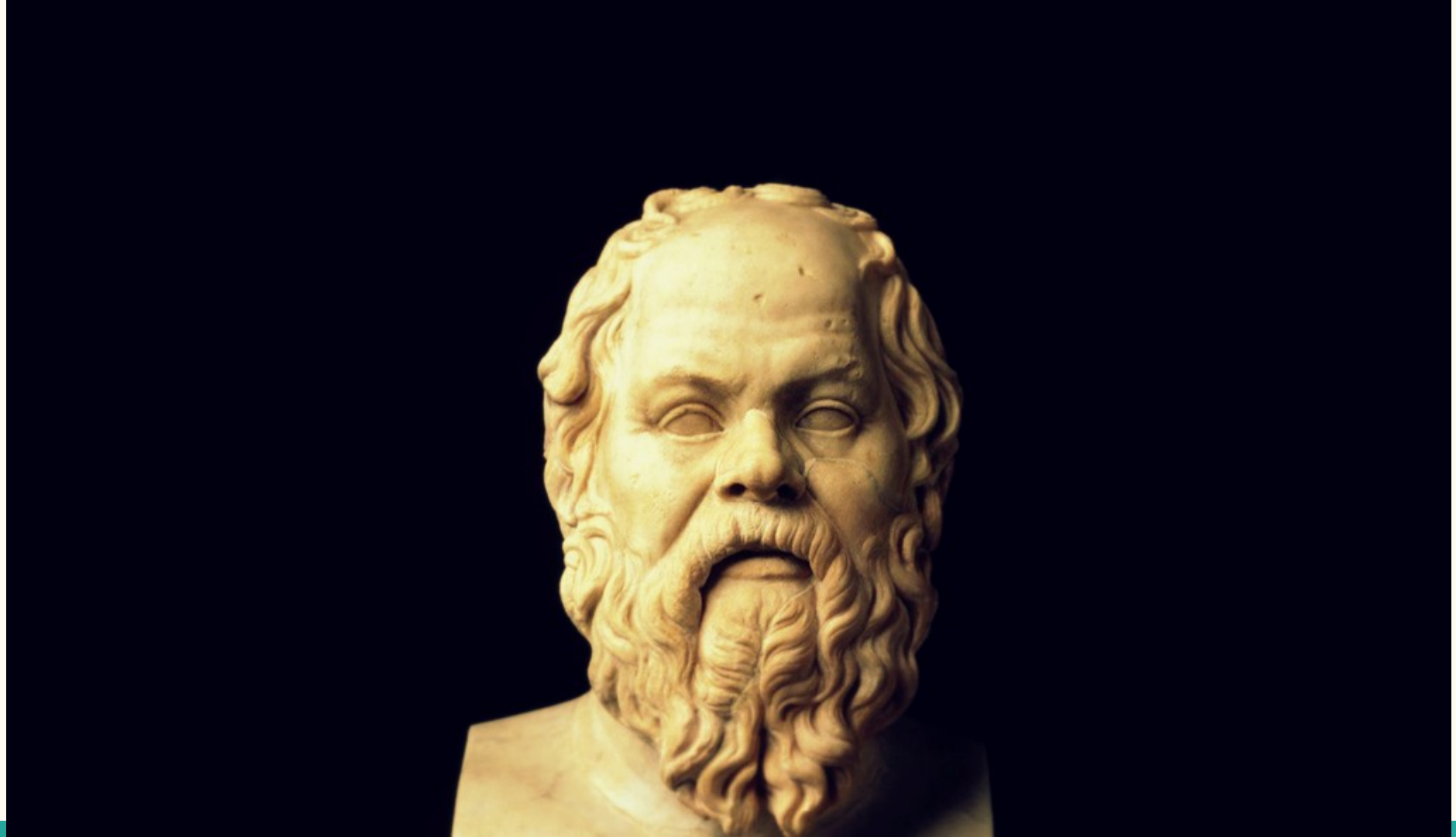
Modern Technologies and Conflicts

Information Technology and Society

2.10. 2019

Jakub Drmola

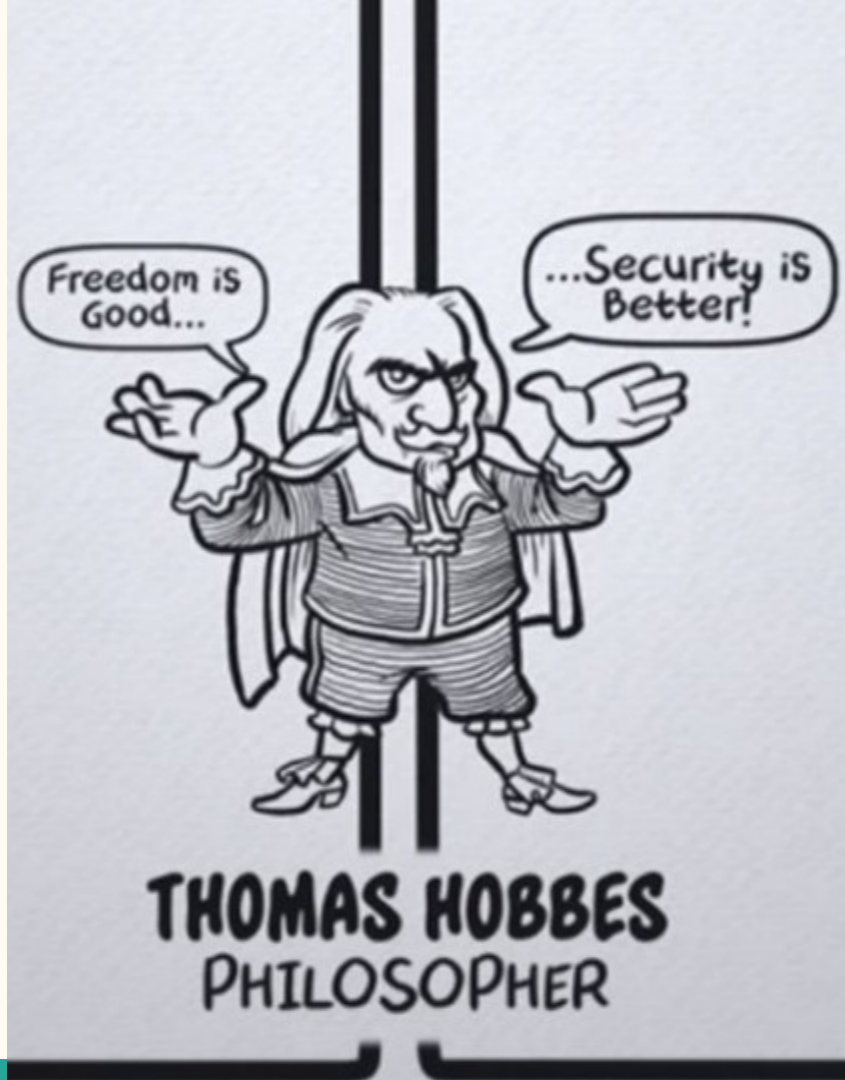


Freedom versus security

- or privacy versus security

- ongoing massive debate over this question in cyberspace

- no good solution in sight



Cybercrime

- anything from phishing, to ransomware, RATs and black market

- evolves with technology itself
- key role of anonymity
- lack of user awareness and good security practices

- less anonymity online would make it harder for perpetrators to get away with it

Piracy

- unauthorized distribution of intellectual property

- printing press > magnetic tapes > floppy discs > CDs/DVDs > internet > ???
- securitization (ethics, economy and hard security)
- lacking/slow adaptation of businesses

- stronger IP protection laws might serve as a deterrence

Hacktivism

- political and ideological activism in cyberspace, using direct hacking, DDoS, disclosing secrets, propaganda, doxing, defacements, etc.

- beginnings in 2008
- grows strong from 2010
- currently a well established *modus operandi*

- stricter laws and sentencing could discourage perpetrators

Organizing protests

- using social media to organize and coordinate protests, looting, riots, rallies etc.

- first seen in Iran 2009
- visible issue since 2011
- London riots, Arab spring, India, USA

- shutting off the service during the events would stop people from using it to self-organize

Terrorism online

- promotion of violence, extremism, intolerance, dissemination of guides, recruitment, inciting hatred and fear

- gradual development from 90s
- became major force in 2010s
- dominant issue with ISIS

- demands for stricter censorship by content curators

Privacy and corporations

- accumulation of personalized data for advertising and other purposes, interconnected platforms, ecosystems

- mainstream boom circa 2007-2012
- social networks of all sorts (facebook, twitter, ...)
- access to their service in exchange for private data

- is it a problem?
- or just a matter of personal choice and responsibility?

CNN
FAKE
NEWS

Surveillance

- metadata collection, intrusion into company systems, weakening of protections, dragnet collection

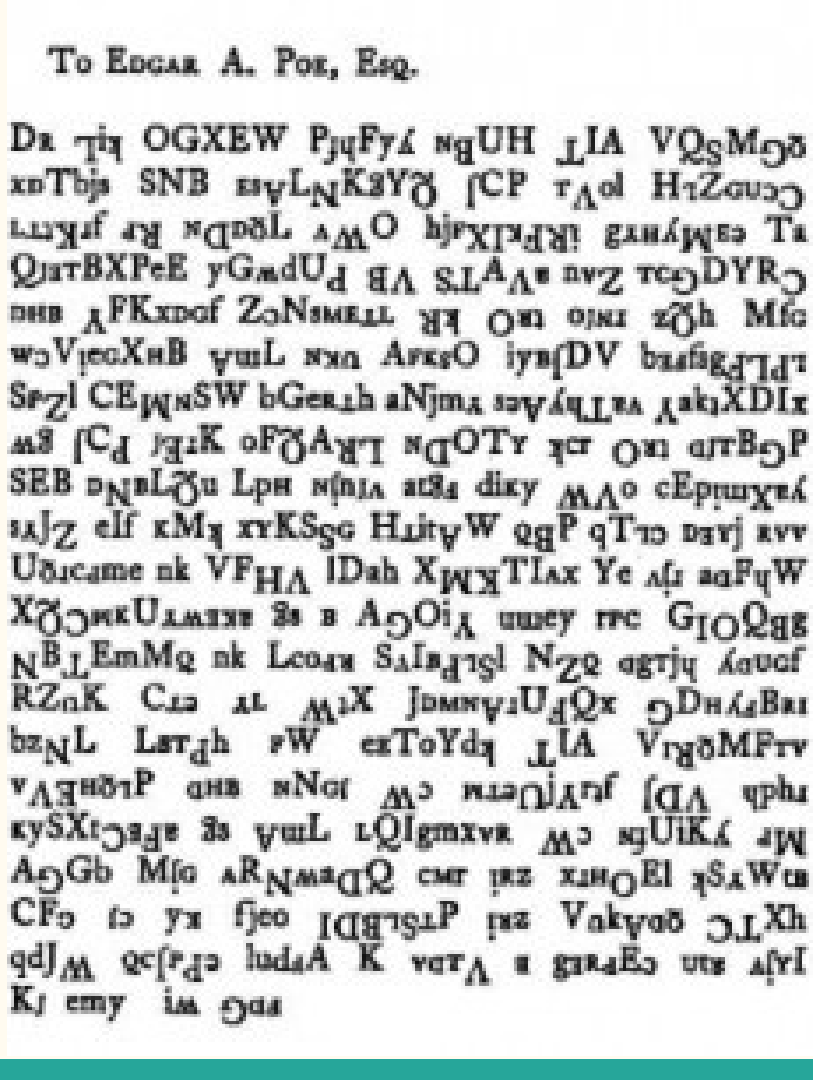
- roots in WW2 and Cold War, all in the name of security, many conspiracy theories
- Snowden and NSA PRISM reveal, 2013

- intensive and extensive data collection might serve to prevent security threats such as terrorism, etc.

Encryption

- runs through all the issues above, typical double-edged technology (TOR, crypto$)
- long history, today absolutely indispensable and ever-present
- ongoing fight for weak/strong encryption: states vs. corporations vs. people
- “catching terrorists, endangering users”
- case: San Bernardino iPhone

- “solved” by forcing backdoors and masterkeys



VR/AR

- very probable and very close proliferation of virtual/augmented reality technology in society

- entertainment, communication, traveling, education, training, therapy… anything else?

- health risk (nausea, injuries, eyesight?, psychology?)
- societal and security risks?