DIGITALT SELVFORSVAR

TAG KONTROL OVER DINE DATA OG DIT DIGITALE LIV

DIGITALT SELVFORSVAR – Tag kontrol over dine data og dit digitale liv
7. Edition, 1. printing. 2020

Book layout: Spintype.com
Cover design: Paws Fabrik
Printed by: AKAPRINT A/S
Published with: Spintype.com
Editor: Pernille Tranberg
Co-author: Pernille Tranberg
Co-author: Luise Søe

CONTENTS

CHAPTER 1

HVAD ER PRIVACY

Hvad kan dine lærere, forældre, venner og arbejdsgivere se om dig, når de søger dit navn på nettet? Og, hvordan kan du forhindre virksomheder og andre i at overvåge din digitale adfærd, profilere dig og lave forudsigelser om dig? Dvs. bruge data om dig til at skabe værdi for andre f.eks. virksomheder og ikke nødvendigvis for dig. Det at have kontrol over egne data er definitionen på digitalt privatliv:

> Retten til selv at bestemme, hvem der ved hvad om dig hvonår

Der er mange gode grunde til at have eller tage kontrol over sine personlige data.

1. Den første er dit 'digitale CV' – altså det man finder om dig, når man søger på dit navn. Det skal du sørge for så vidt muligt selv at styre. Så du ved, hvad der kommer frem i en Google søgning på dit navn.
2. En anden god grund er at du kan slippe for målrettede priser, reklamer og politiske budskaber fra folk og firmaer, som du gerne vil være foruden.
3. Den trejde er, at du så kan undgå kun at få serveret indhold, som er målrettet dig ud fra dine digitale fodspor. Da der er en risiko for, at du ender i en filter-boble, og ikke bliver udfordret med ny og overraskende viden.

Dette er din guide til at tage nogenlunde kontrol over dine egne data og passe på dig selv i den digitale verden.

I den perfekte verden havde vi alle kontrol over alle vores egne data. Guiden fremstiller det ideelle, så tag den som en inspiration og et skridt ad gangen. Vi forsøger at guide dig ved hjælp af de mest brugervenlige værktøjer, uden at vi dermed siger, at værktøjerne er perfekte. Det er der ikke noget, der er. Så tag det som nogle tips til værktøjer, der forsøger at beskytte dit privatliv.

Der er masser af gode etisk ansvarlige måder at bruge data på. Desværre er de bare ikke så udbredte endnu. Og dette hæftes fokus er individuel beskyttelse og kontrol.

Teknologien går hurtigt, så denne guide bliver opdateret med hver udgave og findes digitalt på **DataEthics.eu/selvforsvar**

CHAPTER 2

SØGNING

HVORDAN KAN JEG SØGE PÅ NETTET UDEN AT DATA OM MIG GEMMES?

Alt, hvad du søger på, når du bruger søgemaskiner som Google, Bing og Yahoo trackes og gemmes om dig til senere brug. Måske du søger på emner, du ikke ønsker at dele med andre. F.eks. om hvordan det er at være teenager, at kroppen ændrer sig, eller hvordan det er at få sin første kæreste. Men generelt er det bedst at bruge private søgemaskiner. Her kan du søge hemmeligt dvs. uden at data gemmes om dig og dine interesser.

Liste over nogle af de private søgemaskiner er:

- **Metager.de/en** (tysk)
- **Startpage.com** (hollandsk)
- **Qwant.com** (fransk/tysk)
- **Mojeek.com** (britisk)
- **Duckduckgo.com** (amerikansk)'
- **Swisscows.ch** (schweizisk)

Der er forskel på en søgemaskine og en browser. En browser er det værktøj, der hjælper dig ud på nettet. Du kan bruge alle slags søgemaskiner på den samme browser og du kan også installere en fast søgemaskine i browseren, som starter, når du åbner browseren. Google betaler sig til at være fast standard søgemaskine i mange browsere og er det også i sin egen browser, Chrome. Så når du bruger Chrome, Firefox og Safari så kan du selv installere en ny søgemaskine, hvis du ikke vil bruge Google og have alle dine data gemt. I Firefox går du ind under

'indstillinger', 'søgemaskine', 'find flere søgemaskiner' og tilføj fx Startpage som du så kan sætte som standardsøgemaskine i stedet for Google. I Safari skal du også ind under 'indstillinger' men her kan du kun vælge 'DuckDuckGo' i stedet for Google. Alternativt kan du gå ind på startpage.com, scolle ned og klikke på 'gør Startpage til standardsøgemaskine' i alle de browsere, du vælger at bruge.

CHAPTER 3

BLOKERINGSVÆRKTØJER

HVORDAN FORHINDRER JEG, AT ANDRE FÅR VIDEN OM MIG, JEG IKKE ØNSKER?

Du kan forhindre andre i at følge dig i din adfærd på nettet og indsamle viden om, hvad du interesserer dig for og evt har af problemer, ved at installere nogle værktøjer – kaldet udvidelser – i din browser.

De *kan* give dig problemer med visse tjenester som fx din bank, men så må du have en ren browser til det. Det er godt at bruge flere browsere, da det spreder dine digitale fodspor. Blokeringsværktøjerne blokerer typisk ikke for

førsteparts-cookies, der er et stykke kode, som husker passwords eller indhold i indkøbskurven, og de deler *ikke* data om dig med andre. Værktøjerne blokerer for *tredjepart-cookies* eller *marketing-cookies*, der deler dine data med alt og alle.

Gode værktøjer, der forhindre at andre (fx. firmaer) får data om dig:

- **Disconnect.me/disconnect** er rigtig god til din computer. Med den installeret, kan du stadig se reklamer (og støtter dermed fx nyhedssider, der lever af det). Det, Disconnect gør, er at den blokerer for marketing-cookies.
- **uBlock.org** til Chrome, Safari og Firefox er en god cookie-blocker, der også blokerer for reklamer.
- Appen **AdblockPlus** er bedst til dine mobile enheder. Den blokerer både for

reklamer og marketing-cookies. Slås til og fra med et enkelt touch på skærmen.

- **Ghostery.com** blokerer cookies og malware (ondsindet programkode) og kan bruges både som plugin til browser på computere eller som browser på dine mobile enheder. Den er blevet købt af den tyske browser Cliqz, som kan anbefales, da den beskytter dine data som standardindstilling – altså pr default.

CHAPTER 4

SIKRE CHAT APPS

HVORDAN KAN JEG KOMMUNIKERE MED ANDRE, UDEN AT NOGEN LYTTER MED?

Facebook Messenger, WhatsApp og lignende er ikke sikre kommunikationsværktøjer. Enten lytter de med på det, du skriver eller gemmer og bruger metadata; hvem du skriver med, hvor længe, hvorfra og hvornår.

Heldigvis findes der andre chat fora, som ikke lytter med eller samler data til at profilere dig. Det kræver lidt en indsats, at få dinner venner eller kollegaer med, men, så er du sikker på, at du ikke aflyttes, og at du har private samtaler:

- **Wire**.com (tysk/schweizisk) som er finansieret af bl.a. Janus Friis, der medgrundlagde Skype.
- **Signal** (US) er også god – omend ikke så brugervenlig og lækker som Wire.
- Der er mange andre, fx **Telegram** (russisk), **Threema** (tysk) og **Riot.im** (UK og open source)

CHAPTER 5

VPN

HVORDAN KAN DU PASSE PÅ DIG SELV, VED AT LADE SOM OM DU ER PÅ EN ANDEN LOKATION?

Et VPN-værktøj krypterer (sikrer) trafikken mellem dig og det, du laver på nettet. Er som en slags vejbom på den digitale landevej. F.eks. når du går på et gratis og åbent wifi, der ofte er på hoteller og cafeer, så kan du med en VPN sikre, at ingen kan hacke dig og suge alle dine data ud af din gadget.

Med en VPN-tjeneste kan du også bestemme og kontrollere din lokation – altså hvor i verden

du ønsker at befinde dig digitalt. Websites og apps indsamler lokation til blandt andet at give dig skræddersyede tilbud og priser, så med VPN kan du opnå bedre priser fx ved at lade som om du er i Tyskland, hvor priserne er billigere. Med en VPN kan du også se dansk tv, når du er i udlandet.

En VPN-tjeneste, du kan stole på, koster penge (men så betaler du heller ikke med dine data). Men med den norske **Opera-browser** kan du begynde at lege med VPN. Den giver dig gratis adgang til at hoppe på servere i tre forskellige kontinenter. Download browseren på opera.com, og gå ind i indstillingerne under 'beskyttelse af personlige,' scroll lidt ned. Her kan du aktivere VPN, så kan du lade som om, du er i en anden region.

Fif: Du kan altid se, din IP-adresse på Whatismyipaddress.com.

Når du vil købe en VPN-tjeneste vælg en, der har hovedsæde i Europa og tjek hvilke lande, de har servere i. Rejser du meget i Italien og vil se DR, så skal tjenesten have en server i Danmark. Her blot nogle bud;

- **IBVPN.com** (rumænsk) mange servere
- **Earthvpn.com** (cypriotisk) - mange servere
- **F-secure.com** (finsk)
- **Ipredator.se** (svensk)

CHAPTER 6

SIKKER CLOUD

HVORDAN SIKRER JEG, AT MINE DATA OPBEVARES SIKKERT

Hvor vores data før i tiden altid blev opbevaret på egne servere i kælderrum (og stadig bliver hos en del, da det anses for mest sikkert), er der firmaer, som har specialiseret sig i, at opbevare vores data centralt på 'cloud-tjenester' - i skyen så at sige.

Brug sikre cloud-tjenester fremfor de meget populære, ofte 'gratis' tjenester som Dropbox, Google Drive eller OneDrive. Apples Icloud er efter alt at dømme sikker, fordi Apple er seriøs

omkring privacy. Men her nogle af dem, som du i hvert fald kan have tillid til:

- **Tresorit** (schweizisk)
- **Seafile** (tysk)
- **Nextcloud** (open source, oprindeligt tysk – gratis, ubegrænset, minder om Dropbox)
- **Cozy** (fransk)
- **Sync** (canadisk)

CHAPTER 7

SELF-TRACKING

Selftracking betyder, at man måler sig selv på forskellige områder indenfor især sundhed og ernæring. Man indsamler, måler og fortolker sine data ved hjælp af række app's og gadgets. Den mest kendte er nok løbe- og gå-app, der måler dine skridt. Men der findes fx også en app, som fortæller, hvor bilen står parkeret, og løbehjulene i storbyerne er også et eksempel på selftracking.

Du skal være opmærksom på datapolitikken på dine selftracking apps. De er blevet bedre gennem årene, bl.a. fordi det norske forbrugerråd

har været efter dem. Men her er i hvert fald to sikre self-tracking apps.

- Withings (fransk)
- **Apple Smartwatch** (amerikansk)

De største apps, der lader dig tracke din fertilitet og dermed styre din graviditet, er amerikanske og reguleret efter forbrugerlovgivningen dvs ikke så stramt som sundhedsdata i hænderne på læger og forsikringsselskaber. Derfor anbefales denne;

- **Clue** på helloclue.com (tysk) men sign ikke op med din Facebook account

CHAPTER 8

FAKENAMEGENERATOR

HVORFOR KAN DET VÆRE EN GOD IDÉ AT BRUGE ALIAS = DÆKNAVN PÅ NETTET?

Hvis du ønsker at bruge Facebook, Instagram, SnapChat YouTube eller Tiktok til noget, der ikke har med dit skolearbejde eller faglighed at gøre, så overvej at bruge et andet navn end dit eget. Derved kan du holde dit rigtige navn 'rent', indtil du skal opbygge en professionel identitet. Det vil sige - når du er ude på arbejdsmarkedet eller skal fremstå seriøs. Brug kun Facebook og Instagram i eget navn, hvis det er til dit professionelle virke. Brug aldrig Facebook til det, du opfatter som privat – heller ikke i et

andet navn, da det at bruge et andet navn kun giver en lav grad af sikkerhed. Med et andet navn, er det dog sværere for arbejdsgivere, uddannelsesinstitutioner, eks-kærester, identitetstyve og andre at finde dig.

Brug også et alias, når du downloader rapporter, apps, spil osv., hvor de beder om dit navn, adresse, email o.lign. medmindre du har fuld tillid til servicen, eller skal betale med kreditkort og derfor skal bruge dit eget navn.

> Brug dit rigtige navn på services, du har tillid til - herunder din skoles og andre offentlige tjenester - og når du optræder seriøst og professionelt.

Fif: Find aliaser på fakenamegenerator.com.

Husk ikke at stjæle andres navne eller lade som om, du er en anden – det er kriminelt. Dem, du

chatter med i et dæknavn, skal vide, hvem du er. Det handler ikke om at snyde andre mennesker, men om at passe på dig selv og dine data. Når du bruger et alias, skal du huske at tilknytte en alias-email til det. Der kan du bruge nogle af de gratis emailtjenester til, fx Gmail og Hotmail, som du så ikke behøver at tjekke regelmæssigt.

CHAPTER 9

BESKYT DIN EMAIL

Der er masser af gratis email-services, men de færreste er private. Det er en betalings-emailkonto som regel. Disse email konti er tit knyttet op via din families teleselskab, et webhotel eller fx services som;

- **Protonmail** (schweizisk)
- **Mailbox** (tysk)
- **Countermail** (svensk)

De går alle op i at beskytte dine data og tracker dig ikke på samme måde, som de fleste og mest udbredte gratis email-services gør.

CHAPTER 10

BRUG FLERE BROWSERE

HVORDAN SPREDER DU DINE DIGITALE FODSPOR?

Det er godt at bruge flere browsere for at sprede dine digitale fodspor. **Firefox** og **Safari** er blandt de mest kendte og benyttede browsere. De er også de bedste. Firefox, fordi der er så mange gode plug-ins (udvidelser), som beskytter dine data. Safari, Apples browser, er god, fordi den helt automatisk blokerer for tredjepart-cookies, så viden om dig ikke bliver delt med alt og alle. Det gør Firefox også. Derudover er følgende gode:

- **Cliqz.com** (tysk) anonymiserer alle de data, der måtte blive opsamlet om dig og sikrer dermed, at du er anonym, når du bruger den. Den har egen søgemaskine men leder over til Google Search ved svar, som den ikke selv har, så her bør du installere en privat søgemaskine (gå i 'preferences' og 'search' og vælg fx Startpage, Qwant eller DuckDuckGo)
- **Brave.com** (amerikansk) blokerer automatisk for tracking og er hurtig.
- **TOR browseren, torproject.org** er den absolut mest private, fordi den også skjuler din ip-adresse, men den kan godt være langsom. Bedst til computer. Ikke særlig god til mobil (hvor den hedder Onion).

CHAPTER 11

SOCIALE MEDIER

HVORDAN KAN JEG STYRE DATA OM MIG PÅ SOME?

De kendte sociale medier er offentlige platforme. Dvs alt hvad du laver der, kan andre end dig selv få adgang til. Nogle påstår, at du kan være privat derinde ved at sætte 'privatlivsindstillinger,' eller at billeder forsvinder. Det betyder, at du måske kan kontrollere dit sociale liv – altså hvem der umiddelbart kan se dine opdateringer, men det sociale medie selv har typisk fuld adgang til alt. Og hvis en af dine venner deler en opdatering, tager et screendump eller tagger dig på sin offentlige væg, så er din

kontrol væk. Derfor; tænk altid før du poster; ville jeg sige dette til 100.000 youtubere, i TV-Avisen eller til X-faktor finalen? Husk, at det du poster, bliver gemt i mange år.

Overvej at operere med flere identiteter på sociale medier. Du behøver ikke bruge dit eget navn. Gem dit rigtige navn til du er klar til dit første job og kan begynde at opbygge en professionel identitet. Læs mere om det under 'FakeNameGenerator' og 'Professionel identitet'.

Grunden til, at du skal være påpasselig med at dele oplysninger, er, at sociale medier bruges af data-købmænd (*data brokers*) og andre til at høste data, kategorisere mennesker og sælge data videre i form af fx lister over dem, der har været ramt af kræft eller fædre til børn, der er døde i bilulykker.

De færreste forstår 'privatlivs-instillingerne' på Facebook, SnapChat, Instagram eller Tiktok. Derfor her et par tips til i hvert fald Facebook:

Facebook-indstillinger:

- Som minimum bør du slå den funktion til på Facebook, der gør, at du skal godkende, hvis nogen tagger dig, før det ryger ud på din væg. Det finder du under *Indstillinger/Settings* og *Timeline/ Tagging* - nederst under *Review/ gennemgang*.
- Under *Privatliv/Privacy* kan du sige nej til, at søgemaskiner kan finde din Facebook-profil samt sikre, at det kun er dig, der kan se din vennekreds (da den er offentlig som udgangspunkt og siger mere om dig, end du tror).
- Hvis du orker, er det en god ide at *slette sine likes*. Desværre kan man ikke bare

gøre det i et hug (det er især likes Facebook tjener penge på) men skal gøre det en for en.
- Hvis du vil slette dig fra Facebook er her et link: https://www.facebook.com/help/delete_account.

Du har selv et ansvar for en del af den data, der er om dig på nettet: Derfor bør du nøje overveje, når du deler dine informationer. Her er en liste over ting vi anbefaler, at du ikke deler:

- **Helbredsoplysninger** (heller ikke, at du, din bror eller din ven er blevet helbredt for kræft) og selvfølgelig ikke dit cpr-nummer. Ja, helst ikke din fødselsdato, da det er guf for identitets-tyve verden over.
- **Rejseplaner** før og under rejsen. Hvis du vil dele feriefotos, så gør det efter ferien. Der er smarte tyve derude, og

det samme er forsikringsselskaberne. Du ville jo heller ikke skrive ikke på din hoveddør, hvis du ikke er hjemme.

- **Løbe- og cykelruter** (så man kan se, hvor du bor).
- **Billeder af børn** (de skal selv have lov til at kontrollere deres data, når de bliver store nok) - herunder dine mindre søskende.
- **Negative tanker om andre**. Skriv ikke noget, du ikke kan sige til person ansigt til ansigt. Brok, sladder, mobning om andre er noget din kommende arbejdsgivere vil kunne fremsøger og ikke ønsker.
- **Nøgenbilleder, drukbilleder** eller andre kompromitterende billeder af dig selv og andre. Det er ulovligt at dele nøgenbilleder af folk uden deres samtykke.

- **Religiøse, politiske og seksuelle holdninger** - husk det, når du deltager i debatter med politikere på Facebook.
- **Risikoadfærd,** der kan skade dit omdømme i forhold til bl.a. banker og forsikringsselskaber, fx hvis du er vild med sorte løjper.
- **Din lokation**, hvor du opholder dig og hvor du bor . Også på Snapchat, hvor du i dag kan se, hvor alle dine venner er, hvis de har sagt ja til at dele deres lokation med Snapchat.

Alternative sociale medier

- **Mastodon**
- **Diaspora**
- **Minds**
- **Ello**

Fif: Prøv at få dine venner med over på sociale medier, som giver dig kontrol over dine data. Hvis I alle - eller en gruppe af jer - flytter samtidigt, er det jo ligemeget hvor I kommunikerer.

CHAPTER 12

APPS & INDSTILLINGER

HVORFOR SKAL DU SIKRE DINE INDSTILLINGER PÅ DINE APPS?

Vær varsom når du downloader apps til din smartphone (og undgå så vidt muligt Facebook apps), hvad enten det er spil, quizzer, karriere-apps eller programmer. Tjek først hvilke data, de vil have af dig. Og spørg dig selv, om tjenesten er dine data værd. Brug din sunde fornuft!

Det ér svært at vurdere prisen på dine data, men nogle apps beder om adgang til din kalender, dine kontakter, din indbakke og din mikrofon, uden at det er nødvendigt. Måske er der et

alternativ, der ikke beder om så meget? En vækkeur-app behøver vel ikke kende din lokation? Det gør din løbe-app, så det måske er ok, så længe du stoler på virksomheden, der står bag appen.

Du bør gennemgå dine indstillinger på din smartphone (på iphone; 'anonymitet'). Hvilke apps har adgang til hvilke data. Ofte har mange apps adgang til din mikrofon og lokation og kan dermed lytte med på det, du taler med andre om, eller følge din fysiske færden. Måske skulle du slå apps' adgang til mikrofon, lokation, fotos og kamera fra, når du ikke bruger dem? Du bør slå lokalitetstjenester fra dit kamera, for på den måde forsvinder de 'metadata' - tid og sted - som ligger gemt i alle billeder. På en iphone kan du også overveje at slukke 'hyppige lokaliteter', som du finder under 'systemtjenester' under 'lokalitetstjenester'.

Fif: Et godt værktøj til at styre, hvem du vil give adgang til dit webcam og mikrofon på din Mac er Oversight på objective-see.com.

CHAPTER 13

SLET DINE SPOR

Det er aldrig for sent at gå i gang med at få kontrol over sine data og slette de spor, du ikke er glad for. Noget er måske videredelt, og det kan du ikke få kontrol over, men meget ofte kan du få slettet det, du vil af med.

Første trin er at spørge sig selv, hvem har **oprindeligt** postet det? En ven, dig selv på en andens site eller en helt tredje. Du går så til originalkilden og beder om at få det fjernet. Hvis det fx er noget, du har skrevet på Instagram, så fjern det selv. Hvis du er tagget, bed vedkommende om at untagge dig, og hvis du har deltaget hidsigt i en debat på et nyhedssite, som ofte kommer

højt op i søgeresultaterne, kan du bede dem om at fjerne dit navn eller i det mindste pseudonymisere det – altså bruge et andet navn end dit eget (men det rigtige så er redaktionen bekendt). Dermed forsvinder det efter kort tid, når man søger på dit navn, for Googles og andre søgemaskiners algoritmer bliver overskrevet igen og igen.

Hvis du ikke kan overtale dem (brug argumenter som *Det ødelægger mit omdømme* eller *Jeg har ret til selv at kontrollere mine data* eller *Jeg går til Datatilsynet*). **Datatilsynet** skriver faktisk, at de bør pseudonomisere dig. Det samme kan du gøre over for venner, som har delt billeder o.lign af dig uden dit samtykke (accept). Det er ulovligt, hvis der fx er delt nøgenbilleder af dig uden dit samtykke.

Værktøjer til at slette min spor:

- På norske **slettmeg**.no eller amerikanske **justdelete**.me kan du få hjælp til at slette dig selv på forskellige hjemmesider. På **deseat**.me kan du få hjælp til at finde alle de tjenester, du har signet op med ved hjælp af Google og så slette dem.
- Her www.facebook.com/help/delete_account kan du slette dig på Facebook.
- Hos **Google** kan du få slettet søgeresultater på dit navn, hvis det er løgn eller uddateret. Find linket ved at søge på 'Delete me Google'. Det er en rettighed, vi kun har i Europa. Se også kapitel 14 om dine rettigheder.
- Dit mobiltelefonnummer er offentligt pr default – så du skal selv sige det til

dit teleselskab, hvis du ønsker hemmeligt nummer.

- Hvis du ønsker hemmelig adresse, så gør du det på **cpr.dk,** hvor der er forskellige former for beskyttelse – herunder **robinsonlisten.dk** som sikrer, at ingen må ringe til dig for at sælge dig et eller andet.

CHAPTER 14

DINE RETTIGHEDER

Som europæer har du en række rettigheder i forhold til dine data, som ikke findes i hverken USA eller Kina. Retten til et privatliv er en menneskeret, og med den europæiske datalovgivning GDPR har du ret til følgende;

- **Adgangsret.** Du har ret til få information om behandlingen af dine persondata
  Ret til berigtigelse. Du kan få rettet forkerte, unøjagtige el ufuldstændige persondata.
- **Ret til sletning.** Du kan anmode om at få data slettet, når de ikke længere skal

bruges, eller hvis det er ulovligt at behandle dem.

- **Ret til begrænset databehandling.** Du kan anmode om begrænsning af behandlingen af dine data i bestemte tilfælde.
- **Ret til dataportabilitet.** Du har ret til at få udleveret dine data i et maskinlæsbart format og sende dem til en anden virksomhed, myndighed eller oganisation.
- **Ret til indsigelse.** Du er berettiget til at gøre indsigelse mod visse typer databehandling , fx til markedsføringsformål eller af årsager, der omhandler bestemte forhold, der gælder for dig.
- **Ret til at sige nej til profilering og automatiske beslutnigner.** Du kan anmode om, at automatiske afgørelser,

som omhandler eller påvirker dig, og som er baseret på dine data, træffes af fysiske personer og ikke kun af computere.

CHAPTER 15

HVEM KAN JEG STOLE PÅ?

De fleste vil dig det godt, men for at finde ud af, hvem du kan stole på nettet, lige som du gør, når du handler fysiske butikker, så tjek følgende:

- Hvad **lever** virksomheden af? Andres data eller sælger den – for penge – et produkt eller en ydelse, som ikke er baseret på dine data? Med andre ord: Tager virksomheden ikke penge for sit produkt, er det ikke gratis, for så er du produktet – du betaler med dine eller dine venners data (såsom lokation, kontakter, beskeder mv). Der kan være virksomheder, som giver noget væk

gratis for at få opmærksomhed, men tager så penge for sit hovedprodukt.
- Hvor har virksomheden **hovedkontor?** Hvis den bor i Europa, skal den efterleve en strengere lovgivning end i USA og Kina.
- Kan du tydeligt se, **hvem der står bag** sitet, og hvordan man kan komme i kontakt med dem?
- Kan brugerne af sitet **interagere** med dem, der står bag sitet og med hinanden, og hvad siger de om produktet?
- Har virksomheden en **privatlivspolitik**, en datapolitik eller nogle handelsbetingelser, der er til at forstå for helt almindelige mennesker, så har den sandsynligvis tænkt godt og grundigt over, hvordan den passer på dine data.

- **Videresælger** eller -deler virksomheden data med andre, og hvem er det? Husk 'gratis' betyder betaling med dine data – ofte også til tredjeparter.
- Er virksomheden **ærlig omkring de data**, den indsamler og henter? Sammenlign det, den siger, den samler ind, med de data, som du kan regne ud, at den har brug for for at give dig den service, du efterspørger.
- Hvordan optræder virksomheden på forskellige tjenester, der **rangerer dem på privacy**, fx Ranking Digital Rights, TOSDR, TermsOfConditions, Electronic Frontier Foundation og TrustPilot. Og hvad kommer der frem om den, hvis du søger på dens navn og så persondata/privacy?
- Husk; mange virksomheder markedsfører sig som om, de er på din

side. Vær varsom overfor den slags markedsføring. Er det for godt til at være sandt?

CHAPTER 16

EKSTRA

FOR DIG, DER TAGER DIG TIDEN TIL AT TAGE KONTROL OVER DINE DATA

- **Sluk wifi og bluetooth** og slå din **mikrofon og lokation fra** så ofte som muligt. Giv kun de apps, du har tillid til, adgang til din mikrofon (mange apps 'lytter med' for at indsamle viden om dig) og lokation (som kan sige lige så meget om dig som dine fingeraftryk). Sæt tape over dit webcam, da din gadget kan blive hacket, og andre kan

kigge på dig fra den anden side af dit webcam.

- Alternativ fotodelingsapp: Shoeboxapp.com (canadisk).
- Brug ikke det samme kodeord på alle dine tjenester. Det er bedre at have forskellige kodeord på en lille seddel i din pung. Der skal altid være store og små bogstaver samt tal i dine kodeord. Download evt. en **password manager** (som du kan have som app på både computer og mobil), hvor du kun skal huske ét svært kodeord, og så ligger resten bag lås og slå. Vælg **1password** (canadisk) eller **Keepass** (fransk - *open source*, som er godt, fordi så kan andre se, hvordan det er udviklet). Hvis du har en iPhone kan du bruge dens password manager som du finder her:

Indstillinger, Adgangskoder og Konti, koder til websteder og apps

- Vælg så vidt muligt hjemmesider, der begynder med **HTTPS** - s'et er et tegn på, at siden krypteret og dermed beskytter dine oplysninger.
- Brug **tofaktor-identifikation** hos de tjenester, du bruger, som tilbyder det, eller gør det selv med; FreeOPT eller Yubikee. To faktor autentifikation betyder, at der skal mere end én adgangskode til for, at tilgå et system. Der tillægges derfor et ekstra lag af beskyttelse.
- **Apple Maps** er bedre end Google Maps, når det gælder privacy. Open Street Map er også god og sikker: Download **OsmandMaps** appen og inde i den, kan du gratis downloade de/t kort, du har

brug for. Her openstreetmap.org finder du **Open Street Map** til din computer.

CHAPTER 17

SAMARBEJDSVÆRKTØJER

Google Docs er et fremragende værktøj, men ved at bruge det fodrer man datamonopolet Google med mere guld (data). Heldigvis kommer der flere og flere alternativer. Nedenfor nogle gode samarbejdsværktøjer.

Alternativer til Google Docs:

- **Nextcloud.com** (tysk)
- **Cryptpad.fr** (fransk)

Gode live værktøjer til at quizze, aftstemninger mv uden logging og anonymt

- **Screen.io** (finsk)
- **Kahoot.com** (norsk)

Alternativ til Skype og Zoom, hvor man blot kreerer et navn og mødes på et link i browseren:

- **Whereby.com** (norsk)
- **Meet.jit.si** (australsk)

CHAPTER 18

PROFESSIONEL IDENTITET

Det er vigtigt, at du er synlig digitalt. Sociale medier er gode til at dele din professionelle identitet med, dvs dit job og jobrelaterede ting, eller hvis du har en faglighed. Er du fx super god til at programmere, jonglerer eller har en sportsgren, som du kan vise frem, så fortæl om det.

Opret dig med dit rigtige navn på **LinkedIn, about.me** og evt **Twitter.**com. Sørg for et godt foto, et kort og klart resumé/bio (det er det, de fleste orker at læse) og en kontakt-mulighed til dig – gerne en email, som de fleste chefer bruger.

Lav din **egen hjemmeside** og find nogle faste tagord, som du bruger igen og igen, når du skriver blogs og indhold på dit site (så bliver du lettere fundet i søgninger). Det handler om at producere søgbart indhold.

På **applymagicsauce**.com kan lave en analyse af din psykologiske profil på Twitter eller en af dine tekster og få en ide om, hvad andre også kan finde ud af om dig. På **Crystalknows.com** kan du analysere folks professionelle personligheder via LinkedIn.

Husk at det er nemt for andre at tolke ting om dig, som du er uenig i, og har du ikke nogenlunde kontrol over dine digitale fodspor, kan det nemmere ske. Hvis du ikke kom til en jobsamtale eller fik et studenterjob, får du det sjældent at vide, hvis det skyldtes dine digitale fodspor. Så få styr på dem. Tænk bare selv, hvad du

gør, når du skal undersøge noget nyt eller et menneske, du vil vide mere om.

CHAPTER 19

BLIV KLAR PÅ EN UGE

Brug 15 minutter hver dag på at blive en digital ninja. Her er en mulig plan:

Dag 1: Vælg en sikker browser, fx Click (kap 10) og installer en søgemaskine i den (kap 2) Brug også Firefox og Safari som browser og installér en sikker søgemaskine i den.

Dag 2: Gennemgå dine såkaldte privatlivsindstillinger på dine SoMe og beskyt din venneskreds mv (kap 11) og luk for adgangen til din mikrofon, lokation, kamera mv på din mobil (kap 12 og 16) og så tænd dem kun, når du skal bruge dem.

Dag 3: Arbejd med at skille din private identitet fra din professionelle. Eller gem dit eget navn til du skal i gang med den professionelle og ændr dit navn på Facebook, Instagram, SnapChat, Discord etc. Du kan få gode navne på Fakename-generator (kap 8)

Dag 4: De store gængse browsere som Firefox, Safari og Chrome bør have en adblocker installeret. Installer og aktiver fx Ghostery i alle dine brosere (kap 3) og installer AdblockFast eller AdblockPlus på din telefon.

Dag 5: Skift Facebook Messenger ud med en sikker chat som Wire eller Signal og lok dine venner derover.

Dag 6. Overtal dine forældre til at købe en VPN, fx IBVNP.com og installer den på alle dine gadgets. Indtil de er klar til at betale, så

eksperimenter med VPN på Opera-broseren (kap 5)

Dag 7. Før en samtale med en ven på appear.in (kap 17) og brug den i stedet for Facebook Messenger eller nogen af de andre stor

For dig der vil endnu videre: Tjek samarbejdsværktøjer (kap 17) og professionel identitet (kap 19)