Privatlivs Fred

Hvorfor privatliv er væsentligt – et eksempel fra det virkelige liv

Sippo Rossi and Irfan Kanat

25/04/2021

Vi har i de tidligere moduler gennemgået hvordan individer og virksomheder kan spore personer online. Der findes dog en tredje mulighed, nemlig regeringer og dermed indirekte offentlige instanser. Materialets fokus flyttes nu fra stalking (individuel) og sporing (virksomheder) til overvågning (regeringer).

Målgruppe og Undervisningsmål

Studerende på ungdomsuddannelserne og yngre voksne er de primære målgrupper for denne case, men essensen er relevant for alle internetbrugere.

Hensigten med casen er at illustrere hvordan regeringer, og mere specifikt efterretningstjenester, indsamler data om borgere ved brug af både lovlige såvel som ulovlige metoder. Emnet bliver gennemgået således de studerende bliver opmærksom på, at deres data og internetaktiviteter aldrig kan garanteres at være helt private, da både inden- og udenlandske efterretningstjenester er blevet afsløret i indsamling af store mængder data om helt almindelige borgere. Dette tjener som incitament for de studerende til gøre sig tanker om samt diskuterer klassiske dilemmaer relateret til masseovervågning, og om "målet helligere midlet".

Tiltænkt Undervisningsform

Vi anbefaler følgende tilgangsvinkel til undervisningen: Først introduceres de studerende til temaet via den tilhørende videolektion og / eller underviser giver en forelæsning. Derefter læser de studerende artiklen i Læseøvelse 1, og gennemgår indholdet med medstuderende og underviser. De studerende opfordres til aktiv deltagelse i diskussioner, og til at reflekterer over de etiske overvejelser og implikationer introduceret af casen. Herefter, bør de studerende læse artiklen i Læseøvelse 2, hvor casen foregår i Danmark, med efterfølgende diskussion og refleksion.

Casen

Baggrundsinformation Part 1

Statsovervågning er en realitet og eksisterer i forskellig grad i ethvert land. Omfanget af borgerovervågning kan bruges som test for et lands demokratiske standarter. Ofte ses en højere grad af overvågning i lande med stigende autoritarisme, som eksempelvis Østtyskland, Kina og USA.

Et godt eksempel er Snowden afsløringerne (2013). Hvor Edward Snowden lækkede en guldgrube NSA, en amerikansk sikkerhedstjeneste, dokumenter, der afslørede omfanget af NSAs spionage. Det var chokerende; for det første, at alle amerikanske telefonselskaber delte opkaldslister, hvem ringede til hvem og hvornår, med NSA. Millioner af amerikanske borgeres private informationer var delt via

hemmelige retskendelser. Disse retskendelser var meget omfangsrige, og tillod NSA at indsamle informationer fra tusindvis af urelaterede borgere for enhver udenlandsk mistænkt person, de var interesseret i. Det har særdeles stor betydning, fordi normalt kræver overvågning af amerikanske statsborgere meget mere kompleks lovhjemmel. For det andet, kunne NSA tiltvinge sig adgang til amerikanske firmaers registreringsdata via overvågningsprogrammet PRISM. Google, Apple, Facebook etc. Alle disse firmaer delte information med NSA og var i den forbindelse pålagt tavshedspligt. For det tredje, gav XKeyscore programmet NSA adgang til overvågning af din onlineaktivitet. Disse informationer inkluderer browser historik, søgninger, emails, chats og forskellige typer metadata. NSA træningsmateriale beskrev programmet som dækkende "næsten alt en typisk bruger benytter internettet til". Mest chokerende var dog, at programmet ikke var afhængig af en forudgående godkendelse. NSA kunne få adgang til informationerne, uden rets- eller dommerkendelse. For det fjerde, forsøgte NSA at underminere kryptering. For det femte, krævede PRISM kun minimal lovhjemmel. Hvis ikke NSA kunne opnå den ønskede adgang via PRISM, benyttede de deres software backdoors, og havde derved direkte adgang til de amerikanske tech-giganters datacentre.

Læseøvelse 1

Læs følgende artikel fra 2014: https://www.bbc.com/news/world-us-canada-23123964

Her tages en pause med klassediskussion. Forsæt kun efter alle relaterede klasseaktiviteter er afsluttede.

Emner

- Onlineovervågning
- Parløb mellem regeringer og virksomheder

Læring

- Nationale efterretningstjenester har adgang til næsten alt data

Spørgsmål for Diskussion

1. Findes der legitime årsager til en regering ønsker overvågning af egne borgere?
2. Er der en signifikant forskel mellem masseovervågning og specifik overvågning? Er én mulighed mere legitim end den anden? Med specifik menes in denne sammenhæng, at en eller flere borgere, der overvåges, er individuelt identificeret, i stedet for eksempelvis indsamling af alt datatrafik for et område.
3. Burde borgere kunne forvente at deres regering respekterer deres privatliv?
4. Breve og telegrammer er beskyttet mod regeringsovervågning uden retskendelse. Kan du forvente denne beskyttelse automatisk er gældende for dine e-mails og tekstbeskeder?

5. Hvordan med de tilfælde hvor sikkerhedssamarbejdsaftaler mellem din regering og fremmede regeringer kan kompromittere dit privatliv? Kan du forvente, at din regering beskytter dit privatliv mod fremmede regeringer og efterretningstjenester?

Baggrundsinformation Part 2

Snowden afslørede omfanget af den amerikanske regerings formåen, men overvågning og magtmisbrug af overvågning er ikke et unikt amerikansk fænomen. Danskere kan forvente at regeringen respekterer borgernes privatliv, da paragraf 72 i den danske grundlov og tilknyttede love sikre privatlivets fred. Alligevel har Danmark haft sin andel af overvågningsmæssige faux pas. Siden 2014, er Forsvarets Efterretningstjeneste (FE) næsten hvert eneste år blevet afsløret i ulovligt samarbejde med NSA. Alligevel synes disse afsløringer ikke føre til ændringer. Efterretningstjenester der lovmæssigt er forhindret i at overtræde deres egne borgeres privatliv, benytter hinanden til overvågning og aflytning af hinandens borgere, og deler informationerne i de sager der kræver de mest ekstreme lovovertrædelser.

Det er åbenlyst, at det er problematisk at efterretningstjenester ulovligt indsamler informationer om deres borgere. Hvilket tydeliggør et klassisk dilemma. Hvis borgere ikke har noget at skjule, er der så nogen grund til at være bekymret over regeringsovervågning?

Nyttige overvejelser for diskussionen.

- Hvad du betragter som en basal rettighed i dag, kan blive ulovliggjort i morgen.
- Kan du stole på at din regering altid tager dit parti?
- De juridiske rammer tilpasses samfundet. Hvad vi tidligere betragtede som ulovligt, bliver nu hurtig normalt, eksempelvis interracialt ægteskab, samme køn forhold og marihuana. Hvis ikke borgere har frihed til udforskning af de juridiske grænser, vil lovbestemmelserne være endegyldige og aldrig udvikle sig, og mange ændringer, der generelt betragtes som favorable, vil aldrig være blevet realiserede.
- Online overvågning er markant mere gennemgribende end tidligere tiders overvågning. Det formodes at den Østtyske regering havde en meddeler / spion ansat for hver seks borgere. Med det nuværende teknologiske niveau, bærer vi alle rundt på vores egen lille spion i vores lommer, og automatiske algoritmer overvåger vores adfærd kontinuerligt. Med denne totalovervågning, kan samfundet være låst i stasis.
- Nødvendigheden for balance mellem sikkerhed og privatliv er indiskutabel, men har vi hidtil kompromitteret privatlivets fred for let øget sikkerhed?

Læseøvelse 2

Læs følgende artikel fra 2020. Forsæt først efter du har afsluttet Læseøvelse 1 og de tilhørende klasseaktiviteter: https://www.reuters.com/article/us-denmark-defence-idUSKBN25O1XP

Emner

- Overvågning I Danmark

Læring

- Danmark er ikke isoleret fra resten af verden når det handler om privatlivs fred og fremmede magters overvågning.

Hvordan ageres hensigtsmæssigt

- Deltag aktivt i samfundet og stem på politikere der deler din synspunkter vedrørende privatliv.

Spørgsmål for Diskussion

1. Hvordan forholder du dig til informationerne der beskriver samarbejdet mellem danske og udenlandske efterretningstjenester?
2. Hvad tænker du om følgende udsagn ” men hvis borgere ikke har noget at skjule, er der så nogen grund til at bekymre sig om regeringsovervågning”?
3. Er det rimeligt at kompromittere en hel befolknings private beskeder og informationer, hvis det eksempelvis
    - forhindrer et terrorangreb om året?
    - forhindrer 10 terrorangreb om året?
    - reducerer organiseret kriminalitet med 5%?

Bemærk! De ovenstående værdier er fiktive. Pointen er at få de studerende til at evaluere acceptable fordele og ulemper.

4. Hvilke potentielt negative konsekvenser ser du ved at en regering, national eller fremmed, har adgang til alle dine personoplysninger?