Digital Surveillance

- Arguments for government surveillance:
  - Security: guard against criminals and terrorists. Pro-active security
  - Economical argument – saves money rather than in-person surveillance
  - Non-repudiation – hard evidence for supporting your case
  - Collects useful data e.g. for smart cities
  - Knowing you are under surveillance might make you behave better

- Arguments against government surveillance:
  - Legal today is not legal tomorrow – after the fact charging of a crime
  - Keeping surveillance restricted / narrow to a specific group
  - Can’t immediately react to something unfolding
  - Is there hard evidence that pro-active surveillance actually results in catching terrorists?
  - Invasion of privacy:
    - Makes you paranoid/uncomfortable
    - Could violate constitution rights
  - Whistleblowers don’t feel safe
  - Secret courts to allow surveillance
  - Potential for abuse: digital video can be taken out of context or synthetically generated, could be leaked

- Where do you draw the line? What are some guidelines to help regarding when too much surveillance occurs:
  - Having a well-defined scope to the surveillance: laws / rules about what to do if your surveillance catches something else
  - Governance of the surveillance process
  - Governance about the data collected
  - Laws to protect whistleblowers
  - Transparency in some sense: need to be access the information regarding why surveillance was performed, transparency about the process
o Who does the governance?
   ▪ An independent branch of the government (e.g. elected officials in the legislature)
   ▪ Maybe an independent agency outside the government (e.g. watchdogs)
     • Do they have any power? Public outreach, public opinion, lobbying
   ▪ Maybe an international agency to help with accountability

o Private surveillance of public places (e.g. self-driving cars)
   ▪ Lots of data being stored that could be useful to other parties
   ▪ Who is allowed to have access? How do you manage requests to access?
   ▪ Need to manage misuse/abuse
   ▪ Respond ethically, make sure the data is trustworthy