two questions should not be more than one page in all (and it can be shorter; it’s OK to state the arguments simply and list the references).

1. What are the two strongest arguments you found that would support the resolution?

2. What are the two strongest arguments you found that would oppose the resolution?

3. Formulate one question that you would pose to the side arguing in favor of the resolution:

4. Formulate one question that you would pose to the side arguing against the resolution: