

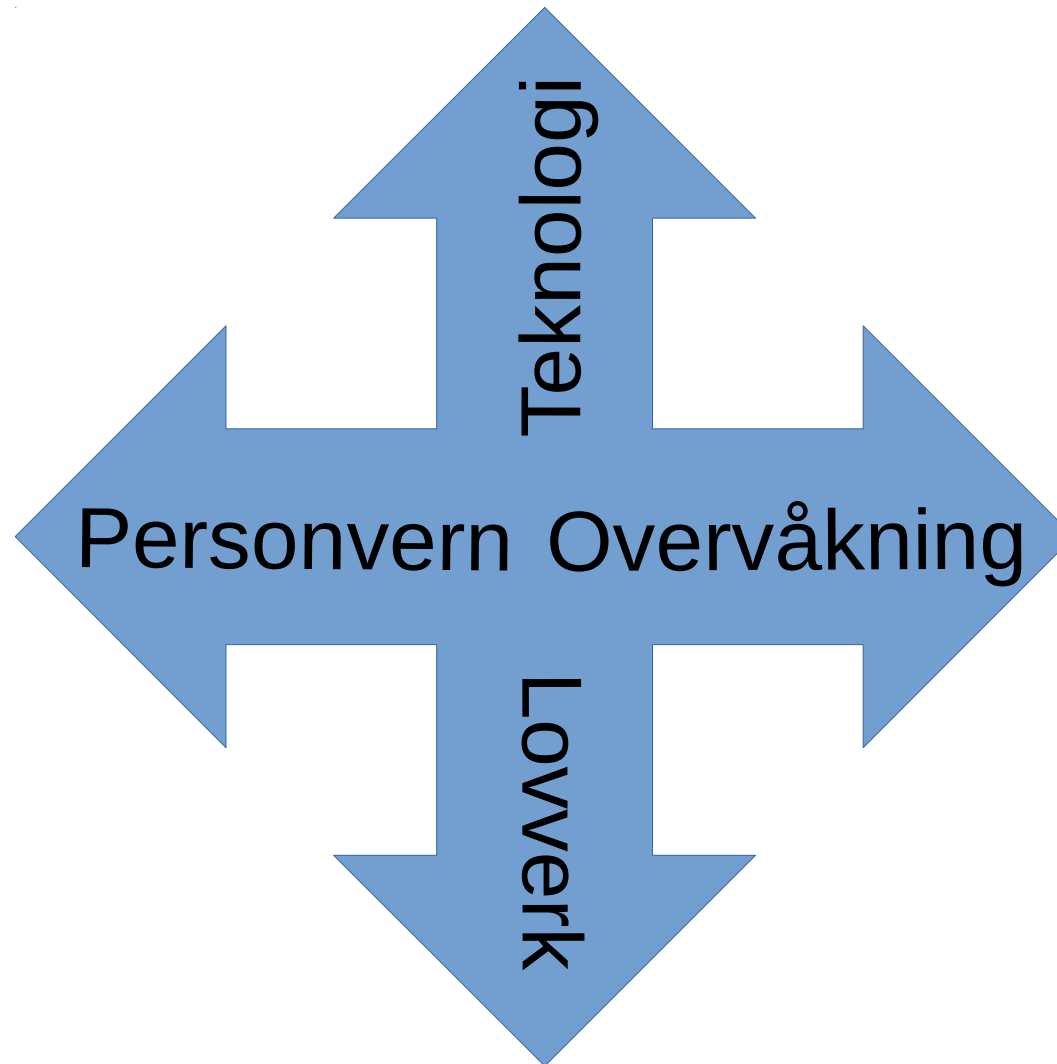
***Nettskyen: Nok tåkelegging,
mer klarhet Takk!***

thomas.sodring@hioa.no

Men først

I.A.N.A.I.L

Multidimensjonal debatt



Bakteppet

- Snowden lekkasjene og uklarheter om hvorvidt de store teknologigigantene har samarbeidet med NSA om masseovervåkning
- En media som ikke har evnen til å forklare hva dette egentlig handler om
 - Mangler dybde i rapporteringen
- Et ekstremt stort og voksende etjeneste i USA som samler inn store mengder data om folk
- For å gjenreise tillit har gigantene gått hardt ut mot amerikanske myndigheters forsøk på å få tilgang til data

Bakteppet

- Det er problematisk at sikkerhetsmyndighetene snakker et språk som kun de forstår
 - Begrep som «å samle inn», «tilgang», «overvåke», «kommunikasjon» har andre definisjoner enn det vi er vant til
- Hvis du ikke er amerikansk statsborger så har du ingen rettigheter i forhold til hva NSA gjør med data om deg
- **Foreign Intelligence Surveillance Court** ^[1]
 - «Hemmelig» domstol som ga NSA fundamentet til å utvikle sin overvåkningsprogram

Bakteppet

- NSA brukte sine kapasiteter til å overvåke under klimamøte i København 2009
- Yahoo prøvde å unngå å bli dratt inn i PRISM-programmet til NSA [2]
 - Ble truet med dagsbøter på \$250 000
- Eiereren av LavaBit epost-tjenesten valgte å legge ned tjenesten etter at han ble pålagt å gi fra seg krypteringsnøkler
 - Han fikk en vanskelig behandling og ble satt under mye press

Etter Snowden?

- Verizon Wireless la til (super) sporingsdata i TCP-pakker [3]
- Noen amerikanske ISPer strippet bort en viktig del av metadata tilknyttet til eposter som da begrenset mulighetene for kryptering [4]
- *Never attribute to malice that which is adequately explained by stupidity*

Safe Harbour

- *Safe Harbour* regulerte hvordan virksomheter kunne overføre personopplysninger fra EU til virksomheter i USA
 - Ble kjent ugyldig
- Bli erstattet av *Privacy Shield* med amerikanske forpliktelser mot masseovervåkning av europeiske innbyggere
 - Hvordan defineres masseovervåkning?
 - Flere som mener at denne avtalen kjøper EU/USA mer forhandlingstid

A right to privacy

- Retten til å holde noe hemmelig
 - Fra en leverandør
 - Banken, Teleselskapet, Nettsky-leverandør
 - Fra myndighetene
 - Skatteetaten, Tollvesenet, Politiet
 - Det vi gjør på offentlig sted (Internett)
- Skille mellom metadata og innhold

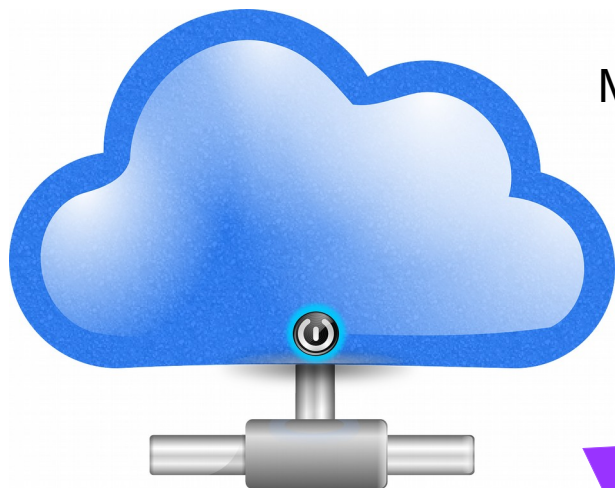
Det er bare metadata!

- De vet at du ringte en telefonsex-linje og at du snakket i 22 minutter
 - Men de vet ikke hva du snakket om
- De vet at du ringte en krisetelefon fra et område som er et kjent sted der folk begår selvmord
 - Men de vet ikke hva du snakket om
- De vet at du ringte sjekk-punkt (HIV-testing)
 - Men de vet ikke hva du snakket om
- De vet at du ringte en lege og senere ringte en abortklinikk
 - Men de vet ikke hva du snakket om

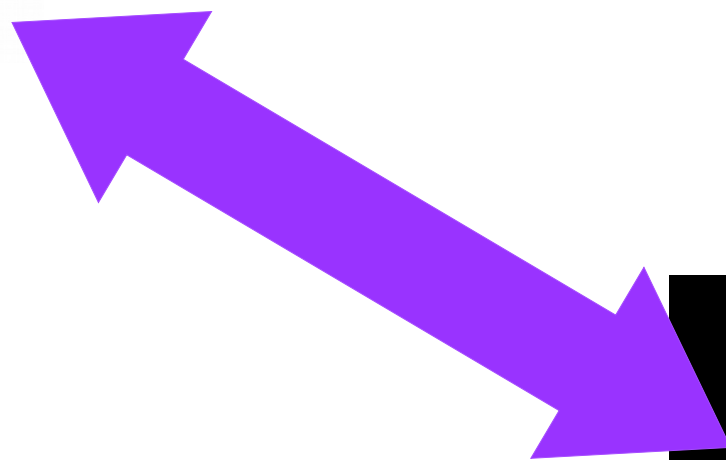
A right to privacy

- Skille mellom hva jeg som privatperson velger å gjøre og det forvaltningen velger å gjøre
- Fra myndighetenes perspektiv er det et viktig prinsipp at
 - You have no legitimate expectation of privacy in information you voluntarily turn over to third parties
- I et massesøksmål mot Google i 2013, valgte faktisk Google å bruke dette^[5] som et viktig argument – *og de vant*

Hvor er debatten?



Microsoft epost på en server i Dublin



Apple dekryptering av en terrorists telefon

MS epost-saken

- Amerikanske myndigheter vil ha tilgang til en epost til en hotmail bruker som lagret på en server som MS eier i Dublin
- Amerikanske lover gjelder ikke i EU
 - Tenk om russiske myndigheter krevde å få utlevert informasjon fra en server i Seattle
 - Det er ikke våre data, men kundens
- Det handler om *tilgang* ikke *lokasjon* eller *eierskap*
 - Krigen mot [***insert straw man***] er global
 - Du kan ikke lagre data i en annen jurisdiksjon for å hindre etterforskning

MS epost-saken

- Denne saken må nok helt opp til Supreme Court før det avgjøres
 - Hvis MS taper her så må de velge om de skal bryte europeisk lov eller amerikansk lov
 - Vil dette da brukes av NSA i FISC for å kreve full tilgang til datasentrene i Europa?
- MS har sagt at de skal lansere en ny type datasenter i Europa
 - MS eier datasenteret men et annet selskap drifter tilgang til informasjon
 - Stoler ikke MS på seg selv med tilgang til kundenes data?

Apple iPhone-saken

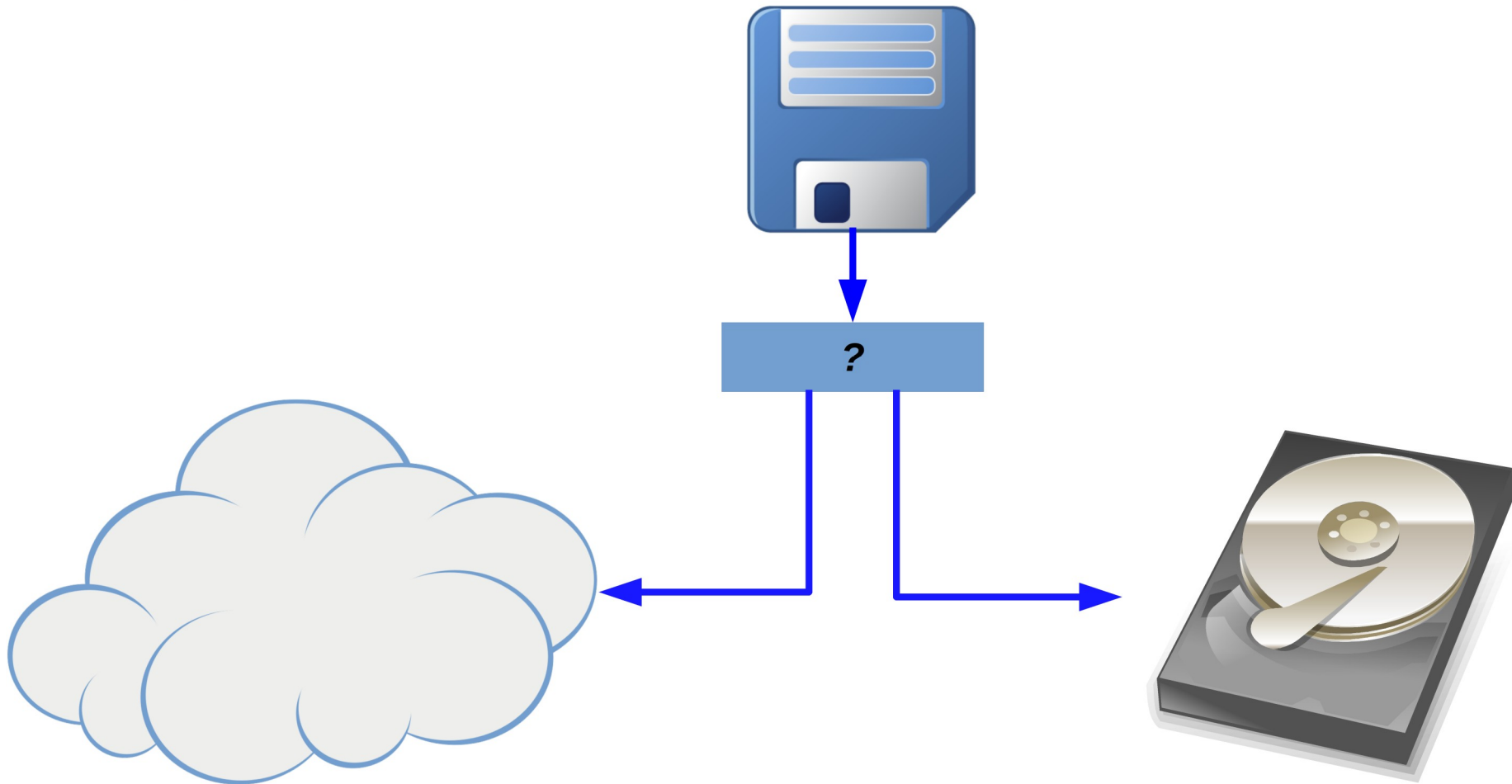
- Snowden lærte oss at masseovervåkning var for billig og flere teknologiselskaper introduserte kryptering for å beskytte kundenes data
- San Bernardino-terroristen hadde en Apple iPhone (jobbtelefon) som FBI ønsket tilgang til
- FBI prøvde å tvinge Apple til å hjelpe dem å dekryptere telefonen
- Selve scenarioet var jo egentlig rimelig
 - Avgrenset til en telefon og en gang
- Det hele ble redusert til en prinsipiell sak som egentlig handlet om fastsette en presedens

Apple iPhone-saken

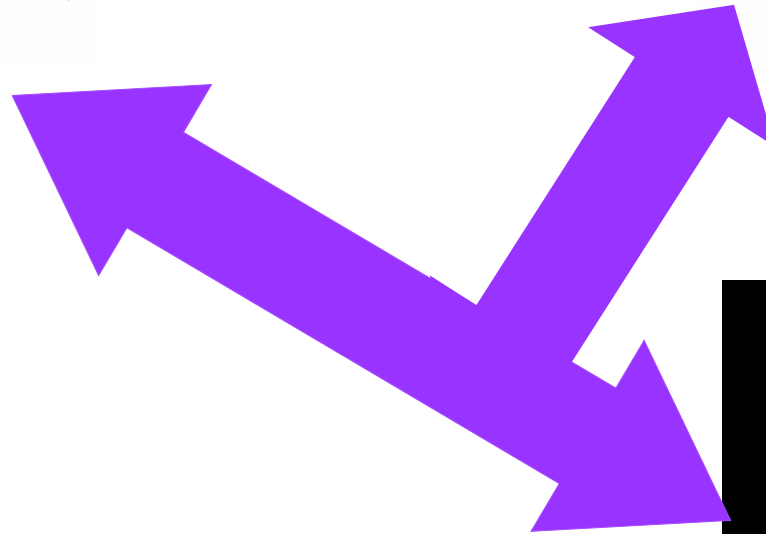
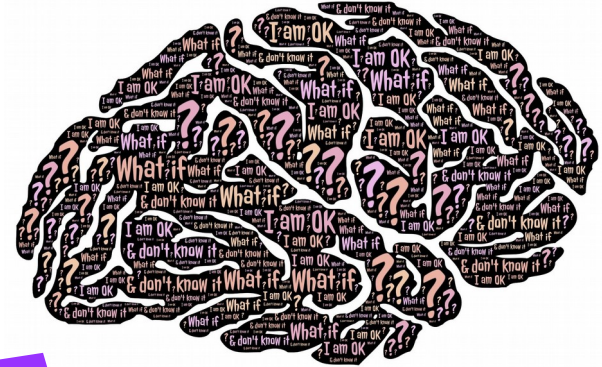
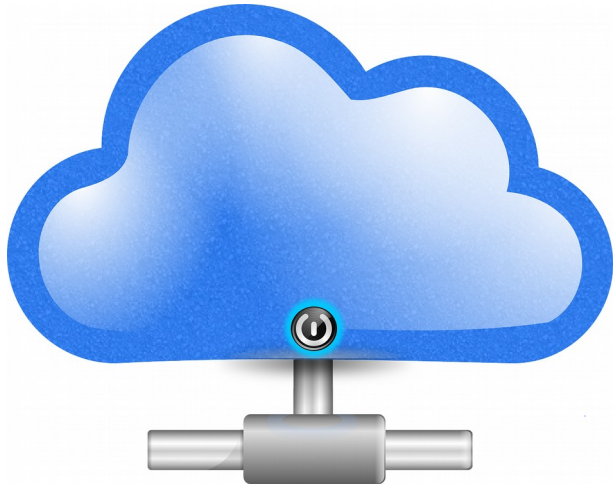
- Når denne oppdateringen eventuelt var laget så var det usikkert om den kunne holdes hemmelig
- FBI fant en annen måte å knekke krypteringen på
 - Dette er alt blitt brukt flere ganger av politiet rundt omkring i USA
- En annen dimensjon er at Apple ble veldig sta fordi forespørselen var offentlig kjent
 - De ønsket at det skulle være hemmelig [6]

Å lagre i nettskyen

- Hvis jeg lagrer noe til nettskyen har jeg mistet en *right to privacy*?
- Ingen har turt å ta tak i det enda [7]



Hvor går debatten nå?



Nettskyen som teknologisk ideologi

- Nettskyen er en teknologisk ideologi om hvordan mennesker samhandler med data
 - Vi kan ikke la selskaper underlagt hemmelig tolkning av lovgivning og hemmelige domsavsigelser misbruke arkivets data
- Støtt initiativene om flere nettskyer basert på fri programvare og åpne standarder
 - Ikke lukket plattformer som oppfører seg som skadevare
- **Dere** velger om dataene deres skal være underlagt amerikansk lovgivning

OPINIONS ON INTERNET PRIVACY

THE PHILOSOPHER:

"PRIVACY" IS AN IMPRACTICAL WAY TO THINK ABOUT DATA IN A DIGITAL WORLD SO UNLIKE THE ONE IN WHICH OUR SOCI-

SO BORED.



THE CRYPTO NUT:

MY DATA IS SAFE BEHIND SIX LAYERS OF SYMMETRIC AND PUBLIC-KEY ALGORITHMS.

WHAT DATA IS IT?

MOSTLY ME EMAILING WITH PEOPLE ABOUT CRYPTOGRAPHY.



THE CONSPIRACIST:

THESE LEAKS ARE JUST THE TIP OF THE ICEBERG. THERE'S A WAREHOUSE IN UTAH WHERE THE NSA HAS THE ENTIRE ICEBERG.

I DON'T KNOW HOW THEY GOT IT THERE.



THE NIHILIST:

JOKE'S ON THEM, GATHERING ALL THIS DATA ON ME AS IF ANYTHING I DO MEANS ANYTHING.



THE EXHIBITIONIST:

MMMM, I SURE HOPE THE NSA ISN'T WATCHING ME BITE INTO THESE JUICY STRAWBERRIES!!

OOPS, I DRIPPED SOME ON MY SHIRT! BETTER TAKE IT OFF.

GOOGLE, ARE YOU THERE?

GOOGLE, THIS LOTION FEELS SOOOO GOOD.



THE SAGE:

I DON'T KNOW OR CARE WHAT DATA ANYONE HAS ABOUT ME.

DATA IS IMAGINARY. THIS BURRITO IS REAL.



Referanser

- [1] <https://www.eff.org/deeplinks/2013/06/president-obama-called-fisa-court-transparent-despite-it-being-shrouded-secretcy>
- [2] <http://www.wired.com/2014/09/feds-yahoo-fine-prism/>
- [3] <https://www.eff.org/deeplinks/2014/11/verizon-x-uidh>
- [4] <https://www.eff.org/deeplinks/2014/11/starttls-downgrade-attacks>
- [5] <http://www.yalelawjournal.org/forum/rileys-implications-in-the-cloud>
- [6] http://www.nytimes.com/2016/02/19/technology/how-tim-cook-became-a-bulwark-for-digital-privacy.html?_r=0