Workshop Week 3

Guiding Questions

- To what extent do you think individuals/consumers/citizens are being under surveillance - by who and why?
- When people protested the NSA's surveillance practices, the US government replied that they were "only collecting metadata". How did governments reportedly use metadata in the cases covered by four corners?
- Do you think surveillance is solely harmful or are there benefits related to governments' alleged mass surveillance of their citizens? Explain your opinion!

Facilitation

To prepare for facilitating a group discussion, consider the following for preparation:

- Who facilitate the discussion? Who knows the topic but can assume an 'objective' role? What do each group member know about the topic?
- Two students co-facilitating is viable, whereas more could be challenging. Ensure all roles are distributed and how the facilitation will take place. The main facilitator(s) should know their own beliefs before beginning as a facilitator.
- Identify the goal of the session. What are you trying to accomplish?
- Consider the format. Small or large group? Formal or informal session?
- Schedule tentative time blocks. Time management is important.
- Prepare interesting, challenging or controversial questions to keep discussion moving

Plan for materials beforehand. For your convenience, I have uploaded additional readings on the art of facilitating a group discussion.

Moderation Questions

- To what extent...
- Is surveillance inherently harmful?
- Would you give up your privacy? Would you be more willing if they actually tell you what they use?
- Is it worse than traditional intelligence?
- Should infosec and politics be evaluated hand in hand?
- People change their behaviors, but still operating to expose. People are too scared, they know that they're watched. Is that justifiable for the merits of surveillance?
-

Notes

- Go from the data
- The more terrorists, the more people will prefer security over privacy
- Every terror plot foiled used sophisticated equipment from arms producers

- Malware is easy to install if you let them physical access
    - To the point they can even know if they change their SIM cards
- Ahmed Mansoor: Dissident to the UAE government
    - "It's a violation of privacy to be watched"
    - Protesting against unfair trials and insulting nation's leadership, with his email hacked that he fell down for to phishing
    - UAE government was responsible
    - Charged after diclosing information
    - Crime was social media to share false and misleading information
    - UAE has powers to monitor private communications
    - Surveillance completely external, so impossible to detect
- James Lynch: AMnesty International
    - Implications of sending or providing sophisticated surveillance equiment are very serious
- Mass Surveillance is the new tool of external information extraction
- States begin with mass surveillance, with everyone being monitored, which is then used to identify key individuals.
- Denmark's new center of knoweldge economy, with companies specializing in surveillance, operated by BAE Systems
    - Nobody speaks to people, except former employees
    - "After a while I was allowed to go to the equipments. It can catalog and analyze communications, private and public."
    - And it can be through anything
- One tool: Evident
    - Pinpoint locations based on cellular data
    - Voice recognition, decryption
- We generate more data about ourselves and technology makes it easy for anyone to access
- Metadata identifies all information by providing context, and this is easily recorded.
- Nicholas Weaver
    - As an intelligence agency, I want to monitor everyday, and record everything until I know who I need to look for
    - Cybersurveillance technology is military weaponry
    - Whoever can pay can get access, but no one admits it
    - "It's creepy" - everything is captured because all that stuff is unencrypted
    - Even if something is never abused, it disturbs people
- It is possible to monitor an entire country's communications.
- It helps identify criminals and extremists - significant in counterterrorism efforts in the decade
- There's a mood along the public to move to security rather than privacy, recognizing as a tradeoff
- UK Mindef spends a lot of money to BAE
- UK government is considered world expert for cyber intelligence
    - But should they sell this too to everyone?
- Lasseskou
    - BAE is always the exporter
    - BAE needs a Danish license after getting Freedom of Information, and had objections
    - BAE sells this to Middle Eastern countries, and license spells out what they can do
    - BAE sells its products according to normal commercial imperatives

        - Including CSR...
    - Cyber and intelligence gives 1.8 billion pounds to the business
    - "We have policies that all exports are compliant with international export regulations and criteria to evaluate contracts"
- Tunisia's Dictating Overnthrown President (Bin Ali)
    - Installs the Evident system below his own house
    - ETI installed it, tool works by searching keywords and seeing everything they post anywhere
- You know that there's people at a protest, or people who has read a given article, and you go from there and build a profile of what they do
    - If somebody's really interesting, they can switch to attack
    - Teams work closely with Bin Ali
    - They'd ask info about specific people, I was told to change it, or to upload it, some information went to the president, most to the opponents.
    - Focused on all opposition
    - Ben Ali wants to know his enemies and allies
    - This ignited the Arab Spring, which made Middle Eastern governments find surveillance technologies
- Saudi Arabia's system
    - BAE sells equipment to Saudi Arabia
    - People change their behavior - "Smartphones have ears"
    - It's not easy since you're so connected to the internet, and you can't tell if they used any of your inputs
- Part of that grid of human rights and amnesty has left Saudi Area, and if they do open their mouth, they're very likely to be listened to
- There's a lot of fear - more than 90% of activists have now vanished. Things change and so does their belieffs. Some arrested, some silenced.
- No country monitors its own people the way the do in the Gulf, because they can afford the software.
- People now leave the country, in fear of what will happen if people have no freedom of expression
- Young people see the ideas as impossible dreams, and turn into violence because people who demand peaceful change is silenced.
- BAE's Arms Sales have always been controversial due to Saudi's human rights laws
- No export license is supposed to be granted if there is a strong chance that the sale will increase the likelihood of breaking international humanitarian law
- The British Government may be acting illegally in selling equipment to Saudis
- They also sold it to Oman. It's almost impossible to know if it's been used
- Nebhan al
    - It was an abduction
    - Two people abducted him from in a coffee shop and put him in solitary confinement
    - He was calling for the king to step down, and was labeled as terrorists by the government
    - He got asylum in London.
    - Some people I get in touch to gets incarcerated
- Omani Authorities watch private accounts
    - Nobody knew how we communicated
    - If I send something, no one should know
    - But the precautions were in vain, as all of them were picked up by the authorities

    - Anyone writing to him are called in.
    - Auhtorities jail and torture any information leaker
- They're doing bulk recording and email metadata
    - Moss sugestive evidence of mass surveillance
    - Once you get something of interest, it's about polling threats
    - What it is is starting with some piece of information and go from there
- Surveillance software can take data from operators easily
- Privacy International, London
    - Tapping in the Arab World is the biggest global trend
    - Surveillance will destroy people's confidence in expressing and sharing ideas, and trying to create a movement. Surveillance will be everywhere.
- Evident also does decryption/cryptoanalysis
    - Export of this is supposed to be tightly controlled
    - This has been sold to the Middle East
    - UK Export Authority were worried from the exports, but Danish authorities granted it anyway, even if it's against the laws
    - Refusing due to Criteria 5 (national security and allies - country can use the country to get access to Britain's own comms)
- Ross Anderson
    - Once you sell the kit, they can do whatever they want
    - Suppose they have embassies in foreign countries, what's to stop them to put the equipment there and use it to decipher all comms overseas?
    - If you allow the Middle Easterners to get it, they have the power to track international comms, too
- It's a trade off. None of these countries have the same ethical moral code as Britain, so every country has some form of compromise on how those tools will be used.
- Even if the UK has export controls, they're still dubbed "case-by-case", taking all relevant factors including human rights considerations
- Marietje Schaake
    - If anyone is silenced or imprisoned due to EU made technologies, it's unacceptable
    - The fact that these companies are commercial players, and can have a deep impact on national security, requires us to look again with the restrictions before it turns against our own interest.
- They've met a dozen people from BAE and the govenrment, only one talks out
    - There's loopholes taken advantage by companies
    - Ultimately you have no control on how they can be sold and used

---

- politics and mass surveillance - argue from other side? - internal/commission?
- tradeoff between police officers - vulnerable data
    - take into account the failure rates