TOTALT ÖVERVAKAD

Så hotar dagens digitala massövervakning

att rasera fria samhällen

MULLVAD VPN

TOTALT ÖVERVAKAD

Så hotar dagens digitala massövervakning
att rasera fria samhällen

MULLVAD VPN

INNEHÅLL

Andra upplagan. Tryckt i Sverige augusti 2024

Den kommersiella massövervakningen

Affärsmodellen 8–21
De stora techbolagen vet allt om dig – oavsett om du använder deras tjänster eller ej.

Aktörerna bakom datainsamlingen – big tech 22–33
Här är bolagen som kartlägger ditt liv. Del 1: big tech – har samlat in så mycket data om dig att de tappat kontrollen.

Aktörerna bakom datainsamlingen – data brokers 34–39
Här är bolagen som kartlägger ditt liv. Del 2: data brokers – du har aldrig hört talas om dem. De vet det mesta om dig.

Tekniken bakom datainsamlingen 40–53
Så går det till när den kommersiella massövervakningen samlar in din data och kartlägger ditt liv.

Insamlad data går inte att hålla anonym 54–57
De som samlar in data påstår ofta att den är anonym. Forskningen visar att det är omöjligt.

Den statliga massövervakningen

Demokratiska och auktoritära länder tävlar i vem som kan massövervaka flest och bäst (värst). 58–79

Going dark: ett amerikanskt-europeiskt samarbete för att knäcka privat kommunikation i det dolda. 80–105

Konsekvenserna av massövervakningen

Så används datan som samlas in 106–117
Övervakningen av ditt internetbeteende får konsekvenser, du kanske inte bara ser dem än.

Så hotar datainsamlingen ett fritt samhälle 118–133
Både den statliga och den kommersiella massövervakningen riskerar att förvandla fria demokratier till rena kontrollstater.

Vi har alla något att dölja 134–141
Till dig som inte har något att dölja: en dag kanske du har det. Eftersom det inte är du som sätter reglerna.

Källor 142–152

FÖRORD

Vi lever i en värld där allt vi gör på internet spåras och sparas (om vi inte gör motstånd med privacy-fokuserade tjänster). Det har byggts en infrastruktur som innebär att stora techbolag kan följa varje steg vi tar, där dina innersta tankar (dina googlingar) inte längre är dina egna. Det här har pågått i över tjugo år och nu börjar vi på allvar se konsekvenserna av det.

Några av världens största techbolag har tillåtits samla in högst personlig data om världens alla medborgare. De gör det via sociala medier och appar. Men framförallt gör de det via varenda hemsida som besöks. Du behöver inte ens ha laddat ner Facebook-appen för att Meta ska ha koll på exakt vem du är.

Det är inte bara de stora techbolagen som agerar så här. Testa att läsa det finstilta nästa gång du går in på en sajt. Det är hundratals, ibland tusentals, aktörer som finns på plats för att registrera vad du gör. De flesta av dem är så kallade data brokers – bolag med ett enda syfte: att samla in data om dig för att paketera och sälja vidare. I grunden är det här olagligt (Meta och Google har åkt på dryga böter för detta). Frågan är varför det får fortgå? Det korta svaret är väl att för många bolag är intresserade av att tjäna pengar på det. Och för många stater är intresserade av att använda datainsamlingen för politisk påverkan och kontroll.

2013 avslöjade Snowden hur USA bedrev olaglig (konstaterat i amerikansk federal domstol) massövervakning av både utländska som amerikanska medborgare. Han visselblåste om lagöverträdelser – ändå kan han inte återvända till sitt hemland med risk för konsekvenserna. Så sent som våren 2024 förlängde USA den undantagslag som strider mot deras konstitution och som gör det möjligt för dem att kartlägga varenda människa på jorden.

I Europa har EU-kommissionen och delar av ministerrådet försökt införa så kallad chat control genom att helt köra över både EU-domstol och mänskliga rättigheter. Gång på gång bryter makten mot den mänskliga rättighet som handlar om att var och en av oss har rätt till ett privatliv. Minst fem EU-länder har blivit påkomna med att använda spionverktyget Pegasus mot meningsmotståndare. Ändå tycker de att de har rätt att massövervaka under parollen ”har du inget att dölja har du inget att oroa dig för”.

Redan idag ser vi hur insamlad personlig data används i påverkanskampanjer för att vinna val. Vi kan känna av konsekvenserna här och nu. Men den stora frågan är var vi hamnar om vi inte får stopp på utvecklingen. I Kina ser vi hur massövervakningen används för att kontrollera befolkningen och förfölja dem som är kritiska mot staten, för att bygga social score-system och ta sikte på en framtid som påminner om dystopiska filmer och böcker. Det där är slutstationen. Om demokratiska länder tror att det går att flytta gränsen framför sig i all oändlighet så har de fel. Till sist återstår bara total övervakning och total kontroll.

Personlig integritet är rättigheten som alla andra rättigheter vilar på. Om vi inte har rätten att utforska nya tankar och idéer utan att någon hela tiden registrerar det, om vi inte har rätten att föra privata samtal med våra närmaste, om vi inte har rätten att själva bestämma när och till vilka vi vill yttra något – har vi då yttrandefrihet? Yttrandefrihet handlar om rätten att få säga sin mening, men borde också

handla om rätten att få bestämma när och var och till vilka man säger det. Har vi inte rätten till ett privatliv har vi förlorat rätten som självständiga människor.

Till dig som säger att du inte har något att dölja: det handlar inte om dig. Det handlar om oss alla. Det handlar om alla de som faktiskt har något att dölja (regimkritiska aktivister, visselblåsare, journalister, advokater som arbetar för mänskliga rättigheter, utsatta människor, statsmän som bär på hemligheter för rikets säkerhet, innovatörer med banbrytande idéer, med flera, med flera). Framförallt handlar det om vad datainsamlingen gör med oss som människor och hur den påverkar hela samhällen på sikt. Det handlar om allas vår framtid. Om kommande generationer. Och om de ska växa upp i ett fritt eller kontrollerande samhälle.

Det är dags för världens politiker att ta itu med grundproblemet. Det spelar ingen roll om enskilda metoder (till exempel tredjepartscookies) skulle förbjudas. Det handlar inte om att reglera detaljer, eftersom de stora datainsamlarna ständigt vänder sig till ny teknik. Det måste till en större förändring. Att samla in personlig data och sälja eller dela den med andra måste förbjudas. Vi måste lämna affärsmodellerna som bygger på människors beteendedata. Vi behöver också ställa myndigheter till svars för deras lagöverträdelser. Som folk behöver vi rösta fram politiker som värnar om grundlagar, konstitutioner och överenskommelser om mänskliga rättigheter. Demokratiska samhällen bygger i mångt och mycket på att vi satt gränser för dem som sitter på makten. Vi har gjort det av en anledning. Så länge de gränserna fortsätter att överträdas kommer vi på Mullvad bidra med tekniskt motstånd.

Jan Jonsson
VD, Mullvad VPN

DEN KOMMERSIELLA MASSÖVERVAKNINGEN: AFFÄRSMODELLEN

De stora techbolagen vet allt om dig – oavsett om du använder deras tjänster eller ej.

Ditt beteende online är råvaran som byggt en av de största ekonomierna i världshistorien. Men det är inte bilderna du postar, kommentarerna du skriver eller meddelandena du skickar som är hårdvalutan. Det är datan om datan som är guldet. Med det som kallas metadata nöjer sig de stora techbolagen inte med att övervaka ditt liv – de har bestämt sig för att styra det.

Internet har utvecklats till en infrastruktur där det i grova drag är möjligt att ta reda på vad som helst om vem som helst när som helst. Och det är inte bara teoretiskt dravel, utan det är en möjlighet som utnyttjas varenda dag. Övervakning har blivit själva motorn för the world wide web. Att kartlägga jordens alla människor har gött en av världshistoriens fetaste kassakor. Det kan låta svulstigt och tillspetsat när det kommer från ett företag som erbjuder tjänster för integritet online, men faktum är att det är så den krassa verkligheten ser ut. Varenda steg vi tar stoppas in i stora system där AI och maskininlär-

ning används för att registrera, kategorisera och räkna ut vad vi ska göra härnäst.

I grunden finns det två sorters massövervakare i den digitala världen: De som övervakar människor för att tjäna pengar (techbolag) och de som övervakar människor för att kontrollera dem (stater). Inte sällan korsas deras vägar, inte minst när de senare åker snålskjuts och rotar i techbolagens datalagring. Vi ska återkomma till de statliga övervakarna, men börjar med de som samlar in mängder av data i kommersiellt syfte.

Låt oss börja med det uppenbara. De stora techbolagen loggar din aktivitet på deras plattformar för att tjäna pengar. Om du har ett Facebook-konto samlar Meta in data på din aktivitet där och använder du Messenger så sparar Meta de privata meddelande som du skriver till vänner och familj[1] (om du inte klickar i den end-to-end-kryptering som de nu lanserat på senare dar). Om du använder Googles tjänster – om du till exempel skickar e-post med Gmail eller loggar in på Youtube för att kolla videoklipp – då sparar och kategoriserar Google allt du gör, eftersom du hänger på deras plattformar. När du använder apparna i din telefon loggar de så klart din aktivitet. Och de sociala medierna byter så klart den här informationen fram och tillbaka med varandra hej vilt[2]. Bland annat har läckor avslöjat att Meta läckt personliga konversationer till några av de 150 samarbetspartners[3] som verkar gå utanför de integritetsregler som bolaget satte upp efter Cambridge Analytica-skandalen[4]. Det här är samarbeten som inte syns på ytan och som inte går att reglera i användarinställningar[5], utan som oftast bara kommer till allmänhetens vetskap i samband med läckor, rättegångar och utfrågningar i till exempel kongresser och parlament. Den insamlade datan används för att skräddarsy din filterbubbla och för att rikta information och annonser till dig (och så ingår den i ett större ekonomiskt sammanhang av kommersiell massövervakning som vi snart kommer till). Detta är

som sagt uppenbart; detta är data som du överlåter när du accepterar användarvillkoren. Det är lika uppenbart att det går att välja bort den här typen av tjänster. Det finns så klart alternativa sociala medier som valt en annan väg (de är inte direkt i numerärt överläge så att säga, men de finns). Du kan till exempel välja meddelandetjänsten Signal[6] om du vill kommunicera privat. Men det stora problemet med dagens utbredda datainsamling är att du inte ens behöver vara aktiv på de stora tjänsterna för att bidra med big data till big tech.

Det räcker att surfa med en vanlig webbläsare för att bidra till datainsamlingen.

Den insamlade datan som kommer från din inloggade aktivitet på sociala medier är bara toppen av isberget. Den riktigt stora datainsamlingen, den som maler på dag in och dag ut och registrerar allt du gör – den pågår oavsett om du väljer att använda Facebook och Google eller ej. Du kan ha undvikit Meta i hela ditt digitala liv – de vet allt om dig ändå. Det räcker att du surfar med en vanlig webbläsare för att bidra till karusellen. Hur det är möjligt? Meta avslöjar själva metoden redan i namnet. Tekniken de använder sig av är metadata.

”Metadata gjorde det tekniskt möjligt att spola tillbaka händelserna i någon persons liv till en tidpunkt månader eller till och med år tillbaka.”

Edward Snowden

2012 hände något som förändrade hur Edward Snowden såg på sin arbetsgivare (NSA, som ansvarar för USA:s signalspaning) och hur han såg på sin omvärld. Regeringarna i Australien och Storbritannien kom med ett förslag om att göra det obligatoriskt att registrera metadata på internet. I sin bok Permanent Record berättar han om hur ”detta var första gången som demokratiska regeringar offentligt uttalade ambitionen att inrätta en sorts övervakande tidsmaskin, som skulle göra det möjligt för dem att tekniskt spola tillbaka händelserna i någon persons liv till en tidpunkt månader eller till och med år tillbaka”. Snowden argumenterar för att det var en slutgiltig markering på västvärldens omvandling från att vara skapare och försvarare av det fria internet till att bli dess motståndare och blivande förstörare. Men för att parafrasera NSA i nutid: det handlade ju bara om metadata?

Så, vad är metadata? Bruce Schneier, som är en framstående amerikansk kryptograf och säkerhetsexpert, beskriver det som data om data. I sin bok Data and Goliat skriver han:

”I en meddelandetjänst är själva meddelandet datan. Men kontona som skickade iväg och tog emot meddelandet, tiden som meddelandet skickades, allt det där är metadata. I ett e-postsystem är det på samma sätt: texten i mejlet är data, men sändaren, mottagaren, routing data och storleken på meddelandet är metadata. Metadata kanske låter ointressant, men det är allt annat än ointressant.”

Efter att Snowden läckt NSA-dokument arbetade Bruce Schneier tillsammans med en av journalisterna som hängde med Snowden på det där hotellrummet i HongKong: Glenn Greenwald på the Guardian. Schneier hjälpte Greenwald med att analysera de mer tekniska delarna av läckorna, och i samband med det beskrev han problemet med att vifta undan metadata som något icke-personligt.

”När regeringen samlar in metadata försvarar de sig ofta genom att säga att det ’bara är metadata’. Det kan kännas förmildrande för

många människor, men det ska det inte. Att samla in människors metadata är att sätta dem under övervakning.”

Bruce Schneier jämför det med att anlita en privatdetektiv. En privatdetektiv kan bugga ditt mål: lyssna på att allt den personen säger i sitt hem, i sina telefonsamtal och så vidare. Det är data. Men sen kan du också sätta privatdetektiven på att övervaka ditt mål. Då får du en annan sorts rapport. Vem personen träffar, var personen går, var personen spenderar tid, vilka människor personen skriver till, vad personen läser och köper. Det är metadata.

”Avlyssning ger dig alla konversationer. Metadata ger dig allt annat,” skriver Schneier. ”Metadata avslöjar vilka som är dina nära vänner, vilka affärsrelationer du har, vem du är intresserad av och vad som är viktigt för dig. Oavsett hur privat det är.”

”Metadata säger precis allt om någons liv. Om du har tillräckligt mycket metadata så behöver du egentligen inte själva innehållet.”

NSA-chefen Stewart Baker

Insamlingen av metadata i kommersiellt syfte innebär att de stora techbolagen kan kartlägga hela ditt liv. I grova drag så gör metadata det möjligt att föra ett register över alla sajter du besöker, alla sökningar du gör, alla människor du pratar med, hur ofta du pratar med dem och hur länge. Utöver detta har de stora techbolagen den tekniska kompetensen och inte minst viljan att logga även på detaljnivå: exakt vad du shoppar online, vilka annonser du tittar på, vilka produkter du gillar och vilka du snabbt scrollar förbi, vilka texter du läser och vilka videor du tittar på (och återigen, hur ofta du kollar och hur länge). Och allt detta har de tillgång till oavsett om du är inloggad på deras tjänster eller inte, eftersom internets infrastruktur innebär att i princip alla sajter i världen hänger ihop med de stora techbolagen i affärssyfte.

Stewart Baker, tidigare general counsel på NSA, uttryckte det med tydlighet[7] : ”Metadata säger precis allt om någons liv. Om du har tillräckligt mycket metadata så behöver du egentligen inte själva innehållet.”

Hans kollega Michael Hayden, tidigare director på NSA och CIA, håller med och refererade i en debatt på John Hopkins University[8] till Baker när han sa: ”Baker har absolut rätt, vi dödar människor baserat på metadata.”

”Vi ljuger inte för våra sökmotorer. De vet mer om mina tankar än vad jag själv gör.”

Den här texten ska som sagt inte handla om den statliga massövervakningen, men vi tycker att de statliga representanterna bidrar med en tydlig bild av vad metadata är och hur den pricksäkert kan användas. Det är också viktigt att poängtera: NSA sorterar in sökhistorik under metadata. Bruce Schneier menar att det går att diskutera huruvida data från sökmotorer är data eller metadata, men eftersom sökningarna är inbäddade i våra webbläsares adressfält faller de in

under den kategorin. Det om något borde räcka för att avfärda argumentet ”det är ju bara metadata”.

”Vi ljuger inte för våra sökmotorer,” säger Schneier. ”Google vet vilken sorts porr vi söker efter, vilka gamla älskare vi fortfarande tänker på, vad vi skäms för, vad vi oroar oss för, vilka hemligheter vi har. Om Google bestämmer sig kan de räkna ut vilka av oss som är oroliga för vår mentala hälsa, vilka som planerar skatteflykt eller vilka av oss som bestämt sig för att protestera mot ett särskilt regeringsbeslut. Jag brukade säga att Google vet mer om mina tankar än min fru. Men det är inte ett tillräckligt starkt uttryck. Google vet mer om mina tankar än vad jag själv gör, eftersom Google kommer ihåg exakt allt och gör det med exakthet i oändlighet.”

Leah Elliott, som är satirtecknare och digital rättsaktivist, är inne på samma spår. I sin serie Contra Chrome[9] – How Google’s Browser became a threat to privacy and democracy – uttrycker hon det så här:

“Du tror att det är du som kollar upp saker på nätet, men i själva verket är det Google och andra som kollar upp dig. De extraherar ditt beteende utan ditt medvetande, din kunskap eller ditt medgivande.”

Bruce Schneiers jämförelse med privatdetektiven är god, men den är inte tillräcklig, eftersom livet vi lever digitalt inte är helt jämförbart med livet vi lever i den fysiska världen. Eftersom det vi söker efter i sökmotorer och sidorna vi besöker reflekterar våra tankar på ett sätt som inte vårt fysiska beteende gör. Internet har kortat avståndet mellan tanke och agerande på ett sätt som saknar motstycke i den fysiska världen. Om vi är oroliga över att vi dricker för mycket kan vi googla det; vi måste inte gå ut och slänga alla spritflaskor i soptunnan, smygläsa en bok i ämnet på biblioteket eller gå till ett fysiskt möte med privatdetektiven i hasorna. Kartläggningen av människor online innebär att man tränger in i människors huvuden och läser av funderingar innan de blommar ut och blir agerande.

På samma sätt är metadata inte heller jämförbart med de direkta konversationer vi för online. Det finns delar av ditt liv som du kanske inte är redo att skriva eller prata om med andra, men som du utforskar i din ensamhet. Metadata gör det till och med möjligt att upptäcka saker som vi kanske inte ens visste om oss själva. Små justeringar i vilka sorts livsmedel du söker efter kan indikera att du är gravid innan du själv gjort testet. Metadata är också lika med insamling av data som inte är lagligt i många länder. Till exempel registrering av politisk, sexuell eller religiös läggning. Om du är inne på din kyrkas webbplats varje söndag är det sannolikt att du tillhör just det trossamfundet. Det är data som de stora techbolagen har på dig, men som är förbjudet enligt lag. Techbolagen gömmer sig bakom argumentet att ”det bara är metadata” och att det är anonym data – men på mindre ett ögonblick skulle den informationen kunna av-anonymiseras och kopplas till dig som person.

I dokumentären The Big Data Robbery[10] kallar Harvardprofessorn Shoshana Zuboff metadatan för avfall.

”I början av 2000-talet såg man på den här typen av data som just extradata. De kallade det för dataavgaser. Men så småningom förstod man att det här avfallet var material som innehöll själva rikedomen: datan som kunde förutse framtiden.”

Den här insikten förvandlade internet i grunden. Människors sätt att surfa blev det nya guldet och de stora techbolagen gjorde sig en förmögenhet på metadatan. Men det är inte bara de kända stora företagen som trängs på den nya digitala marknadsplatsen. Den nya ekonomin har lockat till sig bland annat data brokers som roffar åt sig en del av kakan genom att bara samla in, köpa och sälja data om vilka sidor människor besöker, vilka sökningar de gör och så vidare.

”De insåg från första början att de var tvungna att dölja datainsamlingen. De var tvungna att observera användarna genom en envägs-spegel. Det är det som gör det till övervakning.”

Shoshana Zuboff

Zuboff kallar internets nya infrastruktur för övervakningskapitalism. Kapitalism för att de tjänar pengar på att kartlägga människors beteende på internet. Övervakning för att de observerar oss i hemlighet och använder sig av metoder som är utvecklade för att vi inte ska bli medvetna om dem.

”De här företagen gillar att säga att ’vi samlar in data så att vi kan förbättra vår tjänst’ och det är sant. De samlar in data och en del av den används för att förbättra tjänsten för dig. Men betydligt mer data används för att analyseras och för att träna det som de kallar modeller, mönster av mänskligt beteende. När de väl har de här modellerna så kan de se hur människor med en viss typ av karaktär beter sig över tid. Sen placerar de in människor på ark i det här systemet och där kan de se vad du sannolikt kommer att göra, inte bara i stunden utan även snart och inte minst långt senare. Det här är vad jag kallar för beteendeöverskott; dataströmmar som är fyllda med förutseende data. Varför överskott? För att redan från start var det här mer data än vad som krävdes för att förbättra produkter och tjänster.”

Ditt beteende på internet säljs till både banker och försäkringsbolag.

I sin bok The Age of Surveillance Capitalism skriver Zuboff om de stora techbolagen att de tidigt förstod att de var tvungna att dölja deras affärsmodell. I en intervju i Contagious magazine[11] utvecklade hon sitt resonemang.

”Google fattade att detta inte skulle landa så bra hos folk; att de bara tog ditt beteende online och förvandlade det till data för sin egen vinnings skull, för att gynna sitt eget system för produktion och försäljning. Från allra första början insåg de att de här mekanismerna var tvungna att döljas. De var tvungna att observera användarna genom en en-vägs-spegel. Det är det som gör detta till övervakning.”

Själva utförandet är dolt. Det är begravt i hundratals policysidor som ingen orkar läsa (det är mycket lättare att bara trycka acceptera när cookie-frågan kommer upp). Eller inte ens känt: som när Meta vägrar att svara på vilken data de samlar in, till och med när domstolen frågar[12]. Men själva filosofin bakom övervakningskapitalismen har de stora bolagen varit hyfsat transparenta med redan från start. Mark Zuckerberg har pratat om att integritet inte längre är en rådande norm[13]. Eller som när Eric Schmidt, vd för Google under åren 2001-2011, i en intervju[14] uttryckte sig så här:

”Om du gör något som du inte vill att andra ska veta om, då kanske du inte ska göra det till att börja med”.

Det lustiga var att Schmidt sen svartlistade tidningen CNET[15] efter att deras journalister hängt ut en mängd information om Schmidt i en artikel. Informationen hade de fått tag på enbart genom att googla.

Ett ännu tydligare uttalande och bevis på Googles inriktning i början av 2010-talet kom i ytterligare en intervju[16] där Schmidt sa: ”Vi vet var du är. Vi vet var du har varit. Vi vet mer eller mindre vad du tänker på.”

Sedan dess har mängden insamlad data bara ökat. Som Tristan Harris, tidigare design ethicist på Google och senare grundare för The Center of Humane Technology[17,] uttryckte det i dokumentärfilmen Social Dilemma[18]: ”De vet när folk känner sig ensamma. De vet när folk är deprimerade. De vet när folk tittar på bilder på sina ex. De vet vad man gör sent på kvällen, de vet allt. De vet om man är introvert eller extrovert, vad för sorts neuroser man har, vad man har för personlighet.”

”Företagen kallar det marknadsföring, men det är inget annat än övervakning.”

Bruce Schneier

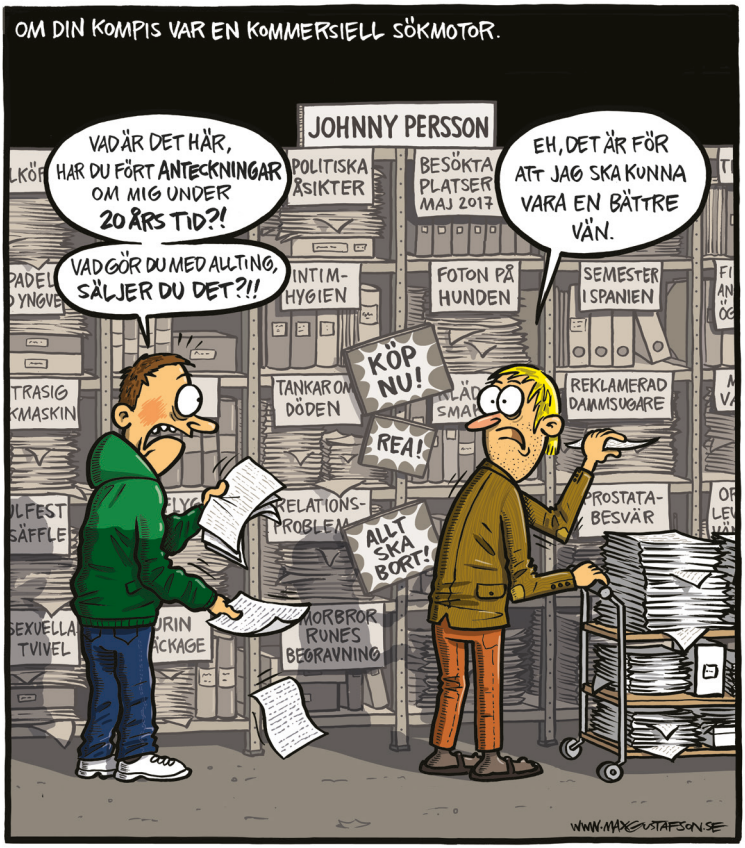
Precis som Shoshana Zuboff är Bruce Schneier noga med att peka ut den här affärsmodellen som övervakning och inget annat.

”Företagen kallar det för marknadsföring, men det är övervakning. Övervakning är affärsmodellen som internet bygger på idag. Vi har byggt system som spionerar på människor i utbyte mot deras tjänst.”

Övervakning handlar i grunden om kontroll, det är själva syftet med den. Och det är tydligt att affärsmodellen som råder på internet idag inte bara handlar om att observera. Den infrastruktur som är byggd gör det möjligt att använda det som Zuboff kallar ”framtida beteenden” för att styra människor i den riktning som man önskar. Beteendedata har blivit verktyget som används för att tilta människor i olika riktningar, för ekonomisk eller politisk vinning. Zuboff menar att de stora techbolagen gått från att övervaka till att aktivera[19]. I sin bok The Age of Surveillance Capitalism skriver hon:

”Automatiserade maskinprocesser inte bara känner till våra beteenden utan också formar våra beteenden. Den här nyorienteringen från kunskap till makt gör att det inte längre räcker med att automatisera informationsflödena om oss; målet är nu att automatisera oss. Dagens prediktionsprodukter finns på en marknad för framtida beteenden som handlar om oändligt mycket mer än bara riktad

reklam på internet. Numera innefattar denna affärsmodell bland annat försäkringsbranschen, detaljhandeln, finansbranschen och en växande sektor av transport- och tjänsteföretag som är fast beslutna att delta i dessa nya och lönsamma marknader. I de tusentals transaktioner vi gör, så betalar vi för vår egen underkastelse."



DEN KOMMERSIELLA MASSÖVERVAKNINGEN: AKTÖRERNA BAKOM DATAINSAMLINGEN

Här är bolagen som kartlägger ditt liv.

Del 1: Big Tech – har samlat in så mycket data om dig att de tappat kontrollen.

Du vet redan vilka de stora bolagen är som samlar in data i kommersiellt syfte. Men frågan är om du har koll på den absurda omfattningen? Du kan fundera på svaret, men svaret är nej. Inte ens företagen själva vet hur mycket data de samlar in, var den tar vägen och hur de ska kontrollera den.

Kartläggningen av människors beteende på internet genom insamling av data, som i allra högsta grad är privat, har lagt grunden för en av världens största ekonomier. Exakt hur det går till och vad datan används till kommer vi till senare. Men nu ska vi ägna några rader till att peka ut techbolagen som driver på den marknadsplats av beteendedata som internet förvandlats till och hur absurt mycket data de samlar in.

Låt oss börja med internetleverantörerna. Det är ju ganska uppenbart att de håller koll på vad du gör online (om du inte använder en VPN förstås). Det är inte heller särskilt konstigt att de gör det; i väldigt många länder är de enligt lag tvingade att logga din trafik.

Det betyder inte att alla internetleverantörer gör sig en extra hacka genom att sälja datan vidare, men i ett land som USA hör det till vanligheterna[20]. En granskning av Vice visade att det till och med gått att köpa människors geografiska position i realtid[21]. Och i en rapport slår The Federal Trade Commission i USA fast att minst sex av de största internetleverantörerna kartlägger sina kunders internetbeteende[22] och att deras alternativ för att erbjuda kunderna integritet är en illusion.

Vad har vi mer? Betalningstjänster: Paypal har till exempel rapporterats ha villkorstexter som är längre än Shakespeares Hamlet[23], vilket signalerar om en lite väl tilltagen datainsamling. Apparna i din telefon: Washington Posts journalist Geffrey A. Fowler räknade samman antal ord i sina telefonappars privacy policies[24] och kom upp i en miljon – eller dubbelt så långt som Tolstojs Krig och Fred om vi ska fortsätta jämföra med klassisk litteratur. Och ja, så långa användaravtal är lika med att samla in data. När det gäller apparna är det inte minst location data som är åtråvärd. Och i just den här kategorin finns det ingen gräns för hur känslig data[25] som går till högstbjudande; besök på läkarkliniker och trossamfund tillhör basvarorna på en marknadsplats där människors fysiska rörelsemönster omsätter 12 miljarder dollar per år[26.] Och tro inte att du är skonad för att du stängt av platstjänster. Låt oss för enkelhetens skull använda Meta som exempel. I deras affärsmodell ingår det att betala sig ur åtal. Det är inget problem för dem ekonomiskt, men för varje förlikning får vi veta lite mer om deras metoder. I en enda uppgörelse under 2022 betalade de till exempel 37 miljoner dollar efter att ha spårat 70 miljoner användare[27] trots att de klickat bort platstjänstsfunktionen. Ännu dyrare blev uppgörelsen med de som drabbats i Cambridge Analyticaläckan där Meta gick med att betala 725 miljoner dollar[28] efter att ha läckt bland annat privata konversationer. Just Meta förtjänar en mer utförlig presentation. Du kommer nog hålla med om det när du läst kommande stycken.

Meta – vet inte ens själva hur mycket data de samlar in, var den tar vägen eller hur den ska kunna raderas.

Både Google och Meta erbjuder dig som användare att kontrollera och ta en titt på den samlade data som bolagen har på dig. Men det är en falsk föreställning och långt ifrån hela sanningen. Inte ens i domstol vill Meta berätta om hur mycket data de sitter på. I ett rättegångsförhör kopplat till Cambridge Analytica-skandalen[29] gick bolaget med på att dela med sig av data som går att finna under ”Download Your Information” men argumenterade för att de ville hålla data som kom från ”non-consumer parts of Facebook” utanför rättegången. När rätten inte riktigt gick med på det och krävde svar från två av Metas utvecklingschefer svarade de att inte ens Meta har koll på hur mycket data de har på människor: ”Det finns inte en enda person på Meta som kan svara på den frågan.”[30]

Läckta dokument våren 2022 gav samma bild när anställda på Meta erkände att ”vi har inte kontroll på hur våra system använder datan”[31]. Tidningen Vice publicerade delar av läckan där anställda på Meta jämförde deras system med att hälla bläck i vatten.

”Vi har byggt ett system med öppna gränser. Tänk dig att du har en flaska med bläck. Den innehåller alla möjliga användardata; tredjepartsdata, förstapartsdata, data klassad som känslig. Sen tar du flaskan och häller bläcket i en sjö; alltså vårt datasystem. Bläcket flyter ut överallt. Hur ska du kunna stoppa tillbaka bläcket i flaskan? Och hur ser du till så att bläcket bara flyter i vissa delar av sjön?”

Bilden av ett Meta utan kontroll på sin (din) insamlade data växer fram. Återstår då bara att försöka reda ut hur mycket data de sitter på. Genom åren har vi fått många tecken på att mängden är absurd. När ProPublica gjorde en kartläggning av Facebooks insamling av data visade det sig redan 2016 att Meta hade svindlande 52 000 unika attribut[32] som de kategoriserade människor utifrån med hjälp av

maskinlärning. Meta vill gärna ge sken av att datainsamlingen till största del kommer från användarnas aktivitet på deras plattformar. Men det räcker att läsa om skandal[33] efter skandal[34] efter skandal[35] där Meta och dataläckor har gått hand i hand för att en annan bild ska växa fram. Oftast är läckorna kopplat till den teknik som de en gång i tiden döpte till Facebook Pixel; annonssystemet som miljontals sajter hakat på och som gör det möjligt för Meta att nå långt utanför sina egna appar när de matar sitt AI- och maskininlärningssystem med data.

Meta samlar in information om kunder som köpt graviditetstest och sökt konsultation gällande potensproblem. Detta gäller människor världen över oavsett om de har ett Facebook-konto eller inte.

Enkelt förklarat går Metas Pixelsystem ut på att hemsidor ger Meta tillgång till hur deras hemsidebesökare beter sig – vad de handlar, vad de väljer bort, vilka texter de läser, vilka videor de tittar på och så vidare – och i motprestation får sajterna i sin tur använda sig av Metas totala datainsamling för att skräddarsy och rikta sina annonser (på Metas plattformar och i deras annonssystem) på bästa sätt. I en kartläggning av The Markup[36] visade det sig att var tredje sajt av världens 100 000 populäraste hemsidor var kopplade till Meta Pixel. Det är den här infrastrukturen som gör att Meta har koll på internetanvändare världen över oavsett om de har ett Facebook-konto eller inte[37]. När en läcka via Meta Pixel avslöjas handlar skandalrubrikerna ofta

om att känsliga köp eller beteenden online har gått att knyta till riktiga personer via mejladresser eller telefonnummer. Det har till exempel framgått att pixeltekniken registrerar data om apotekskunder som köpt hiv-test, graviditetstest och sökt konsultation gällande potensproblem[38]. Men egentligen är det ingen skillnad på en ”skandalläcka”, där personuppgifter som mejladress har läckt ut tillsammans med onlinebeteenden, och det konstanta flöde av insamlad data som når techbolagen varje dag, där datan kan knytas till personer med andra metoder: med hjälp av IP-adresser, cookies och andra tekniker. Det spelar ingen roll hur mycket de stora techbolagen svär sig fria genom att säga att datan de har på profiler är anonymiserad. Har du bara tillräckligt mycket data på en person går det inte att hålla den anonym. Det går hur snabbt som helst att lägga ett pussel som avslöjar vem som döljer sig bakom datan och så är den av-anonymiserad. Speciellt om hela din affär bygger på stora AI- och maskininlärningssystem vars enda syfte är att kategorisera allt du gör för att bygga en profil på dig.

Även om Meta har tillgång till data om sina två miljarder användare och dessutom spårar människor på var tredje sajt i världen, så nöjer sig företaget inte där. Förutom att de samlar in egen data köper de dessutom extra data från så kallade data brokers[39]. De har också blivit påkomna med att köpa vpn-bolaget Onavo för att använda det som ett spionverktyg. Utåt sett såg det alltså ut som att Meta gav sig in i privacy-världen. Men så var inte fallet (ytterligare en anledning till att det är viktigt att tänka igenom vilken vpn-tjänst man väljer). Istället användes vpn-tjänsten till helt andra syften. De användare som laddade ner Onavo fick spionverktyg installerade på sina telefoner[243]. Genom rena hackingtekniker såg Meta till så att deras vpn-app plockade upp data från andra appar. Framförallt handlade det om att komma över krypterad trafik från konkurrerande tjänsten Snapchat. Den totala datainsamlingen ger Meta förmågan – som de själva be-

skriver det i läckta dokument[40] – att rikta annonser till människor utifrån hur de kommer att bete sig, vad de kommer att köpa och vad de kommer att tänka.

Skandalerna och läckorna och de absurda siffrorna över hur mycket Meta samlar in skildrar företaget på ett bra sätt. Men det som kanske säger allra mest om bolagets värderingar och ambitioner är tillvägagångssätten de använder. Det är i de tekniska detaljerna som det blir tydligt att övervakning är själva kärnan i Metas affärsmodell.

Meta samlar in dina rörelser med musen, meddelandena du skrivit på sociala medier men ångrat och aldrig postat, och hur du rör dig med din mobil även när du klickat nej tack till att dela location data.

Meta är inte kända för att vara transparenta med hur de samlar in data och vad de gör med den. Men det går att ta en bakdörr in i deras huvud genom att läsa deras patent. Ett av dem har de döpt till Offline Trajectories[41] och det går ut på att använda tekniker som kan förutspå när du är på väg att tappa täckning och gå offline. Flera av bolagets patent handlar om just detta: att hitta sätt att lokalisera dig även om du gör motstånd. Ett patent heter Location Prediction Using Wireless Signals on Online Social Networks[42] och precis som det låter går det ut på att använda styrkan i din wifi-uppkoppling eller läsa av din bluetooth för att lokalisera dig. På samma vis har Meta använt andra människors mobiler (i din närhet) för att pricka din position även när du har location data avstängt. Meta har blivit stämda för att bryta mot Apples Tracking Transperancy[43] och de har själva erkänt

att de kan spåra människor även när platstjänster stängts av[44].

Men inget har blottat Metas utbredda datainsamling lika väl som efterspelet av den så kallade Cambridge Analytica-skandalen[45] där 50 miljoner användares metadata och personliga meddelande gick rakt till ett analysbolag som använde informationen för att påverka valet i USA. Bland annat framkom det[46] att Meta läser av och registrerar ditt rörelsemönster med datormusen och vilka publika wifi som finns i närheten av spårade mobiltelefoner. De använder sig av mobilmaster och GPS för att räkna ut var du befinner dig. Och loggar batteriprocent, tillgängligt lagringsutrymme, installerade plugins och hastigheten på din uppkoppling för att identifiera dig. Bolaget erkände också att de använder metadata från bilder du tar med din telefon (data som inte är synligt för blotta ögat men som finns inbäddat i bildfilerna) för att identifiera och spåra dig. Talespersoner för Meta bekräftade också att de registrerar IP-adresser och köper data från data brokers för att bygga tydligare personprofiler.

Metas patent avslöjar kärnan i deras affärsmodell och vilka ambitioner de har. Ett av patenten siktar till och med på att kunna förutse när du ska dö.

Meta har också avslöjats med att använda något som kallas för accelerometern för att spåra människor[47]; det är själva hårdvaran i mobiler som mäter rörelse och riktning och som gör att telefonen till exempel kan skifta mellan liggande och stående läge. Genom att kartlägga rörelsemönster och koppla det till andra appar i din telefon har Meta kunnat identifiera hur du rör dig och när du besöker oli-

ka sorters platser. Den här tekniken har även använts för att matcha med mobiler i din närhet och plötsligt blir det extremt tydligt att techbolagen har tillgång till tekniker långt bortom de uppenbara i deras jakt på personlig data. På ett annat inkräktande sätt har Meta övervakat vad människor skrivit men inte postat[48] i olika formulär på internet. Facebook själva sorterar in dessa ”unposted thoughts” under begreppet ”self-censorchip”. Vi tar det igen: text som du alltså skrivit men som du sedan av någon anledning ångrat att du skrivit och valt att aldrig posta har sparats och loggats av Meta. Men inget chockerar egentligen längre. Meta har även patent på teknik som kan förutse när människor går genom ”life changing events” genom att analysera dagliga rutiner och hur din sömn förändras (med telefonen på nattduksbordet är allt möjligt). Patentet siktar till och med på att kunna förutse när du ska dö[49]. Välkommen till en ny skön värld.

Google – med monopol på både sökmotor och webbläsare vet de allt om alla.

Även om Meta framstår som överlägsna på datainsamling så har de förstås en nästan oslagbar konkurrent i Google. När Facebook Pixel har en närvaro på var tredje sajt har Googles motsvarighet Google Analytics en träffprocent på 74[50]. Upplägget är ungefär detsamma: när en hemsida har Google Analytics installerat – för att mäta och analysera trafiken på hemsidan och koppla det till Googles annonssystem för mer pricksäker marknadsföring – får Google också tillgång till hur besökarna beter sig. Men det är inte det enda verktyget i Googles låda.

Bolaget tillhandahåller också gratis typsnitt till hemsidor. Det är ett erbjudande som 60 miljoner sidor har haft svårt att tacka nej till. Och precis som med företagets analysverktyg så kommer det med samma krav på motprestation: att Google får samla in information om besökarna. På hemsidor som använder Google Fonts kan

de övervaka besökare och hur de beter sig genom att registrera deras IP-adress[51] och sedan korsbefrukta det med all annan information som de har kopplat till just den IP-adressen. Samma sorts insamling sker så fort det finns en Google-sökruta inbäddad på hemsidor (detta gäller för övrigt också så fort det finns en ”dela-knapp” från Facebook, Twitter och Instagram). Sammantaget ger det här ett enormt datainflöde till Google. Men vi vet ju alla att det bara är början.

2022 betalade Google 400 miljoner dollar i en enda förlikning innan de fortsatte med sin kärnverksamhet: att samla in personlig information.

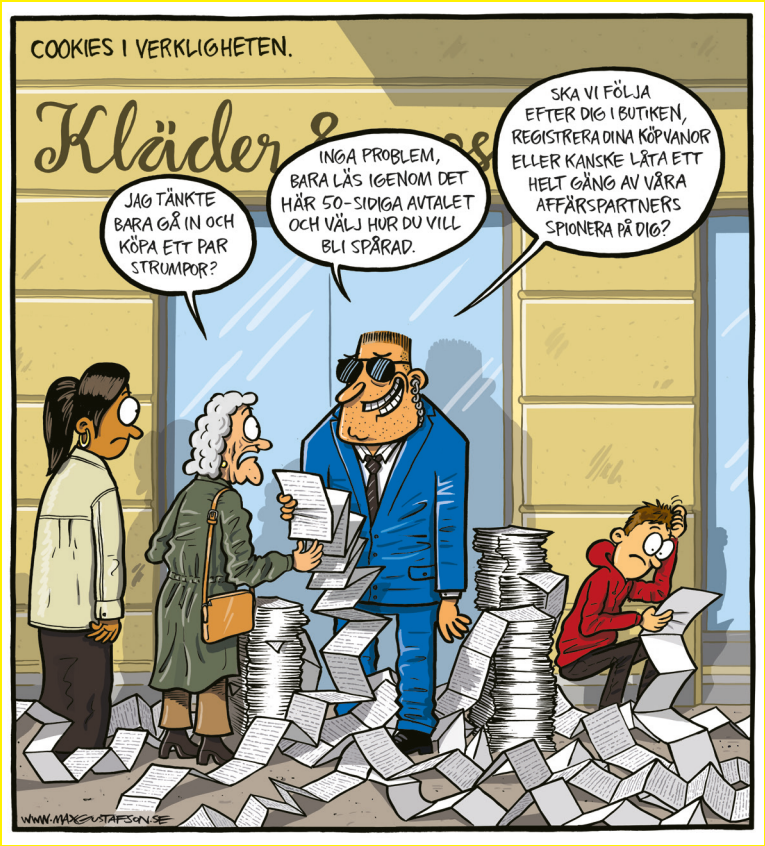
9 av 10 som använder en sökmotor[52] gör det genom att googla. Det innebär att Google har koll på i princip all världens internetanvändares innersta tankar och liv. Och det tar ju inte ens slut där. 7 av 10 webbläsare[53] som används är Googles Chrome, en webbläsare[54] som i princip används för att googla dig snarare än att det är du som googlar vad du nu än googlar. Lägg till Youtube och Gmail så blir det nästan absurt hur mycket Google vet om världen och dess invånare.

Precis som Meta har Google en stor kassa för rättsliga förlikningar[55] (i en enda förlikning 2022 pröjsade de 400 miljoner dollar innan de fortsatte att samla in data). Google köper sig fria, men de rättsliga påtryckningarna har inte lämnat techjätten helt oberörd. Google Analytics har i princip förbjudits i flertalet länder[56] och tredjeparts-cookies har varit under legal press[57], vilket fått Google att åtminstone försöka fasa ut den typen av datainsamling. Problemet är bara att techbolagen är snabbare än lagstiftarna. Det spelar ingen roll om bolag som Google plockar bort en specifik datainsamlingsteknik eftersom de hittar nya sätt att samla in data[59]. Eftersom det är deras

kärnverksamhet. Som Googles medgrundare Larry Page sa i en intervju redan 2001:[60] ”Personlig information är Googles affär.”

På senare år har Google känt sig tvungna att vidta en del åtgärder för att framstå som att de bryr sig om integritet trots att hela deras affärsmodell bygger på motsatsen. De har bland annat gått ut med att de tar bort data efter ett och ett halvt år[61]. Om vi bortser från det allvarsamma i att i princip alla dina digitala avtryck sparas 18 månader i taget så är ju den återkommande frågan: spelar det någon roll vad Google säger att de gör? När Washington Posts journalist Geffrey A. Fowler hörde av sig till Google och frågade varför de har 167 gigabyte data – eller 83 500 romaner av Stephen King om du så vill – sparat på honom svarade de bara: “We’ve long focused on minimizing the data we use to make our products helpful”[62]. När abortlagarna ändrades i USA sa Google att de proaktivt skulle ta bort ”särskilt personlig” data om ställen som människor besökt[63], som abortkliniker och sjukhus. Ett år efter uttalandet hade det inte infriats[64]. Det tål att upprepas: personlig information är Googles affär. Det innebär inte att de helt kan ignorera sin omvärld. Men det innebär att de sannolikt bara kommer att hantera nya lagkrav och press från allmänheten genom att försöka hitta nya sätt att samla in data. Åtminstone tills de ändrar sin affärsmodell.

Det finns fler techbolag som förtjänar omnämnande. TikTok har blivit anklagade för att samla in mängder med data[65] och dela den med kinesiska staten. De är dessutom tydliga, på sin egen sajt, med att de samlar in till exempel tangenttryckningsmönster och rytmen i hur du skriver[66]. Amazon har avslöjats med att samla in absurt mycket data i både sitt digitala ekosystem[67] och i fysiska butiker[68]. Var dina kreditkortsköp tar vägen[69] vill du knappt veta. Som sagt, den stora delen av internet har förvandlats till en infrastruktur där insamlingen av personlig data är det som används till att öka både intäkter och makt. Det kommer att krävas starkt motstånd för att vända utvecklingen.


COOKIES I VERKLIGHETEN.
Kläder &
JAG TÄNKTE BARA GÅ IN OCH KÖPA ETT PAR STRUMPOR?
INGA PROBLEM, BARA LÄS IGENOM DET HÄR 50-SIDIGA AVTALET OCH VÄLJ HUR DU VILL BLI SPÅRAD.
SKA VI FÖLJA EFTER DIG I BUTIKEN, REGISTRERA DINA KÖPVANOR ELLER KANSKE LÅTA ETT HELT GÄNG AV VÅRA AFFÄRSPARTNERS SPIONERA PÅ DIG?
WWW.MAXGUSTAFSON.SE

DEN KOMMERSIELLA MASSÖVERVAKNINGEN: AKTÖRERNA BAKOM DATAINSAMLINGEN

Här är bolagen som kartlägger ditt liv.

Del 2: Data brokers – du har aldrig hört talas om dem. De vet det mesta om dig.

Det är inte bara de stora techbolagen som sysslar med kommersiell massövervakning. Det finns företag som verkar i det dolda, med ett enda syfte: att samla in, köpa och sälja data om din aktivitet online. Listorna de lägger ut till försäljning är ingen rolig läsning.

Om du går in på en hemsida för första gången, och istället för att klicka acceptera trycker på hantera cookies när den där störiga cookie-varningen dyker upp, då kan du gå igenom en lista på de (ofta) hundratals företag som har cookies eller andra spårningstekniker representerade på sidan. Du kanske förväntar dig att hitta bolag som Meta och Google här, och det gör du, tillsammans med flera andra världsföretag som Amazon, Twitter, Microsoft och så vidare. Men om du bara scrollar ett par gånger dyker det upp namn som inte klingar lika välkänt: Kochava, Veraset, Cuebiq, Spectus, X-Mode … listan tar i princip aldrig slut. Det här är så kallade data brokers. Bolag som

uteslutande ägnar sig åt en enda sak: att samla in, köpa och sälja information om ditt internetbeteende.

Data brokers erbjuder alltså ingen social media eller någon annan app i utbyte mot att samla in data om dig. De driver inte någon sajt där de säljer annonser. De handlar med data, det är allt. Och som de handlar. Acxiom är en av de stora aktörerna. Redan 2018 hade de data på mer än 700 miljoner personer och de har själva skrutit om att kunna erbjuda fakta om allt från människors inkomst, civilstånd och intressen till vilka matbutiker de handlar i och om deras köksutrustning behöver bytas ut[70].

Data brokers sålde information om hur barn rört sig i den fysiska världen, om vilka människor som besökt kliniker kopplade till graviditet samt listor på människor med beroendeproblematik.

De här aktörerna spårar alltså dig via tredjeparts-tekniker på var och varannan sajt. På ett sätt är data brokers det ultimata beviset på vad internet förvandlats till. Varenda gång de dyker upp i en cookie-lista är de en påminnelse om att ditt surfande övervakas. Låt oss använda Acxiom som exempel igen: de säger själva att de har 1 500 olika informationspunkter på var och en av de 200 miljoner amerikaner som de har i sina system. Den mängden data har de inte bara fått in genom att själva spåra människor via cookies och andra tekniker på hemsidor. Det är en total datamängd som de tillförskaffat sig genom att även köpa data från andra aktörer. Data brokers köper och säljer data sinsemellan, men de köper också data från andra typer av tech-

bolag; till exempel genom att köpa information om din aktivitet i olika appar. 2021 avslöjades det att data brokers hade köpt location data från Life360[71], en app där 33 miljoner föräldrar håller koll på var deras barn befinner sig genom att spåra barnens telefoner. Man undrar ju varför data brokers ska ha koll på var miljontals ungar befinner sig och till vem de säljer just den data. Men det är bara ett exempel på vilken rutten marknad detta är. Det finns fler exempel, framförallt om vi tar en titt på vilken typ av data som data brokers säljer vidare.

2022 stämdes bolaget Kochava för att de spårat hundratals miljoner människor och sålt känslig data om var de befunnit sig[72]. I datan som Kochava sålde gick det bland annat att identifiera personer som besökt beroendekliniker, religiösa institutioner och skyddshem för människor som blivit utsatta för våld i hemmet. Vice har rapporterat[73] om att det för ynka 160 dollar gick att köpa en hel veckas register över vilka människor som besökt en specifik klinik kopplat till graviditet – det gick även att se var besökarna kom från och var de tog vägen efteråt. Det här är data som vem som helst kan köpa. Även staten. Det har framkommit att myndigheter köpt uppgifter om människors immigrationsstatus[74], religiösa uppfattning och sexuella läggning. Redan 2013 gick det att köpa register med polisers adresser[75], uppgifter om människor som våldtagits och listor på människor med drog- och alkoholberoenden.

I en klassisk 60 minutes-intervju[76] gav Tim Sparapani, Facebooks första Director of Public Policy, tittarna en inblick i hur data brokers handlar och hur marknaden ser ut (Meta köper ju en hel del data från dessa data brokers[77]). Vi avslutar den här texten med att lyfta en del av konversationen rakt av.

Tim Sparapani: Du kan köpa listor på människor i Amerika som lider av en viss sjukdom eller ett visst tillstånd.

Steve Kroft: Alkoholism?

Tim Sparapani: Ja, absolut.

Steve Kroft: Depression?

Tim Sparapani: Tveklöst.

Steve Kroft: Psykiska problem?

Tim Sparapani: Utan tvekan.

Steve Kroft: Genetiska problem?

Tim Sparapani: Ja. Cancer, hjärtsjukdomar, vad som helst, ner till minsta lilla sällsynta och oväntade sjukdom.

Steve Kroft: Sexuell läggning.

Tim Sparapani: Så klart.

Steve Kroft: Hur avgör de det?

Tim Sparapani: Genom en serie av datapunkter som de köper och säljer. Vilka klubbar du frekvent besöker, vilka barer och restauranger du gör köp på, vilka produkter du köper online.

Steve Kroft: Och allt det här kan hamna i en fil som kanske säljs till en blivande arbetsgivare?

Tim Sparapani: Ja, det inte bara kan hamna där Steve, det gör det.

Steve Kroft: Med all den här informationen och med ditt namn längst upp?

Tim Sparapani: Ja, exakt så.

Ashkan Soltani (**privacy- och tekniкspecialist**)**:** Hemsidor registrerar IP-adresser och det är inte svårt för data brokers att matcha det mot andra identifieringspunkter. Det finns speciella bolag som jobbar med det.

Steve Kroft: Så du kan kombinera den här datan med annan data som finns tillgänglig och räkna ut vem någon är?

Ashkan Soltani: Det är korrekt.

DEN KOMMERSIELLA MASSÖVERVAKNINGEN: TEKNIKEN BAKOM DATAINSAMLINGEN

Så går det till när den kommersiella massövervakningen samlar in din data och kartlägger ditt liv.

De stora techbolagen följer varje steg du tar oavsett om du använder deras tjänster eller inte. Men hur går det egentligen till när de roffar åt sig ditt beteende och placerar det i stora AI- och maskininlärningssystem för att bygga en profil på dig? Här är metoderna bakom övervakningen.

Hur fungerar tekniken som används när stora techbolag som Meta och Google samlar in data om i princip all världens internetanvändare? Innan vi svarar på den frågan behöver vi konstatera ett par saker. 1) Använder du de stora techbolagens tjänster är det lika med att frivilligt ge bort data. Om du till exempel använder Facebook samlar Meta in din aktivitet där. Om du använder Chrome registrerar Google varenda steg du tar i webbläsaren[78]. Och nej, incognito mode räddar dig inte[79]. 2) Du behöver inte ens använda de stora techbolagens tjänster för att de ska ha koll på hur du beter dig online. De når långt utanför sin egen användarbas när de samlar in data.

Nu ska vi fokusera på punkt 2, eftersom den typen av massövervakning sker utan att människor är medvetna om den och utan att de gett sitt medgivande till den.

Vi kommer att gå igenom de tekniker som används för att säkerställa att det är just du som besöker en viss sajt eller gör en specifik sökning. De här verktygen är livsviktiga för de stora techbolag som samlar in data. Det säger sig själv: de måste ha koll på att det är du och ingen annan som återkommer till en viss sajt, de måste vara säkra på att det är du som gjort den senaste googlingen för att kunna lägga den i rätt hög. Identifieringen är nyckeln för att kunna bygga en profil på dig. När de väl vet att det är du som är ute och surfar sätter de igång det stora maskineriet: in med allt du gör i stora AI- och maskininlärningssystem som registrerar, kategoriserar och analyserar ditt beteende. Så att de kan förutse vad du ska göra härnäst, så att de kan försöka påverka dig i en viss riktning för kommersiell eller politisk vinning. Låt oss nu börja med den mest använda identifieringstekniken: din IP-adress.

Din IP-adress – det vanligaste och enklaste sättet att identifiera dig.

Alla som har ett internetabonnemang har blivit tilldelad en IP-adress av sin internetoperatör. Det här ingår i internets själva grundstruktur. Alla hemsidor du besöker har också en IP-adress och det är IP-adresserna som ser till så att trafiken hamnar rätt när den skickas fram och tillbaka. Det här är ju bra (du vill ju att internet ska fungera), men det innebär också att vi alla bär på ett digitalt ID-kort som internetleverantörer kan använda för att registrera alla sidor du besöker. Den här loggningen är de tvingade att göra enligt lag i väldigt många länder. Tanken är att detaljer om internettrafiken och uppgifter om vem som finns bakom en viss IP-adress ska kunna lämnas ut ifall en myndighet skulle fråga (till exempel om polisen kräver det i samband med en ut-

redning). Men det stannar ju inte där. Beroende på vilket land du befinner dig i är det mer eller mindre troligt att internetleverantörerna i praktiken ger myndigheter kontinuerlig tillgång till trafiken oavsett om ett lagbrott begåtts eller ej. Eller till och med säljer ditt beteende online för att tjäna pengar[80].

Dessutom finns det fler anledningar till att dölja sin IP-adress (via en VPN), eftersom IP-adressen används i flera andra sammanhang för att identifiera, spåra och kartlägga din aktivitet. Stater använder sig av IP-adresser när de tjuvlyssnar på allas vår trafik genom att helt enkelt koppla in sig på de stora internetkablar som fysiskt går mellan länder. Och inte minst använder sig techbolag av IP-adresser när de massövervakar människor i kommersiellt syfte.

När stora techbolag och data brokers tar till olika tekniker för att förfölja dig från sajt till sajt för att kartlägga ditt rörelsemönster på internet, då är det bland annat din IP-adress som används för att identifiera dig. Samma sak när de i detalj studerar vad du gör på varje sajt (vilka texter du läser, vilka bilder du stannar till vid, vilka köp du gör, vilka produkter du snabbt bläddrar förbi, vilka videor du tittar på och så vidare). IP-adressen används för att knyta samman aktiviteten och person.

Vi kan inte vara tillräckligt tydliga här: IP-adressen är som att sträcka upp handen och säga ”här är jag”. Det är det enklaste sättet att spåra dig på internet. Och det enda sättet att dölja din IP-adress, och få bort den som ett digitalt ID-kort, är att använda en trovärdig VPN (eller Tor-nätverket). Det här är själva grunden till att Mullvad startades en gång i tiden (2009).

Tredjeparts-cookies – spårning som du accepterar (för att du egentligen inte har något val).

Precis som med IP-adresser är cookies en del av hur internet är uppbyggt sedan lång tid tillbaka. Cookies finns på hemsidor för att sidorna ska kunna komma ihåg saker om dig och för att de ska fungera överhuvudtaget. Till exempel: du besöker en e-handel och lägger en produkt i varukorgen, då är det en cookie som kommer ihåg att varan ligger där när du klickar vidare för att gå till kassan. Att du kan vara inloggad på en sajt över tid är tack vare en cookie. När du väljer ett språk på en hemsida är det samma sak; små små textfiler (det är vad cookies är) sparas lokalt på din dator eller telefon och ser till att samma språk dyker upp nästa gång. Cookies gör internet till en bekväm plats att besöka. Så, varför är det då ett sådant liv om cookies? Det är för att det finns olika sorters cookies.

Det finns cookies som är placerade på sajten av den som äger sajten, för att själva hemsidan ska vara användarvänlig. Den här typen av cookies, som vi nämnt ovan, är så kallade förstaparts-cookies. De finns till för att ge funktionalitet åt besökaren. Men sen finns det cookies som är placerade på sajten med ett annat syfte: att registrera ditt besök, åt någon annan än sajtägaren. De här kallas tredjeparts-cookies och de är ofta kopplade till stora techbolag som Meta och Google (eller så kallade data brokers) och eftersom de har tredjeparts-cookies placerade på en majoritet av alla internets hemsidor gör den här typen av cookies det möjligt för dem att bevaka ditt rörelsemönster. När du hoppar från en nyhetssajt till en e-handel till en streamingtjänst är de stora techbolagen där varenda gång med sina cookies. Och det är allt de behöver för att kunna bygga ett enda stort register över vilka sidor du besöker och med hjälp av AI- och maskininlärning bygga en profil av ditt beteende online. Det är den här typen av cookies som gör att annonser förföljer dig på nätet. Det är den här typen av cookies som kartlägger ditt liv.

Du kan säga nej till cookies, men ibland hjälper inte ens det. Det finns så kallade ”nödvändiga cookies” som kickar igång även om du klickar ”reject all”. Bland dem: cookies från de stora techbolagen.

Du kan säga nej till cookies. Alla som någon gång gett sig ut på nätet vet att du måste trycka acceptera, hantera eller avfärda cookies första gången du besöker en sajt. Problemet är bara att infrastrukturen är byggd på ett sätt som innebär att du egentligen inte har något val. Det finns en utbredd cookie-trötthet som gör att vi slentrianmässigt trycker på acceptera för att komma vidare. Ingen människa orkar läsa de närmast oändliga användarvillkoren som det innebär att trycka på hantera cookies. Dessutom är cookie-varningarna designade för att vi ska trycka acceptera. Begreppet dark patterns innebär att *acceptera* kommer med en stor, fet grön knapp och att *hantera cookies* och *avfärda cookies* är mer eller mindre gömda eller otroligt krångliga att ta sig igenom.

Ännu värre: inte ens om du klickar avfärda cookies kan du vara säker på att ditt besök inte registreras av en tredje part. Det finns cookies som är ”nödvändiga”. Du har säkert sett valet *acceptera bara nödvändiga cookies*. Du kanske tänker att ”nödvändiga cookies” är lika med funktionella cookies, men så är alltså inte fallet. Om du klickar dig vidare och börjar läsa de milslånga villkoren hittar du ofta stora bolag under ”nödvändiga cookies”. Och i det finstilta kan du dessutom se att den här typen av cookies också kan kicka in även om du skulle välja avfärda alla cookies. Sajtägaren har nämligen ett

helt nödvändigt samarbete med de stora techbolagen som du inte har en möjlighet att välja bort. Bara en detalj innan vi går vidare: om en hemsida enbart använder sig av funktionella cookies, sådana som det är uppenbart att sidan behöver för att fungera så som den är tänkt att fungera, då behöver man inte ens varna för cookies, då behöver man inte ens ha besökarna till att trycka *acceptera*. Det är därför du slipper den proceduren när du går in på Mullvads sajt.

Så, vad ska man då göra för att inte bli förföljd via tredjeparts-cookies? Det enklaste sättet är att köra en webbläsare som Mullvad Browser, som sköter det och mycket annat åt dig (cookies och IP-adresser är, som du kommer att inse om du läser vidare, inte de enda sätten att spåra dig). Men annars gäller det bara att vara ihärdig och rensa cookies (och cache-minnet) varje gång du använt din webbläsare. Man kan också använda sig av en mängd olika plugin och extensions som blockerar tredjeparts-cookies.

Tredjeparts-cookies har blivit själva symbolen för hur big tech och data brokers kartlägger en hel värld av internetanvändare. Uppmärksamheten kring just den här typen av datainsamling har lett till att Google blivit stämda på hundratals miljoner euro[240] för att ha brutit mot GDPR och till sist kände sig till och med Google tvungna att börja leta efter en utväg. Under flera års tid jobbade på ett nytt trackingsystem[241] som inte skulle bygga på tredjeparts-cookies utan på datainsamling via webbläsaren Chrome[242]. Lanseringen sköts upp gång på gång och till slut meddelade Google att man la ner satsningen.

Även om Google hade lyckats så hade huvudproblemet kvarstått. För det är ju själva datainsamlingen som är problemet, inte exakt hur den går till. Det spelar liksom ingen roll om tredjeparts-cookies försvinner om inte den affärsmodell som internet idag bygger på görs om i grunden.

Så länge inte insamling av beteendedata förbjuds, så länge inte det blir olagligt för företag att samla in data om människor och dela

med sig av den till andra, så kommer inte någon förändring att ske – det enda som förändras är hur datan samlas in.

För det är ju så, även om du maskerar din IP-adress och ser till att blockera eller rensa alla dina cookies från gång till gång, så finns det andra sätt att spåra dig via din webbläsare. Även om tredjeparts-cookies förbjuds, så är det bara en av många tekniker. När cookies försvinner som trackingmetod är det inte otänkbart att det som kallas browser fingerprinting tar över.

Browser fingerprinting – spårningsteknik som sker i det dolda.

När du besöker en sajt så finns det teknik som gör att själva sidan ställer en mängd frågor till din webbläsare: det kan handla om vilken version av webbläsaren du använder, om du kör mobil eller dator, vilket språk du har inställt, vilken tidszon du befinner dig i, vilka olika plugin och typsnitt du har installerat, vad du har för upplösning på din skärm och så vidare. En del frågor handlar också om din hårdvara: till exempel hur snabb din processor är och vilket grafikkort du har inbyggt. Det här är frågor som ställs för att webbläsaren ska kunna presentera sidan på bästa sätt. Precis som med cookies är detta en del av själva grundbulten för att internet ska fungera så användarvänligt som det gör. Problemet är bara att det även ställs en mängd frågor som inte har med funktionalitet att göra, utan som bara finns till för att identifiera och spåra dig. Mängden frågor som ställs och kombinationen av svar gör det möjligt att ta ett unikt fingeravtryck av dig som besökare.

Låt oss avsluta med att konstatera: i tider då tredjeparts-cookies är satt under legal press spelar browser fingerprinting under andra regler. Det är helt enkelt teknik som du inte kan välja bort[81] genom att klicka *avfärda alla*. Spårningen sker helt i det dolda. Och när omvärlden börjar sätta restriktioner för hur de stora techbolagen

övervakar människor via cookies och IP-adresser är det ingen vild gissning att de kommer att använda fingerprinting i ännu större utsträckning i framtiden.

”Varför fingerprinting är ett hot mot integritet online? Det är enkelt. Till skillnad mot cookies och andra spårningstekniker behöver de inte be om lov eller ens berätta att de samlar in data.”

The Tor Project

Övervakning via tredjeparts-scripts – så håller de koll på exakt vad du gör online.

De flesta hemsidor använder sig av scripts (små små bitar av JavaScripts-kod) för att fungera. Scriptsen innebär att sidorna fungerar väldigt bra, men de kan också användas för att övervaka besökarna. Precis som med tredjeparts-cookies blir det ett stort problem när någon annan än ägaren av sajten är inblandad. Om en hemsida använder sig av Google Analytics finns det ett script på sidan från Google. Om en sajt använder sig av ett speciellt typsnitt finns där ett script från font-utvecklaren. Om sidan du besöker använder sig av Meta Pixel för att maximera sina annonsintäkter via Facebook, då har Meta ett script placerat där. Och det är när det finns utomstående scripts på sidorna som de här aktörerna kan räkna ut exakt vad du gör.

En cookie kan bara identifiera dig när du besöker en sajt. Dyker en cookie upp från samma tredjepartsaktör på nästa sida du besöker kan de börja följa dig på nätet och bygga en profil på hur du rör dig. Samma sak med IP-adressen. Det är unika ID-kort för att säkerställa att det är du som är på plats. När det kommer till scripts är det lite annorlunda. De kan användas för att bygga ett browser fingerprint på dig och på så sätt identifiera dig. Men framförallt kan de användas för att ta en närmare titt på exakt vad du gör på sidan. Scripts kan ta reda på exakt vilka minuter av videon du tittar på (och inte bara att du besöker Youtube igen). Scripts kan läsa av hur du scrollar på en sida, vilka annonser du stannar till vid, om du har läst hela artikeln eller gått vidare efter halva. Det var scripts som användes när Facebook samlade in vad människor hade skrivit i kommentarsfält men sen suddat ut och aldrig postat[82]. Det räcker med metadata, alltså den data som samlad bygger en profil på hur du rör dig online, för att kartlägga en persons liv. Men med scripts läggs ett extra lager till.

Det går som sagt att blockera tredjeparts-scripts och med Mullvad Browser finns det teknik för det. Men det är viktigt att komma

ihåg: om en datainsamlare lyckas registrera exakt vad du gör på en sajt via scripts behöver de fortfarande identifiera att det är just du som är på besök för att det ska få någon effekt. Om du maskerar din IP-adress via en trovärdig VPN och använder en webbläsare som ser till att det blir svårt att identifiera dig via cookies och fingerprints, då spelar det ingen roll hur exakt de än kan mäta vilka delar av Youtube-videon du gillade mest, de vet ändå inte att det är du.

Sofistikerad AI kommer med helt nya hot. Därför måste vi redan idag tänka på hur vi kan motarbeta morgondagens massövervakning.

Sofistikerad AI-teknik innebär nya hot.

Att använda en trovärdig VPN och en privacy-fokuserad webbläsare är ett enkelt sätt att motarbeta den datainsamling som sker via metoderna vi nämnt i den här texten. Man ska dock komma ihåg att utvecklingen går snabbt och att de som är intresserade av att massövervaka ständigt jobbar på nya tekniker för det. Ett växande hot är det som kallas för trafikanalys.

När du besöker en hemsida sker ett utbyte av nätverkspaket. De här datapaketen skickas fram och tillbaka mellan dig och webbplatsen du besöker. Det är så internet är uppbyggt i grunden. Och det faktum att paketen skickas, hur ofta de skickas och själva storleken på dem – allt detta är något som är synligt för din internetleverantör oavsett om du använder en VPN (eller Tor) eller inte.

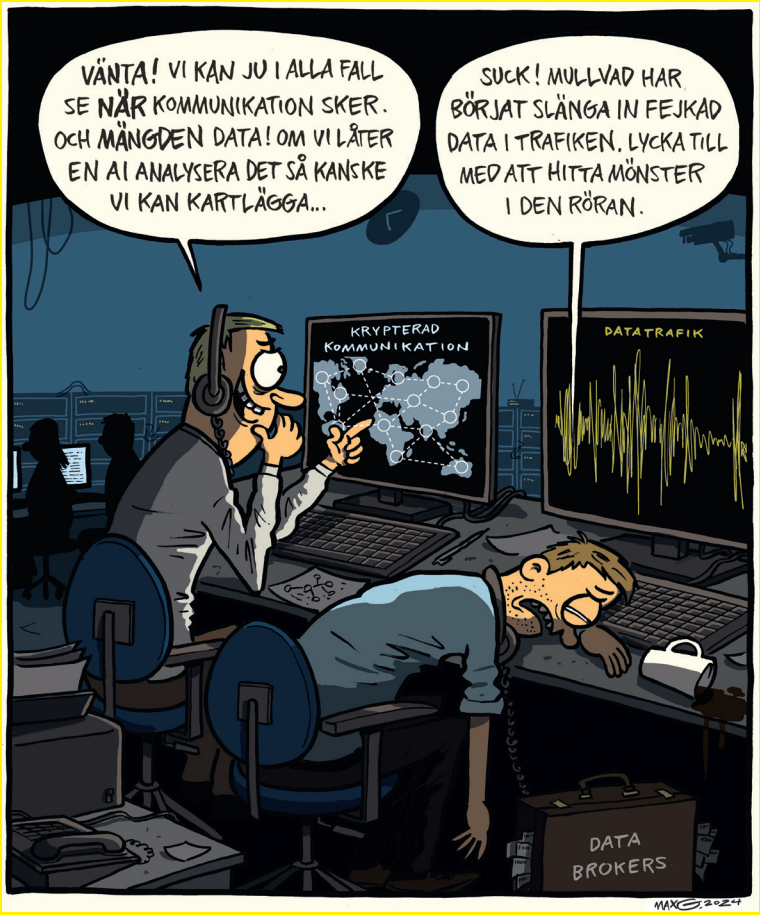
Varje webbplats genererar ett specifikt mönster av datapaket som skickas fram och tillbaka (beroende på hur sidan är uppbyggd med bilder, textblock, filmer, etc.), vilket innebär att din internetleverantör (eller vem som helst som har tillgång till din internetleverantör) kan ta en titt på det här mönstret av datapaket och försöka analysera det för att räkna ut vilka hemsidor du besöker, men också för att ta reda på vem du kommunicerar med genom att använda en så kallad korrelationsattack (du skickar ett meddelande med ett speciellt mönster vid ett givet tillfälle, till någon som tar emot just det trafikmönstret vid samma tidpunkt).

Det här är avancerade attacker, men med tanke på hur snabbt utvecklingen går med artificiell teknik och dess möjligheter att analysera stora mängder data är det ett växande hot.

Mullvad har därför utvecklat DAITA (Defense against AI-guided Traffic Analysis) som är ett försvar mot den här typen av trafikanalyser med hjälp av AI. Tillsammans med Karlstad Universitet har vi tagit fram teknik som går att slå på i vår VPN-app och som ser till att

datapaketen som skickas alltid är av samma storlek, och som dessutom skickar ut fejkade paket.

På samma sätt har vi tillsammans med forskare utvecklat VPN-tunnlar som kan stå emot framtidens kvantdatorer (som riskerar att kunna knäcka kryptering). Vi vet inte hur den här typen av teknik kan komma att användas för massövervakning av hela befolkningar i framtiden, och därför måste vi jobba på motmedel idag.


VÄNTA! VI KAN JU I ALLA FALL SE NÄR KOMMUNIKATION SKER. OCH MÄNGDEN DATA! OM VI LÅTER EN AI ANALYSERA DET SÅ KANSKE VI KAN KARTLÄGGA...
SUCK! MULLVAD HAR BÖRJAT SLÄNGA IN FEJKAD DATA I TRAFIKEN. LYCKA TILL MED ATT HITTA MÖNSTER I DEN RÖRAN.
KRYPTERAD KOMMUNIKATION
DATATRAFIK
DATA BROKERS
MAX 2024

DEN KOMMERSIELLA MASSÖVERVAKNINGEN: INSAMLAD DATA GÅR INTE ATT HÅLLA ANONYM

De som samlar in data påstår ofta att den är anonym. Forskningen visar att det är omöjligt.

När de stora techbolagen samlar in mängder med data om ditt internetbeteende gömmer de sig alltid bakom försvarstal som ”det är bara metadata” eller ”vi har anonymiserat informationen”. Men samlar du in big data är den omöjlig att hålla anonym. Det räcker att din telefon avslöjar fyra platser du varit på för att räkna ut att det är just du.

När stora techbolag samlar in data om människor har de två standard-bortförklaringar. Den första är: ”det är bara metadata”. De menar alltså att det inte är någon fara eftersom de inte samlar in själva konversationen mellan människor (vilket de också gör) eller något annat konkret (i deras ögon). Men som vi redan konstaterat: metadata lika med att kartlägga någons liv. Då brukar de gå vidare med att säga: ”vi har anonymiserat datan”. Och så berättar de om hur de kastat om siffrorna i en IP-adress eller helt enkelt dolt den. Eller tagit bort annan information som går att koppla till en viss person.

Men faktum är: om du samlar in tillräckligt mycket data är den omöjlig att hålla anonym. Och eftersom hela affärsmodellen hos de stora techbolagen bygger på big data innebär det att ditt internetbeteende utan tvekan går att koppla till dig som person. Till att börja med: har du tillgång till olika databaser och kan samköra dem går det fort att av-anonymisera människor. Som när Netflix släppte tio miljoner filmbetyg från en halv miljon anonyma användare och ett gäng forskare på University of Texas[83], som för att bevisa själva poängen, lyckades identifiera flera av dem bara genom att jämföra betygen (och vilken tid de sattes) med betyg som publicerats publikt på IMDb. Ett annat exempel: när The State of Washington sålde hälsodata om anonyma patienter för 50 dollar styck[84] och forskare på Harvard kunde sätta namn på flera av dem genom att jämföra delar ur journalerna med nyhetsartiklar om olyckor och våldsbrott.

Det är svårt att identifiera en person om du bara har tillgång till en eller två datapunkter. Men så fort du får tillgång till fler går det att använda sig av klassisk uteslutningsmetod för att räkna ut vem som finns bakom informationen. Kryptografen och säkerhetsexperten Bruce Schneier ger i sin bok Data and Goliat ett bra exempel: FBI behövde spåra en person som skickat anonyma mejl från olika IP-adresser. När de tog en titt på IP-adresserna visade det sig att de alla tillhörde olika hotell. Personen hade alltså varit noga med att byta hotell varje gång det var dags att mejla. Men då var det bara för FBI att plocka ut kundregister från de olika hotellen. Var det någon person som checkat in på samtliga av de där hotellen vid tidpunkterna för mejlutskicken? Det krävdes inte många hotellnätter förrän listan var nere på en enda person.

Forskningen har flera gånger om bevisat att det inte krävs många datapunkter för att identifiera människor. Allra snabbast går det om du har tillgång till location data, om du alltså har tillgång till flera platser som en anonym person har besökt. Fundera på det själv: Ni

är kanske några stycken på din arbetsplats, men hur många av dem handlar på samma matbutik som du? Ni kanske är ett par stycken som matchar på båda dessa punkter. Men lägg till ett par till så är saken klar. Forskare på universitet i Storbritannien och Belgien har publicerat metoder som säger att det är möjligt att identifiera 99.98 procent av alla personer på anonyma listor[85] om det bara finns 15 demografiska attribut. Ett annat forskargäng menar att det räcker med fyra mätpunkter – om de innehåller plats och tid – för att identifiera 95 procent[86] av individerna. I ytterligare en studie studerade forskare tre månaders kreditkortsuppgifter[87] för att komma fram till att det räckte med fyra punkter – återigen gällande plats och tid – för att identifiera 9 av 10.

Forskare tog sig an sökhistoriken från 657 000 användare. Det fanns bara ett nummer kopplat till varje lista med sökningar. När de var klara hade de bytt ut nummer mot namn.

Med tanke på hur mycket data som samlas in om var och en av oss så fort vi startar en webbläsare så behöver de som vill använda datan (och av-anonymisera den) knappast förlita sig på parametrarna plats och tid. Bruce Schneier berättar bland annat om när forskare tog sig an sökhistoriken från 657 000 användare. Totalt handlade det om 20 miljoner sökningar och informationen var, som det heter, anonymiserad. Det fanns bara ett nummer kopplat till varje lista av sökningar. Men genom att korrelera olika uppgifter kunde forskarna byta ut nummer mot namn. Återigen: ditt internetbeteende är spårat och loggat i detalj. Det krävs ingen längre stund av uteslutningsmetoden för att skala ner det till just dig.

DEN STATLIGA MASSÖVERVAKNINGEN

Demokratiska och auktoritära länder tävlar i vem som kan massövervaka flest och bäst (värst).

USA och deras vänner i övervakningsalliansen 14 Eyes har visat att de har kapaciteten, viljan och erfarenheten av att bevaka vem de vill, när de vill, var som helst i världen. Kina och andra totalitära länder använder massövervakning för att kontrollera sina invånare. Inte sällan framstår det som att det pågår en dystopisk kapprustning runt om i världen. Men vem är egentligen bäst (värst) på att göra verklighet av George Orwells 1984?

Det finns två typer av massövervakning. Den kommersiella som vi redan har gått igenom. Och den som bedrivs av stater och makthavare. Båda varianterna är förkastliga och vår inställning är grundmurad: massövervakning bryter mot de mänskliga rättigheterna[88], inkräktar på den personliga integritet som fria samhällen bygger på, och dessutom är den ineffektiv mot de problem som man brukar påstå att den löser. Det här är själva kärnan i vår verksamhet. Vi bildades år 2009 för att övervakningslagarna gick i fel riktning, och vårt budskap till

makthavare världen över är detsamma nu som då: Det är skillnad på övervakning och massövervakning. Syssla inte med det senare; massövervaka inte er eller andra länders befolkning. Utan rikta endast övervakning vid misstanke om brott, på ett proportionerligt sätt och via oberoende domstolsbeslut.

Vi tycker att de mänskliga rättigheterna är värda att bevara och försvara. Och det är viktigt att komma ihåg att de finns till för att skydda folket mot staten. De är ett riktmärke att hålla fast i för att de värsta delarna ur historien inte ska upprepas. De finns till för att människor och makthavare tar dåliga beslut. För att regeringar byts ut. För att en stat inte ska ha total och okontrollerbar makt. I grund och botten handlar det om att staten faktiskt ska finnas till för folket och inte tvärt om.

Även om en stor del av dagens massövervakning är global, så utgår den från olika länder och skiftar beroende på vilket land du bor i. Låt oss därför gå igenom några av de tydligaste exemplen på hur utbredd den blivit i stora delar av världen.

USA – med kapacitet och erfarenhet av att övervaka all världens befolkning.

Det finns ett problem med att redogöra för massövervakningen som sker av länder som USA (åtminstone om man vill hålla sig till bevisad fakta): de är inte särskilt förtjusta i att berätta om den. Det finns så klart undantag. Som när uppblåsta chefer som CIA-bossen Ira Gus Hunt håller presentationer och skryter inför journalister om hur "we try to collect everything and hang onto it forever"[89]. Eller som när en chef på Pentagon förklarade att inte ens deras anställda kan förvänta sig att få ha sitt privatliv ifred: "De ska inte göra några falska antaganden om anonymitet. Du är inte anonym på den här planeten, inte vid den här tidpunkten av vår existens. Alla går att övervaka, alla är spårbara, alla går att upptäcka."

Och ibland säger ett bygge mer än tusen ord, som när NSA smäller upp enorma serverhallar ute i Utah-öknen för att lagra data[90].

Men för att få massövervakningen i svart på vitt, för att få fram hårda fakta och siffror, krävs det modiga visselblåsare som Edward Snowden. Det är bara via den typen av hjältar som vi får en inblick i hur det verkligen ligger till. Till dags datum har vi inte fått ett bättre facit än det Snowden gav oss 2013. Vi hade hoppats på förändring efter hans avslöjanden, men tyvärr är de relevanta än idag, så därför börjar vi där.

Snowdens visselblåsning visade att amerikanska myndigheter övervakade hundramiljontals människor över hela världen – varje dag.

Den amerikanska massövervakningen är möjlig tack vare section 702 i the Foreign Intelligence Surveillance Act (FISA)[91], en lag som USA förnyar var femte år. Det är section 702 som är själva nyckeln till att amerikanska myndigheter inte behöver något domstolsbeslut för att övervaka människor. Lagen kom till under förevändningen att terrorister skulle jagas efter 11 september-attackerna, och ska egentligen ”bara” gälla avlyssning av icke-amerikanska medborgare, men så som lagen är skriven och så som internet är uppbyggt innebär den i praktiken övervakning av såväl utländska som amerikanska medborgare. När Snowden visselblåste visade det sig dessutom att den inte bara används mot människor som är misstänkta för något brott, utan att den amerikanska administrationen massövervakat miljontals människor[92]. Andra dokument som Snowden läckte demonstrerade

hur National Security Agency (NSA) hade kapaciteten att övervaka i princip varenda människa i hela världen och att de inte sparat på krutet; bland annat visade dokumenten att de samlade på sig 200 miljoner textmeddelanden[93] från olika delar av världen – varje dag.

I programmet XKeyscore hade NSA:s analytiker tillgång till en databas som täckte ”nearly everything a typical user does on the internet”[94]. Det inkluderade både direkt data som mejlen i människors inkorgar, chattkonversationer och privata meddelanden på Facebook. Men också det som klassas som metadata; sökhistorik och exakt vilka sidor som miljontals människor besökte. I XKeyscore kunde analytikerna – utan beslut från vare sig domstol eller överordnade – göra sökningar på människors internetbeteende[95]. Antingen genom en så kallad hård sökning: via till exempel en ip-adress eller e-postadress – då kunde de få tillgång till i princip allt en specifik person gjorde online. Eller via en så kallad mjuk sökning: via en sökning på nyckelord och fraser – då kunde de få fram listor på människor med ett visst internetbeteende. Snowden visade världen hur enkelt det var för NSA att söka i XKeyscore och hur mycket de kunde få fram i programmet. Men var kom all data ifrån?

Section 702 innehåller två delar som ger amerikanska myndigheter som FBI, CIA och NSA tillgång till enorma mängder data och de går under kodnamnen Prism (downstream) och Upstream[96].

Prism innebär att de har rätt att kräva in data från amerikanska bolag utan domstolsbeslut. Om myndigheterna har fritt spelrum att begära ut uppgifter från världens största teknikbolag är det inte konstigt att det slutar med massövervakning. Men Snowden avslöjade att situationen var ännu värre. I de läckta dokumenten framgick det att myndigheterna inte ens behövde göra förfrågningar för att få ut material, utan att de mer eller mindre hade direkttillgång till system och servrar[97] hos techbolagen. Som Snowden skrev i sin bok Permanent Record: ”Prism gjorde det möjligt för NSA att rutinmässigt

samla in data direkt från Microsoft, Yahoo, Google, Facebook, PalTalk, Youtube, Skype, AOL och Apple, inklusive e-post, foton, video- och ljudchattar, webbrowserinnehåll, sökmotorfrågor och alla andra data lagrade i deras moln."

Att FBI, CIA och NSA hade direkttillgång till system och servrar förnekades förstås av samtliga teknikbolag på listan. Vilket i och för sig kanske inte var så konstigt, eftersom själva lagen i sig kan innebära att det är olagligt för bolagen att erkänna inblandning[98].

"Systemen reagerade på sökord som 'anonym internetproxy' eller 'protest'. Sen avgjorde algoritmer vilka av byråns attackmetoder som skulle användas. När den skadliga koden placerats fick NSA tillgång till din dator. Hela ditt digitala liv tillhörde nu dem."

Edward Snowden

Medan Prism gav NSA rätten att kräva ut data från amerikanska bolag som Microsoft, Facebook och Google, så gav Upstream[99] dem rätten att koppla upp sig direkt på själva linan hos de amerikanska telefon- och internetleverantörerna. Det här gällde stora amerikanska telekombolag som AT&T[100] men också världens största routertillverkare som byggde in övervakning åt NSA i sina produkter[101]. Snowden igen:

”Man kan hävda att detta var ännu mer inkräktande. Det möjliggjorde en rutinmässig uppfångning av data direkt från den privata internetinfrastrukturen, de switchar och routrar som skickar internettrafik fram och tillbaka över världen via satelliterna i omloppsbana och de fiberoptiska kablar som dragits under haven.”

Det ska mycket till för att den globala internettrafiken inte ska ta vägen via amerikanska servrar, kablar och tjänster. Det är så den digitala infrastrukturen och styrkeförhållandena ser ut. Prism och Upstream gav därför amerikanska myndigheter möjligheten att övervaka i princip varenda människa på jorden. Snowden visade att de kunde söka i historiken men också övervaka i realtid. För att hantera den datamängden krävdes sortering, vilket gjordes via programmen Turmoil och Turbine. I Permanent Record skrev Snowden:

”Man kan säga att de hade en vakt placerad vid en osynlig brandvägg genom vilken internettrafiken måste passera. När den ser din begäran, kontrollerar den dess metadata för selektorer eller kriterier, som markerar det som förtjänar närmare granskning. Dessa selektorer kan vara vad som helst som NSA väljer, vad som helst som NSA finner misstänkt: en viss e-postadress, kreditkorts- eller telefonnummer, det geografiska ursprunget eller destinationen för din internetaktivitet, eller bara vissa sökord som ’anonym internetproxy’ eller ’protest’. Om Turmoil flaggar din trafik som misstänkt slår den över till Turbine, som avleder din begäran till NSA:s servrar. Där bestämmer algoritmer vilka av byråns attackmetoder, program för skadlig

kod, som ska användas mot dig. När väl den skadliga koden finns på din dator får NSA tillgång inte bara till dina metadata utan även till din dator. Hela ditt digitala liv tillhör nu dem."

Snowdens visselblåsning avslöjade att de amerikanska myndigheterna lyssnade in sig på människors samtal, läste deras meddelanden och till och med tog en titt rakt in i deras hem via kamerorna i datorer och telefoner. Ändå är det vanligt att statliga massövervakare nekar det och försöker gömma sig bakom frasen "vi samlar bara in metadata". Som om det inte vore illa nog. Den amerikanske kryptografen och säkerhetsexperten Bruce Schneier beskriver det så här i sin bok Data and Goliat:

"I en meddelandetjänst är själva meddelandet datan. Men kontona som skickade iväg och tog emot meddelandet, tiden som meddelandet skickades, allt det där är metadata. I ett e-postsystem är det på samma sätt: texten i mejlet är data, men sändaren, mottagaren, routing data och storleken på meddelandet är metadata. Metadata kanske låter ointressant, men det är allt annat än ointressant. Att samla in människors metadata är att sätta dem under övervakning. Avlyssning ger dig alla konversationer. Metadata ger dig allt annat. Metadata avslöjar vilka som är dina nära vänner, vilka affärsrelationer du har, vem du är intresserad av och vad som är viktigt för dig. Oavsett hur privat det är."

Under metadata sorteras även alla hemsidor du besöker och hela din sökhistorik in och plötsligt framstår försvarstalet "vi samlar bara in metadata" som ganska tunt. Stewart Baker, tidigare general counsel på NSA, uttryckte det med tydlighet:[102] "Metadata säger precis allt om någons liv. Om du har tillräckligt mycket metadata så behöver du egentligen inte själva innehållet."

När Snowden bestämde sig för att visselblåsa var han helt övertygad om att han var tvungen att få tag i rätt journalister för jobbet. Frågan var vilka som var bäst lämpade. Han funderade länge. Skissade

på olika kriterier och scenarion. Försökte resonera sig fram. Men sen insåg han att det var bättre att låta NSA-systemet välja åt honom. Givetvis gick det att slå in ett gäng väl valda sökord för att få fram en lista på journalister som var kritiska till USA:s massövervakningssamhälle. Systemet sorterade bland annat fram Laura Poitras[103] och Glenn Greenwald,[104] som var två av de journalister som till slut mötte Snowden på det där hotellrummet i Hongkong.

Att NSA övervakade journalister var inte särskilt konstigt. Den amerikanska övervakningsapparaten avlyssnade ju inte bara terrorister och brottslingar. De sysslade med industrispionage[105] och övervakade rättighetsorganisationer som Amnesty och Human Rights Watch[106]. De lyssnade inte bara på hundratals miljoner amerikaner utan plockade till exempel upp 70 miljoner franska telefonsamtal i månaden[107]. Givetvis användes systemet till att övervaka politiker och världsledare[108].

Vi har inte fått en lika bra inblick i hur de amerikanska myndigheterna jobbar sedan Snowdens visseblåsning. Vi vet inte exakt hur de massövervakar idag. Men section 702 har förlängts. Och för varje år som gått sedan 2013 har det kommit fler och fler uppgifter om hur NSA, CIA och FBI håller fast vid sin taktik att inte bara övervaka misstänkta människor, utan massövervaka hela befolkningar.[109]

2017 fick vi i alla fall en ny inblick i den amerikanska massövervakningsapparaten. Läckan var långt ifrån lika omfattande som Snowdens, men det var uppenbart att massövervakningen hade fortgått när Wikileaks avslöjade att CIA hackade sig in i människors mobiler, datorer och tv-apparater[110] för att massövervaka. Och den här gången förnekade inte ens de kommersiella samarbetspartnerna upplägget[111]: ”If your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition”, som Samsung uttryckte det.

”End-to-end-kryptering var en önskedröm 2013. På den tiden var en stor del av den globala internettrafiken helt naken. Nu är det sällsynt. Men kapaciteten myndigheterna hade 2013 framstår som rena barnleken jämfört med idag.”

Edward Snowden

Citatet var som taget ur George Orwells 1984-dystopi med dess teleskärmar, som både kablade ut propaganda och lyssnade av sin befolkning.

2023 gav Snowden sin bild av hur världen förändrats, tio år efter hans visselblåsning[112]. Han pratade om hur hans avslöjanden fått teknikbolag att införa end-to-end-kryptering och att det på många sätt inte är lika lätt för myndigheter idag att rakt upp och ner lyssna av all kommunikation på internet. Samtidigt har den tekniska kompetensen och utvecklingen gått fort, även på andra sidan. Som Snowden uttryckte det:

”Om vi jämför kapaciteten som fanns 2013 med den som regeringar sitter på idag, då framstår 2013 som rena barnleken. Idén om att avslöjandet 2013 skulle följas av regnbågar och enhörningar dagen därpå var inte realistiska. Det är en pågående process. Och vi kommer att vara tvungna att fortsätta jobba på den processen under resten av våra liv, under våra barns liv och bortom det.”

Tioårsjubileet av Snowdens visselblåsning uppmärksammades brett och de flesta var överens om att den globala massövervakningen knappast upphört, utan att den bara hittat nya vägar.[113]

Bland annat har det framkommit att FBI och andra trebokstavsmyndigheter köpt insamlad data från data brokers[223]. Varför köper amerikanska myndigheter, som ju har undantagstillstånd att övervaka människor utan domstolsbeslut, data från data brokers? Till att börja med behöver de, när de köper datan, inte skylla på att övervakningen av amerikanska invånare ”råkat hänga med i övervakningen av utländska hot”. Men gissningsvis handlar det också om att den kommersiella datainsamlingen blivit så utbredd och inkräktande att det är billigare och smidigare för myndigheter att helt enkelt köpa in datan istället för att själva göra jobbet. Som en konsult för den amerikanska regeringen uttryckte det i en artikel som handlade om hur de amerikanska myndigheterna använt datainsamlingen via

appar för att spåra några av Putins närmaste män[224]: ”Inget ekosystem i historien har samlat in lika mycket information som tekniken bakom annonsnätverken.”

Eller som Michael Morell, tidigare direktör på CIA, kommenterade det[225]:

”Informationen som är kommersiellt tillgänglig är häpnadsväckande. Om vi hade samlat in det genom traditionella underrättelsemetoder hade det varit top secret-känsligt, och vi hade inte lagt det i en databas, vi hade bevarat det i ett kassaskåp.”

Anledningen till att CIA hade tvingats smussla med det är solklar; det beror på att myndigheter egentligen inte får bedriva den här typen av datainsamling enligt den amerikanska konstitutionen (sen att de gör det ändå via undantagslagen section 702 är en annan sak).

Att amerikanska myndigheter köpt stora mängder data från data brokers har de senaste åren bidragit till en allt hetsigare diskussion kring just section 702 – undantagslagen som amerikanerna förlänger vart femte år och som gör det möjligt för myndigheterna att massövervaka utan domstolsbeslut. Senator Ron Wyden har varit en av de mest högljudda kritikerna och uppmanat regeringen[226] att ”sluta finansiera och legitimera en skum industri vars kränkningar av amerikaners personliga integritet inte bara är oetisk utan även olaglig.”

Debatten blev som livligast under 2023, när det åter var dags att förnya section 702 i ytterligare fem år. Representanthuset misslyckades tre gånger om att klubba igenom en förlängning och tvingades skjuta upp beslutet till våren 2024. Samtidigt kom det förslag på korrigeringar i lagen[227]. Den största förändringen som föreslogs skulle tvinga myndigheterna att ha ett domstolsbeslut för att bevaka amerikanska medborgare. Ett annat förslag skulle förbjuda NSA att göra så kallade ”abouts collection” – alltså övervakning som inte bara riktas mot människor som kommunicerar med misstänkta mål, utan som också innefattar innehåll där mål har nämnts.

Det blåste alltså upp en liten storm inför den senaste förlängningen av section 702, och den vittnade om en djupare medvetenhet och en bredare skepticism mot den amerikanska massövervakningen. Hur det slutade? Till sist röstade både representanthuset och senaten ändå igenom en förlängning – men efter striderna i representanthuset slutade det med två års förlängning istället för de vanliga fem. En kortare förlängning hade kunnat kännas som ett steg i rätt riktning, om det inte varit för att man samtidigt röstade igenom en utökning av lagen. För trots alla protester och debatter i representanthuset; när förläningen väl klubbades igenom hade majoriteten i såväl representanthuset som senaten inga problem att bredda listan på de bolag som enligt lagen kan tvingas samarbeta med myndigheterna och deras massövervakning av folket[228]. Definitionen av aktörer som måste ställa upp på att övervaka är numera så luddigt beskriven att den till och skulle kunna innefatta reparatörer som får fysisk tillgång till routrar hemma hos folk[229]. Senator Ron Wyden kallade utökningen för ”dramatisk och skrämmande”[230]. Edward Snowden kommenterade det hela med att ”NSA tar över internet.”[231] Istället för ett steg i rätt riktning blev undantagslagen mer invasiv än någonsin.

Europa – länder i tätt samarbete med USA. Ibland ännu värre än storebror.

Snowdens visselblåsning blottade inte bara de amerikanska myndigheterna. I likhet med Upstream kopplade Storbritannien upp sig direkt på fiberoptiken mellan USA och Europa och fick via det som kallades Tempora-programmet[114] tillgång till internettrafik som gick mellan Europa och USA. Med Tempora påstod sig den brittiska underrättelsetjänsten GCHQ kunna ”Mastering the internet” och Snowdens läcka visade att beskrivningen var spot on. 2013 jobbade 300 GCHQ- och 250 NSA-anställda heltid med att analysera datan som kom in via 40 000 olika key triggers[115]. Totalt sett hade

850 000 NSA-anställda tillgång till det brittiska systemet[116], som dagligen processade 600 miljoner ”telephone events” och annan trafik via 200 fiberkablar. Snowden kallade Tempora ”the largest programme of suspicionless surveillance in human history”[117]. Vad GCHQ sa om saken? När de utbildade nya analytiker i verktyget gjorde de det under presentationsrubriken ”You are in an enviable position – have fun and make the most of it”. Plötsligt låter det inte särskilt otroligt att NSA-anställda skickade runt nakenbilder på människor de övervakade[118].

USA och Storbritannien är inte de enda länder som samarbetar och delar övervakning mellan sig. Sedan andra världskriget har länderna i the Five Eyes electronic eavesdropping alliance delat data sinsemellan. Från början ingick Australien, Kanada, Nya Zeeland, Storbritannien och USA i den engelskspråkiga Five Eyes-pakten. I samband med Snowdens visselblåsning framgick det dock att alliansen utökats och att den numera gick under namnet Fourteen Eyes tillsammans med de nya medlemmarna Danmark, Frankrike, Nederländerna, Norge, Belgien, Tyskland, Italien, Spanien och Sverige.

VPN-aktörer som påstår att de är mer lämpliga för att de inte har sin verksamhet i ett 14 Eyes-land är okunniga och oärliga. Internet är en global företeelse och din trafik passerar flera 14 Eyes-landsgränser så fort du börjar surfa – oavsett var din VPN-tjänst har sitt kontor.

Det är viktigt att poängtera: Mullvad VPN är ett svenskt företag och vår verksamhet utgår från ett så kallat 14 Eyes-land. Det betyder absolut ingenting för våra användare. 14 Eyes-samarbetet går ut på att underrättelsetjänster samarbetar och att de bland annat delar med sig av den internettrafik som passerar deras landsgränser i de fysiska kablar som går under till exempel Atlanten. Som vi redan konstaterat: internet är en global företeelse och majoriteten av all trafik kommer förr eller senare att gå via USA, så det spelar liksom ingen roll var en vpn-aktör har sin hemvist. Oavsett varifrån de bedriver sin verksamhet och oavsett var de har sina servrar, så kommer deras användare inte hålla sig inom de gränserna, eftersom de självklart besöker sidor och använder tjänster som finns någon helt annanstans. Dessutom avslöjades de 14 länderna för mer än tio år sedan. Hur hög siffran är idag och vilka länder som anslutit har ingen vpn-aktör koll på.

Men som tur är går ju själva idén med en vpn ut på att kryptera trafiken, så att den inte ska gå att läsa av ifall till exempel en myndighet skulle koppla upp sig mot en fiberkabel. Därför är det inte bara ett bevis på djup okunskap när vpn-aktörer påstår att de är bättre lämpade för att de har sin verksamhet ”utanför 14 Eyes-länderna”, det är också direkt oärligt och missledande. När det kommer till vilket land som din VPN-aktör har sin hemvist i är det enbart det landets lagar som är relevanta. Lagarna som styr huruvida en VPN-tjänst måste logga och lämna ut data är det som spelar roll. Sverige är ett bra land ur det perspektivet.

Att länders underrättelsetjänster samarbetar kommer knappast som en nyhet och det är inte heller problemet, utan problemet är att de gör det via massövervakning, trots att den ständigt döms ut som vidrig och olaglig. 2018 slog the European Court of Human Rights fast att Tempora-programmet var ”var olagligt och oförenligt med de villkor som krävs för ett demokratiskt samhälle”[119] och 2020 konstaterade amerikansk domstol att NSA:s övervakning av hundramiljon-

tals människor var olaglig och bröt mot konstitutionen [120]. Man skulle kunna tro att skandalerna som avlöser varandra skulle putta världen i en annan riktning. Men istället verkar massövervakningen bara breda ut sig ännu mer.

I EU pågår en intensiv dragkamp. I ena änden: EU-domstolen som gång på gång dömer ut massövervakning[121] som olaglig, plus den del inom EU som försöker sätta rättslig press på techbolagen via direktiv som GDPR. Hittills har GDPR-direktivet varit i det närmaste verkningslöst och som mest delat ut symboliska (i sammanhanget) böter till världens rikaste bolag och samtidigt lyckats med konststycket att göra internetupplevelsen till en cookie-mardröm för alla användare. Men den här typen av regelverk har faktiskt börjat pressa big tech-bolag som Meta och Google[122]. Förhoppningsvis kan det leda till något bra i slutändan, men risken är väl att techbolagen bara anpassar sig, omgrupperar och kommer med nya lösningar för sin datainsamling. Vi applåderar ändå försöken från EU-håll och hoppas att det är den sidan av Bryssel som drar längsta strået. För inom EU finns det också helt andra krafter, som arbetar i totalt motsatt riktning.

I andra änden hittar vi till exempel EU-länder som Frankrike som vill införa AI video surveillance[123] och ett Ungern som installerar black boxes hos internetleverantörerna[124] för att kunna ha direkttillgång till invånarnas internetbeteende utan domstolsbeslut.

I samma sfär hittar vi också delar av EU-kommissionen som vill införa ett totalförbud mot privat kommunikation med sitt lagförslag chat control [125], som skulle innebära en massövervakning som till och med NSA hade varit avundsjuka på. Vi följer med spänning kampen mellan de som vill utveckla EU till en auktoritär allians och de som bryr sig om integritet och försöker föregå med gott exempel inför resten av världen.

Även i Storbritannien finns det krafter som vill underminera den

krypterade trafik som fått ett uppsving sedan Snowdens visselblåsning, genom det så kallade Online Safety Bill-förslaget[126].

I både Europa och andra delar av världen har vi också sett hur spionverktyget Pegasus använts av länder för att övervaka meningsmotståndare, politiska aktivister och journalister[127].

Regeringar och myndigheter i demokratiska länder har bevisat att de inte haft några problem med att massövervaka hela befolkningar och ta en titt rakt in i laglydiga människors hem via kameror och mikrofoner i mobiltelefoner, tv-apparater och datorer. Och i deras ambitioner lyser maktfullkomligheten igenom: som när EU-kommissionär Ylva Johansson tycker att EU:s experter och oberoende tillsynsmyndigheter gör det svårt för Europol att utföra sitt arbete[128]. Det tåls att upprepas: de mänskliga rättigheterna finns till för att skydda folket mot staten. Det är också viktigt att komma ihåg: rättigheter är något som man också måste kämpa för.

Auktoritära länder – döljer inte ambitionerna med sin massövervakning.

Att totalitära länder också använder sig av massövervakning behövs knappast sägas. I världen finns det mer än 4,5 miljarder internetanvändare. 76 procent av dem lever i länder som fängslar människor för saker de skrivit på internet i politiska, sociala eller religiösa frågor[129]. Nästan lika många lever i länder som blockerar och censurerar innehåll på nätet. I auktoritära länder används alltså inte en vpn enbart för att minska massövervakningen, utan också som ett verktyg för att överhuvudtaget komma ut på ett fritt och ocensurerat internet, för att människor ska kunna ta del av fri information.

Ett par exempel: I Iran har staten gjort sig kända för att skifta mellan att helt stänga ner internet och att låta deras övervakningsprogram Siam kontrollera, filtrera och övervaka hur deras befolkning använder sina telefoner[130] (via mobilnätet).

I Egypten övervakar regeringen journalister, aktivister och advokater[221]. I Marocko har styret använt Pegasus för att övervaka[222] människorättsorganisationer.

I Ryssland har den ryska federationens federala säkerhetstjänst (FSB) länge använt sig av systemet Sorm för att lyssna in på telefonsamtal, läsa av e-post och meddelanden[132]. I kombination med censur, svartlistad teknik och annan övervakning är så klart Ryssland svårslagna i den här grenen. I Moskva har staten infört ett system som kombinerar flera hundra tusen övervakningskameror, ansiktsigenkänning och övervakning av mobildata[133]. Systemet har använts för att spåra och fängsla demonstranter, politiska motståndare och journalister. De kallar programmet och det digitala Moskva för Safe City.

Ironiskt nog har dock den massiva massövervakningen börjat slå tillbaka på landet. På den digitala svarta marknaden Probiv, eller cyber-bazaaren som den också kallas[134], har korrupta och/eller lågbetalda och missnöjda tjänstemän läckt data från de enorma databaser som massövervakningen bidragit till. Problemet för de ryska makthavarna var att de själva fanns med i databasen. För i princip inga pengar alls gick det plötsligt att köpa information om Putins närmaste[135] krets, vilket oppositionen, andra länder och grävande journalister inte var sena att utnyttja.

The Great Firewall of China kontrollerar och censurerar internet för 750 miljoner invånare. De är totalt övervakade och polissystem påstår sig kunna förutse när du ska begå ett brott, och var du ska begå det.

Listan över länder som massövervakar[136], censurerar och förföljer sina medborgare är lång. På freedomhouse.org finns en bra genomgång över situationen i olika länder[137] och hur utvecklingen ser ut (spoiler: världen har backat på det här området i tolv år på raken). Det är många länder som tävlar om att vara värst i den här grenen, men oavsett hur man räknar är det svårt att komma ifrån att Kina slår de flesta.

Den kinesiska staten kontrollerar landets 750 miljoner internetanvändare på ”ett häpnadsväckande sätt” som Snowden har uttryckt det[138.] Staten styr vilka sajter som användarna kommer åt, blockerar vpn-tjänster och kräver att invånarna registrerar sig med sina riktiga namn för att kunna posta innehåll[139]. Sociala medier och meddelandeappar i landet är under statlig övervakning[140], utländska appar är förbjudna och till och med egenutvecklade TikTok har en inhemsk version i Kina som blockar internationellt innehåll[141]. Internetleverantörer i landet är tvingade att samarbeta med staten och Kinas samtliga mobiltelefoner är under ständig bevakning via location data[142]. Kinesernas internetupplevelse är totalt kontrollerad och censurerad under det som kallas för The Great Firewall of China[143] och redan 2013 fanns det två miljoner ”internet public opinion analysts”[144] som manuellt jobbade med att censurera invånarnas meddelande online.

Men landet jobbar så klart inte bara med manuell bevakning. I det som kallas för ”public opinion analysis software”[145] samlar staten in data och låter AI reagera på ”känsligt material”. Listan över aktivister, journalister och helt vanliga människor som fängslats för att de kritiserat Kina online tar aldrig slut.[146] Det räcker att du är hånfull mot ”gamla hjältar” för att du ska riskera tre år bakom galler.

I det så kallade Police Cloud[147] har staten dessutom byggt ett system på big data som sägs kunna ”visualisera dolda trender och relationer mellan människor”. Via systemet ritar staten upp så kallade

relationskartor och registrerar ”extrema åsikter”. En annan del av programmet påstås kunna förutse brott och var de sannolikt kommer att ske.

Kina samlar även in ”voice prints” från människor[148], har satt upp mer än hälften av världens en miljard övervakningskameror[149] och dessutom infört teknik som inte bara innehåller face recognition utan även kan läsa av hur du mår[150]. Sammantaget växer ett övervakningssamhälle fram som inte bara påminner om de dystopiska samhällen vi läst om i science fiction-böcker utan som på många sätt överträffar dikten.

I dokumentären Total Trust[236] framgår det hur det styrande kommunistpartiet ”löser problem på gräsrotsnivå” genom att låta 4,5 miljoner rutnätsansvariga föra protokoll hur invånarna inom olika områden (rutnät) sköter sig. Om någon misstänks syssla med något ”opassande” får de snabbt ett besök från polisen.

Till sin hjälp har de projektet ”skarpsynta områden” i form av en stor mängd övervakningskameror som myndigheter använder för att hålla koll, men som även så kallade ”volontärer” kan ta en titt på för att ange sina grannar. ”Alla kan övervaka” som de styrande kallar det.

Via de hundratals miljoner övervakningskamerorna, biometrisk AI och en total övervakning av människors beteende online har de lyckats koppla samman den digitala världen med den fysiska.

Tillsammans bildar landets alla övervakningskameror vad de kallar för ”himmelnätet”. Kamerorna sitter inte bara ute på gatorna, inte bara

utanför bostäderna hos de som klassats som ”opassande” utan även inne i trappuppgångar och vid angiveriglada grannars ytterdörrar.

Via de hundratals miljoner övervakningskamerorna, biometrisk AI (som ansiktsigenkänning, ögonigenkänning och röstigenkänning) och en total övervakning av människors beteende online har de lyckats koppla samman den digitala världen med den fysiska. När människor som inte ställer upp på regimens orättvisor gör sig redo för att lämna bostaden för att träffa en advokat, klaga på en myndighet eller någon liknande aktivistisk aktivitet, då vet polisen redan om det och sätter personal i trappuppgångar för att skapa en tillfällig husarrest.
Tillfälliga husarrester och polistrakasserier är inte det värsta som kan hända. 2015 fängslades och torterades hundratals människorättsadvokater i vad som kallas The 709 Crackdown[237]. De som inte fängslats är konstant övervakade. Journalister som skrivit om deras öden har blivit avlyssnade och inspärrade[238].

Hur den kinesiska staten rättfärdigar allt detta? Genom att säga att de skapar säkra samhällen och smarta städer[239].

För auktoritära länder är massövervakningen ett kontrollverktyg och det kommer att krävas ihärdigt motstånd för att förbättra situationen för invånarna där. I totalitära stater används tekniken för att förfölja meningsmotståndare, censurera information och kväva proteströrelser. Härom råder det inga tvivel och den här typen av länder skäms inte direkt för det.

I demokratiska länder skyltar man inte med det lika mycket och konsekvenserna för de drabbade är inte lika hårda. Men vi har redan sett hur massövervakning använts för att vinna fria val, hur meningsmotståndare och journalister övervakats. Flera demokratiska länder befinner sig mer eller mindre på ett sluttande plan och frågan är vilken sida de vill fastna på när historien skrivs. Vill man fortsätta vara demokratiska eller inte? För det är vad massövervakningen handlar om. Massövervakning är lika med kontroll

och motsatsen till frihet. Och någonstans går gränsen. Någonstans förlorar man till sist sin ställning som fritt samhälle. Det är därför vi kämpar för ett fritt internet, fritt från massövervakning, datainsamling och censur.

På vilken sida vill de demokratiska länderna fastna, när historien skrivs? Vill de fortsätta vara demokratiska eller inte? För det är vad massövervakningen handlar om. Massövervakning är lika med kontroll och motsatsen till frihet.

DEN STATLIGA MASSÖVERVAKNINGEN: GOING DARK

Going Dark: Ett amerikanskt-europeiskt samarbete för att knäcka privat kommunikation i det dolda.

Under parollen ”tänk på barnen” försökte EU-kommissionen införa total övervakning av alla EU-medborgare. När skandalen var ett faktum visade det sig att amerikanska techbolag och säkerhetstjänster varit inblandade i lagförslaget som fick namnet chat control – och att helt andra intressen hade styrt. Nu kommer nästa försök. Under initiativet ”Going Dark” används nya murbräckor. Ambitionen är densamma: att lagstifta in spionverktyg på varenda europeisk mobiltelefon och dator.

Den 11 maj 2022 presenterade EU-kommissionären Ylva Johansson ett lagförslag som gick under det officiella namnet ”Europaparlamentets och rådets förordning om fastställande av regler för att förebygga och bekämpa sexuella övergrepp mot barn.”

Ylva Johansson gjorde en poäng av att detta var hennes lagförslag, det var hon som hade tagit fram det – ingen annan – och om det inte varit för henne skulle Europas rättsväsende ”go blind” i jakten på

sexuella övergrepp på barn. I Ylvas värld skulle EU ”förvandlas till ett paradis för pedofiler” om inte hon fick sin vilja igenom. Det var lätt att förundras över hur Ylva Johansson vid nästan varje givet tillfälle påtalade att detta var hennes förslag. Ett narcissiskt drag? Kanske. Men det fanns kanske också något annat bakom de självcentrerade utspelen. Det skulle så småningom visa sig att Ylva Johansson inte var ensam bakom kulisserna. Redan från start fanns det andra inblandade – aktörer som skulle tjäna på att lagförslaget gick igenom men som inte skulle tjäna på att det framkom att de var med och utformade det.

Retoriken var solklar från dag ett: det handlade om barnen och när det handlar om barn så finns det inget vi inte kan tänka oss att göra för att hålla dem säkra. Så Ylva Johansson la fram ett förslag som innebar total övervakning av alla EU-medborgare och så fort någon motsatte sig drog hon fram tänk-på-barnen-kortet. De som synade bluffen gav snabbt lagförslaget (de delar av lagförslaget som handlade om övervakning på internet) ett kortare och mer rättvisande namn: chat control.

När Ylva Johansson fick frågan om det överhuvudtaget skulle gå att kommunicera säkert även efter att hennes lagförslag införts svarade hon ja. En hel värld av experter frågade sig hur. Ylva svarade med att hon hade något som ingen annan hade. En digital knarkhund.

I korta drag innebar chat control att varenda EU-medborgares kommunikation skulle övervakas. Alla samtal, alla meddelande och chattar,

alla mejl, alla bilder och filmer sparade i molntjänster – rubbet skulle filtreras i realtid via artificiell intelligens och sedan kontrolleras i ett nyetablerat EU-center i nära samarbete med Europol.

Eftersom lagförslaget stred mot Europakonventionen, EU-stadgarna och FN:s deklaration om mänskliga rättigheter blev chat control sågat av instans efter instans. Både ministerrådets och EU-kommissionens egen rättstjänst varnade för förslaget[244], likaså Europaparlamentets dataskyddsmyndighet[245]. FN:s Human Rights Council beskrev chat control som oförenligt med de grundläggande mänskliga rättigheterna och att förslaget skulle leda till massövervakning och självcensur[246]. Tidigare domare vid EU-domstolen menade att förslaget stred mot EU:s rättighetsstadga[247] och 465 forskare gick samman och varnade för konsekvenserna[248].

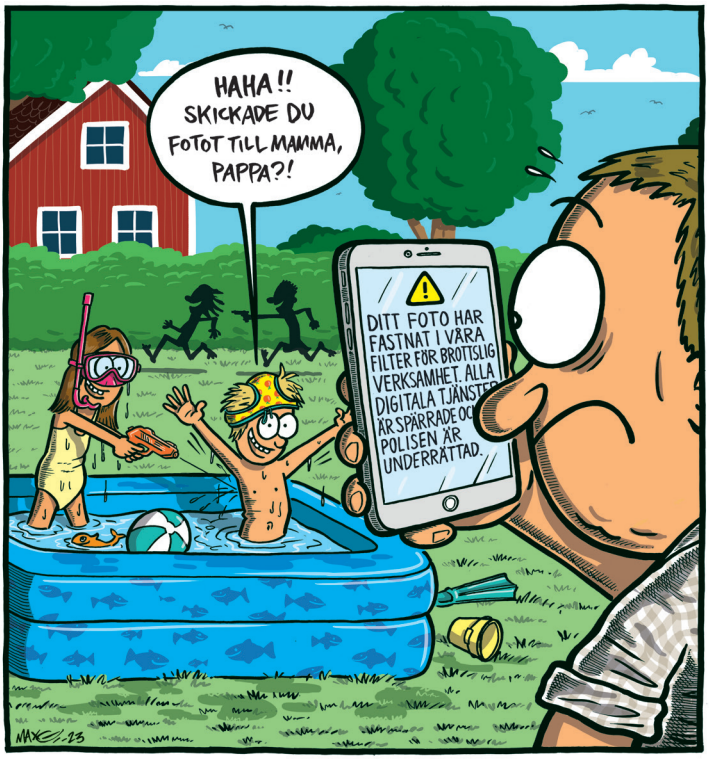
Ställd inför massiv kritik gick Ylva Johansson ut och försvarade sig: alla andra hade missuppfattat lagförslaget, chat control handlade absolut inte om massövervakning och alla som påstod det var ute efter att svartmåla henne.

Chat control – en total övervakning av alla EU-medborgare.

Ibland kallas chat control även för chat control 2.0 eftersom befintlig lagstiftning gjort det möjligt för techbolag som Google och Meta att scanna efter barnpornografiskt material hos sina användare. Att det fanns en lag som gjorde det möjligt för techbolag – om de ville – att scanna efter olagligt innehåll var ett faktum som Ylva Johansson inte var sen att använda sig av. Hon förklarade att hennes lagförslag inte var något annat en förlängning av den scanning som redan pågått i tio år[249]. Hon hänvisade även till den befintliga lagstiftningen när hon sa att EU kommer att bli en frizon för pedofiler om inte hennes lagförslag går igenom – eftersom den lagstiftningen skulle löpa ut sommaren 2024.

Gång på gång överbevisades Ylva Johansson av journalister och experter. För faktum var att inget hindrade EU från att – istället för att införa en ny lag – helt enkelt förlänga den befintliga lagen. Och framförallt: Ylvas lagförslag var allt annat än en förlängning. Skillnaderna mellan den rådande lagen och det nya förslaget var extrema. I Ylva Johanssons EU skulle scanningen inte vara frivillig. Alla meddelandetjänster (även krypterade tjänster som Signal) skulle innefattas av lagen och tvingas scanna sina användares bilder, filmer och konversationer. Det skulle innebära ett stort bekymmer för alla de som inte använder Meta eller Google för att konversera, eftersom de är i behov av säker kommunikation: politiska meningsmotståndare, visselblåsare, journalister och deras källor, utsatta människor som lever under hemlig identitet med flera, och människor med företagshemligheter, för att inte tala om de som bär på information som är känsliga gällande rikets säkerhet – EU-kommissionen själva använder till exempel Signal). Att kräva statlig insyn (antingen via så kallade bakdörrar eller scanning på själva datorn eller telefonen) skulle öppna en Pandoras ask för de länder med auktoritära inslag (bland annat fem EU-länder har blivit påkomna[250] med att använda spionverktyg för att övervaka meningsmotståndare) och lämna dörren på vid gavel för kriminella att utnyttja. Men det var ju inte bara det här som skiljde den rådande lagstiftningen och den som EU-kommissionen ville införa.

Den tidigare lagstiftningen hade bara scannat efter material som tidigare stämplats och registrerats som barnpornografiskt material. Nu skulle AI användas för att hitta ”nytt material” och dessutom leta efter grooming-försök. Chat control skulle därmed med all säkerhet skicka var och varannan människa rakt in i filtreringssystemet. Semesterbilder från stranden, nakenbilder skickade mellan partners, snuskiga sms – allt det där som en AI knappast kan göra skillnad på riskerade att fastna i ett filter som garanterat skulle dränka ett nytt EU-center med oändliga högar att gå igenom: Är det här en



semesterbild på ett barn eller barnpornografi? Är de här lättklädda ungdomarna 18 eller 14? Är det här ett snuskigt sms från en fru till en man eller ett groomingförsök? Men framförallt skulle chat control innebära ett verktyg som skulle kunna användas för att scanna efter helt andra saker.

När Ylva Johansson fick frågan om det överhuvudtaget skulle gå att kommunicera säkert även efter att hennes lagförslag införts svarade hon ja. En hel värld av experter frågade sig hur. Ylva svarade med att hon hade något som ingen annan hade. En digital knarkhund som kunde lukta på krypterad kommunikation utan att titta på

innehållet. En knarkhund som bara reagerade på barnpornografiskt innehåll – aldrig något annat.

Ylva Johansson sysslade med uppenbar vilseledning. Hon använde sig av felaktiga siffror och vinklade undersökningar. I intervjuer var hon populistisk och undvikande.

En samlad expertkår försökte banka in budskapet: antingen är krypterad kommunikation krypterad (så kallad end-to-end-krypterad, som bara sändare och mottagare kan se) eller så är den inte krypterad. Men Ylva stod på sig. Hon återvände till samma argument om och om igen. Hon undvek att svara på frågorna (hon förstod ju uppenbarligen inte hur tekniken fungerade) utan vände istället diskussionen åt annat håll och sa till exempel att det krävdes domstolsbeslut för scanningen, vilket i sig var utstuderat missledande. För det första krävdes det inget domstolsbeslut för hennes scanning, utan det kunde vara annan instans, och för det andra handlade det om att denna instans skulle besluta och tvinga meddelandetjänster att övervaka alla dess användare. När Ylva bröt ut i ett ”det krävs domstolsbeslut” var det alltså inte gällande domstolar och beslut att bevaka till exempel misstänkta pedofiler. Utan ett beslut huruvida en tjänst skulle krävas på övervakning. Vad som krävdes för att en tjänst skulle falla in under övervakningen? Att det fanns en möjlighet att på tjänsten sprida barnpornografi eller grooma barn, vilket så klart är lika med alla meddelandetjänster.

Så fort Ylva Johansson blev överbevisad flyttade hon fokus. Till slut återvände hon alltid till sista tillflyktsorten: det handlar om

barnen. Hon drog anekdoter och hänvisade till siffror som pekade på en explosionsartad ökning av barnpornografiskt material på till exempel Facebook – trots att Facebook själva gick ut och sa att 90 procent av alla rapporter kommer från tidigare spritt material[251].

EU-kommissionen med Ylva Johansson i spetsen fick kritik från alla möjliga håll. Polischefer gick ut och sa att största delen av materialet som de får in idag är material med tonåringar som skickar bilder till varandra[252] och att den typen av rapporter riskerar att leda polisen i fel riktning. Scanningtester som europeisk polis gjort på befintligt material visade att 80-90 procent av alla träffar var felträffar[253]. Nu skulle dessutom ”nytt material” scannas – vilket uppenbart skulle innebära en omöjlig administration för att bara reda ut vad som var olagliga bilder och vad som var semesterbilder från familjedagar på stranden. Felprocenten skulle uppenbart närma sig hundrastrecket. För europeiska rättsväsenden som inte ens idag hinner med att klara upp alla tips[254] de får in skulle det här vara förödande. Och de kriminella skulle förstås vända sig till olagliga meddelandetjänster. Barnen skulle inte hjälpas. Samtidigt skulle varenda EU-medborgare få spionverktyg installerade på sina telefoner.

Hur Ylva Johansson tacklade de här upplysningarna? Inte alls. Istället fortsatte hon som en repig skiva att ”tänka på barnen” och så beställde hon en undersökning som sa att 80 procent av EU:s befolkning stöttar chat control. Problemet? EU-kommissionen använde sig av Europabarometer, en undersökningsbyrå som blivit anklagade för att sudda ut gränsen mellan forskning och propaganda. När Max Planck Institute for the Study of Societies ombads att kommentera chat control-undersökningen kom de fram till att den hade en politisk agenda och bestod av frågor som var vinklade[255] för att stödja kommissionens planer.

Ylva Johansson sysslade med uppenbar vilseledning. Hon använde sig av felaktiga siffror och vinklade undersökningar. I intervjuer

var hon populistisk och undvikande. Men hon var ju tvungen att ta till de här metoderna. För det handlade ju aldrig om barnen.

Amerikanska techbolag och säkerhetstjänster bakom lagförslaget.

I september 2023 kom en stor granskning från de tre journalisterna Giacomo Zandonini, Apostolis Fotiadis och Luděk Stavinoha. Efter att EU-kommissionen i sju månader försökt vägra att lämna ut allmänna handlingar fick de till sist ut ett material som gjorde att de kunde börja lägga pusslet som avslöjade spelet bakom chat control[256]. I granskningen som publicerades i flera europeiska tidningar publicerades bland annat ett brev där Ylva Johansson skrev till Julie Cordua, vd:n för det amerikanska bolaget Thorn: ”Vi har delat många stunder på resan mot detta förslag. Nu vänder jag mig till dig att se till att denna lansering blir en framgångsrik sådan.”

Thorn är ett amerikanskt bolag som bildades av skådespelaren Ashton Kutcher och som utvecklar verktyg som scannar efter barnpornografiskt material. Till det amerikanska departementet för inrikes säkerhet hade de sålt programvaror för miljoner. Ashton Kutcher själv hade haft videokonferenser med EU-kommissionens ordförande Ursula von der Leyen och han hade hållit föreläsningar i EU om hur man med ny teknik kan scanna krypterat innehåll utan att titta på det. Fram trädde bilden av Ylva Johanssons knarkhund.

Under flera år lobbade Kutcher mot EU-kommissionen (fram till att han tvingades kliva av Thorn efter att ha försvarat sin skådespelarkollega Danny Masterson när han dömdes för våldtäkt). Han hade möten med flera på EU-kommissionen och hade ett extra nära band med kommissionens Eva Kaili (fram till hon arresterades för mutbrott och fick lämna sitt parti[257]).

Här hade vi alltså ett amerikanskt bolag som hade direktkontakt med EU-kommissionen och som sålde den teknik som skulle kunna

användas vid ett införande av chat control. Dessutom byggde allt på en falsk införsäljning: tekniken som Kutcher och Johansson pratade om fanns inte. Expert efter expert dömde ut deras prat om knarkhundar[258].

En annan del av skandalen: i EU-s öppenhetsregister var Thorn registrerade som välgörenhetsorganisation – trots att de sålde tekniken som de föreläste om i EU. Tricket att förklä organisationer och bolag i skruden av välgörenhet skulle visa sig vara återkommande i den här soppan.

Ylva Johansson har, sedan lagförslaget chat control presenterades, intensivt pekat på välgörenhetsorganisationer som stöttar hennes förslag. Hon har jobbat med dem i PR-sammanhang, som ett sätt att visa att chat control har stöttning av oberoende, ideella krafter som bryr sig om barnen. En central organisation i detta arbete har varit WeProtect. När Zandonini, Fotiadis och Stavinoha släppte sin granskning visade det sig att EU-kommissionen varit med och grundat organisationen, att den innehöll representanter från såväl techbolag som olika länders säkerhetstjänster. I styrelsen för WeProtect satt Ylva Johanssons kollega i EU-kommissionen, Labradror Jimenez, tillsammans med Thorns vd Julie Cordua och representanter från USA:s och Storbritanniens (som samtidigt som chat control la fram ett eget övervakningsförslag med barnen som murbräcka) regeringar, även Interpol fanns representerade. Thorn hade tryckt in pengar i WeProtect. EU-kommissionen hade bidragit med en miljon euro. Det handlade alltså inte om barnrättsorganisationer som gav Ylva Johansson stöttning. Det handlade om lobbyorganisationer som bildats av EU-kommissionen i syfte att få igenom lagförslaget.

Barnrättsorganisationer bildades med syftet att "divide and conquer' the members of the parliament by deploying in priority survivors from MEPs' countries of origin".

Med i styrelsen för WeProtect fanns även representanter från Oak Foundation, som utöver sitt engagemang i WeProtect även hade varit med och startat ECLAG (ytterligare en välgörenhetsorganisation som stöttat chat control-förslaget). ECLAG lanserades bara några veckor efter Ylva Johanssons lagförslag presenterades och i organisationens kommitté fanns Thorn representerade. Ytterligare en organisation: Brave Movement, en organisation som bildades en månad innan lagförslaget chat control presenterades. Brave lanserades med hjälp av tio miljoner dollar från Oak Foundation och i ett strategidokument som journalistgranskningen kom över stod det att "once the EU Survivors taskforce is established and we are clear on the mobilised survivors, we will establish a list pairing responsible survivors with Members of the European Parliament – we will 'divide and conquer' the MEPs by deploying in priority survivors from MEPs' countries of origin."

Oak Foundation dök även upp i en kartläggning gjord av The Intercept[259]. 2023 hade en amerikansk organisation med namnet Heat Initiative bildats. På pappret var de en "new child safety group" och det första de gjorde var att kampanja för att Apple skulle "detect, report, and remove" barnpornografiskt material från iCloud. Apple svarade med att det var något som kriminella skulle kunna utnyttja och att det också skulle kunna leda till ett "potentiellt sluttande plan av oavsiktliga konsekvenser, att skanna efter en typ av innehåll skulle till exempel kunna öppna dörren för bulkövervakning."

Heat Initiative gillade inte svaret och slog tillbaka med anti-Apple-propaganda på stora reklamskyltar i amerikanska städer under temat ”tänk på barnen”. Vilka som låg bakom Heat Initiative, förutom Oak Foundation? Heat leddes av en före detta vicepresident på Thorn. The Intercept-artikeln hänvisade också till en annan granskning[260] som visade att Thorn samarbetade med Palantir, big-data-bolaget som hjälpte NSA att massövervaka hela världen[261] och som var inblandade i Cambridge Analytica-skandalen där Facebookanvändares privata meddelanden och data[262] användes för att påverka presidentvalet å Donald Trumps vägnar 2016.

Samtidigt satt de riktiga organisationerna som jobbade med att motverka sexuella brott mot barn och undrade varför EU-kommissionen vägrade prata med dem.

EU-kommissionen var alltså med och finansierade och startade upp välgörenhetsorganisationer med målet att använda sig av gamla brottsoffer för att emotionellt påverka EU-parlamentariker. I tätt samarbete med techbolaget som erbjöd tekniken som skulle användas vid ett införande av övervakningen. Tillsammans med representanter från utom-europeisk säkerhetstjänst. Som del av en större apparat, där samma taktik användes för att påverka utvecklingen i USA.

Samtidigt satt de riktiga organisationerna som jobbade med att motverka sexuella brott mot barn och undrade varför EU-kommissionen vägrade prata med dem. I det granskande reportaget berättar Offlimits, som är Europas äldsta hotline för utsatta barn, att Ylva Johansson hellre åkte till Silicon Valley för att träffa företag med vinstintresse än att prata med dem.

Samma sak med teknikexperterna. Matthew Green, professor i kryptografi vid John Hopkins University, berättar i granskningen att ”i den första konsekvensbedömningen av EU-kommissionen fanns det i princip ingen input från externa forskare, vilket är helt otroligt med tanke på den vetenskapliga infrastruktur som finns i Europa, med de bästa forskarna inom kryptografi och datorsäkerhet i världen.”

Med i utformandet av lagen fanns däremot Europol tillsammans med säkerhetstjänster från andra länder[263]. I juli 2022 skrev Europol att de ville kunna använda scanningen och övervakningen till annat än sexuella brott mot barn. EU-kommissionen svarade att de förstod önskan men att de ”var tvungna att vara realistiska i vad som kunde förväntas, med tanke på hur känsligt lagförslaget är”. Även Thorn var tydliga med att scanningen i en förlängning kunde användas till annat[264]: ”När man överväger lagstiftning inom kryptering borde man inte bara fokusera på CSAM. Lösningar för att scanna krypterade miljöer är något som är mycket bredare än ett enskilt brott”, skrev bolaget i ett dokument[265].

Senare framkom det också att Europol var ute efter en ofiltrerad tillgång till det scannade materialet[266]: ”All data är användbar och bör skickas till brottsbekämpande myndigheter. Materialet borde inte filtreras av EU-centret eftersom även oskyldiga bilder kan innehålla information som någon gång kan bli användbart.”

När granskningarna av EU-kommissionens direkt odemokratiska tillvägagångssätt publicerades svarade Ylva Johanssons kontor vid EU-kommissionen med olaglig propaganda på sociala medier.

EU-parlamentet: ”kommissionen var ute efter massövervakning”.

Här satt alltså EU-kommissionen och jobbade fram lagförslag tillsammans med ett Europol som ville ha tillgång till all övervakning oavsett om den innehöll något olagligt eller ej – eftersom det kunde vara bra att ha. Det visade sig handla väldigt lite om barnen.

När granskningarna av EU-kommissionens direkt odemokratiska tillvägagångssätt publicerades svarade Ylva Johanssons kontor vid EU-kommissionen med att annonsera på plattformen X (tidigare Twitter). De riktade annonser (för chat control) så att beslutsfattare i olika länder skulle se dem, men också så att människor som misstänktes vara starkt emot förslaget skulle undgå dem. Annonseringen riktades också utifrån religiös och politisk tillhörighet och bröt alltså mot EU:s egna lagar gällande micro-targeting[267].

Ylva Johansson tvingades till utfrågning i EU-parlamentet där ett nästintill enat Europaparlament öste massiv kritik över hennes tillvägagångssätt.

Tjänstemän på högsta EU-nivå använde alltså insamlad data av big tech för att försöka skapa olagliga filterbubblor utformade för att driva igenom ett massövervakningsförslag. Det hela slutade med att Ylva Johansson kallades till utfrågning i EU-parlamentet. Ett nästintill enat Europaparlament öste massiv kritik över Ylva Johansson och hennes tillvägagångssätt. Hon ställdes mot väggen för Thorns inblandning, för de riktade annonserna och EU:s ombudsman underkände EU-kommissionens ovilja att dela med sig av allmänna handlingar gällande förhållandet med Thorn (EU-kommissionen

tyckte det skulle sekretessbeläggas eftersom det riskerade att undergräva kommersiella intressen …). Ylva Johansson svarade med: tänk på barnen.

I november 2023 kom EU-parlamentets ställningstagande[268]. I en närmast historisk enighet gick samtliga grupper i parlamentet ut tillsammans och sa nej till lagförslaget. På presskonferensen sa representanter från parlamentet[269] att ”det här är ett slag i ansiktet för kommissionen, en kommission som inte fokuserade på att skydda barnen utan som var ute efter massövervakning”. Patrick Breyer, som varit den mest aktiva motståndaren i parlamentet, kallade det en ”seger för barnen, som förtjänar ett effektivt förslag som upprätthåller och respekterar rättigheter och som håller i rätten”.

Breyer hänvisade till att chat control med högsta sannolikhet inte skulle hålla i domstol om lagförslaget hade röstats igenom. Bara några månader senare kom en dom från Europadomstolen[270] som slog fast att myndigheter inte har rätt att kräva tillgång till end-to-end-krypterad kommunikation.

Tyvärr innebar inte parlamentets tydliga ställningstagande emot chat control att kampen var över. I EU är det två instanser som är med och tycker till om lagförslag från EU-kommissionen: EU-parlamentet och Ministerrådet. Och i Ministerrådet var tongångarna annorlunda. Samtidigt som parlamentet i tydlig enighet gick emot förslaget fortsatte Ministerrådet att bråka om en gemensam hållning. Gång på gång försökte man komma fram till kompromissförslag som i det stora hela skulle innebära ett införande av chat control. Däremot blev det uppenbart att inte ens Ministerrådet trodde på Ylva Johanssons knarkhundar, när delar av rådet föreslog[271] att scanningen borde undantas politiker, poliser och underrättelsetjänst, samt allt som klassades som ”professionella hemligheter”. Uppenbarligen fanns det politiker som var rädda för att deras hemligheter skulle läcka, men som däremot inte hade något emot att massövervaka folket.

Patrick Breyer var tydlig i sin respons: “de här personerna är medvetna om att chat control innebär otillförlitliga och farliga algoritmer – och ändå är de redo att släppa lös dem på medborgarna.”

När ett samlat ställningstagande från Ministerrådet drog ut på tiden närmade sig det där slutdatumet som Ylva Johansson hade pratat om i debatterna. Gång på gång hade hon argumenterat för att EU skulle ”go dark” i jakten på brottslingar om inte chat control skulle antas – eftersom den rådande lagstiftningen (den frivilliga scanningen) skulle gå ut sommaren 2024. Gick hon därmed ut, sommaren 2024, och sa att nu var det över? Så klart inte. Snabbt och lätt gjorde hon det som tidigare varit helt utom räckhåll i hennes argumentation: hon gick in och förlängde den tidigare lagstiftningen.

Nytt försök till massövervakning via initiativet ”Going Dark”.

Samtidigt som EU:s medlemsländer försökte komma fram till olika kompromissförslag för att kunna införa chat control var de också med och arbetade på en plan B och nya försök till lagar för massövervakning. Under Sveriges EU-ordförandeskap våren 2023 initierades ett projekt som fick namnet ”Going Dark”. Tanken från det svenska ordförandeskapet var initialt att en så kallad High Level Expert Group skulle sjösättas. Uppdraget att sätta ihop gruppen gick till EU-kommissionen som direkt plockade bort ”Expert”. Istället för en High Level Expert Group bildades en High Level Group. Som tidningen Netzpolitik[272] uttryckte det: ”att ta bort ordet Expert är ingen liten detalj: speciella regler gäller expertgrupper, till exempel när det kommer till transparens, regler som däremot inte gäller High Level Groups.”

Med på mötena fanns en tidigare FBI-anställd som uttryckte sin tacksamhet över att frågan drevs inom EU och att laglig tillgång till data borde prioriteras.

Återigen valde EU-kommissionen att inleda ett förarbete kopplat till övervakning utan att på allvar låta experter vara en del av processen. När gruppen samlades en första gång slog man fast att gruppens syfte var att diskutera metoder[273] för att ”få tillgång till data som kunde effektivisera arbetet för rättsväsendet, guidat och baserat på inputs från EU-medlemsländerna.”

Några utmaningar pekades ut som särskilt angelägna: tillgång till krypterat material (såväl sparad data som kommunikation), datalagring, location data och anonymisering (inklusive vpn och darknet).

Gruppen delades in i tre arbetsgrupper: den första skulle jobba med tillgång till data i användares enheter (dator och mobil), grupp två skulle fokusera på tillgång till data i tjänsternas system (meddelandeapparna till exempel), tredje gruppen skulle diskutera tillgång till data i förflyttning.

Enligt mötesprotokoll från den svenska riksdagens EU-nämnd arbetade gruppen ”för att presentera verksamma rekommendationer inför tillträdet av den nya kommissionen 2024 och för att de rekommendationerna sedan ska genomföras.”[274]

Kommande lagstiftningsförslag från EU-kommissionen kan alltså antas handla om att ge tillgång till data i användarnas enheter, meddelandetjänsternas system och data i förflyttning. Patrick Breyer, som jobbat hårt med att motverka chat control, menade att gruppen bara var en förlängning av tidigare övertramp och att ”Going Dark” arbetade för att införa olaglig massövervakning[275]. När han begärde

ut dokument från gruppens möten och vilka som deltagit fick han tillbaka sekretessmaskerade uppgifter. EU-kommissionen hade alltså satt ihop en arbetsgrupp som jobbade för massövervakning av folket samtidigt som de inte var transparenta gällande vilka som ingick i gruppen. Det var en repig skiva. Borta var den tidigare ursäkten ”tänk på barnen”, men målet var detsamma.

En del insyn gick däremot att få via det svenska justitiedepartementet som på Mullvad VPN:s förfrågan lämnade ut såväl mötesanteckningar som uppgifter om vilka svenska representanter som fanns med i mötena.

Där framgår det att det första ”Going Dark”-mötet leddes av två personer. Den ene var Olivier Onidi, som är biträdande general direkt under Ylva Johansson i EU-kommissionen. Onidi har dels uttryckt att ”det värdefulla” med chat control är att ”förslaget täcker alla former av kommunikation, privat kommunikation inkluderat”[276], dels gick han ut och försvarade Ylva Johansson och chat control när han sa[277]: ”Jag tycker det är totalt orättvist att peka ut det här som en obligatorisk kontroll av all privat kommunikation. Det är inte vad ni har framför er. Det här förslaget är en oerhörd förbättring jämfört med nuvarande situation.”

Onidi har också ifrågasatts för sina möten med det amerikanska bolaget Palantir[278] (ökända för sin inblandning i amerikanska myndigheters olagliga massövervakning).

Den andre personen som ledde det första ”Going Dark”-mötet var Anna-Carin Svensson, internationell chefsförhandlare vid det svenska justitiedepartementet, och som enligt Wikileak-dokument 2010 ska ha uppmanat amerikanska utrikesdepartementet och FBI att fortsätta med ett rådande informellt informationsutbyte länderna emellan istället för att skriva formella avtal. Enligt de amerikanska företrädarna på mötet handlade det om att undanhålla den svenska riksdagen informationen[279]:

”Hon trodde att, givet den svenska grundlagens krav på att presentera ärenden av vikt för nationen inför riksdagen, och i ljuset av den pågående kontroversen om den nyligen beslutade FRA-lagen, kommer det vara politiskt omöjligt för justitieministern att inte låta riksdagen granska några datautbytesöverenskommelser med USA. Enligt hennes åsikt kan offentliggörandet av det här också äventyra de informella informationsutbytena”, stod det i de läckta dokumenten.

Enligt dokumenten frågade Anna-Carin Svensson FBI om de inte kunde fortsätta använda sig av de starka men informella arrangemangen. När dokumenten läckte förnekade Svensson allt och svarade: ”hur amerikanerna uttrycker sig kan inte jag stå för”.

Från svensk sida var justitiedepartementet representerat på ”Going Dark”-mötena, men även säkerhetspolisen (Säpo) och polismyndigheten. Tillsammans med representanter från de andra medlemsländerna använde de High Level Group-mötena till att diskutera hur krypterade tjänster via lagstiftning skulle kunna krävas på att tillhandahålla data i läsbart format. Flera medlemsstater framförde att ”arbetsgrupperna behövde titta på lösningar som innebar ”laglig tillgång genom design”. Det var något som gladde amerikanska representanter.

Med på ”Going Dark”-mötet den 21 november 2023 fanns nämligen även en tidigare anställd vid FBI som sa att ”lösningar för laglig tillgång borde prioriteras” och att ”företagen behövde ha ett ansvar och följa samma regler”. Som tidigare FBI-anställd framförde han också ”sin tacksamhet över att frågan drevs inom EU.”

Europas samlade polischefer: vi kan inte acceptera att kriminella använder säker kommunikation.

”Going Dark”-mötena mynnade ut i ett utspel från Europas samlade polischefer. I april 2024 gick Europol ut med uppmaningen[280]

”European Police Chiefs call for industry and governments to take action against end-to-end encryption roll-out”. Deklarationen var en ”direkt förlängning av initiativet Going Dark”[281] och tillsammans var de europeiska polismyndigheterna tydliga med att ”även om kryptering stärker cybersäkerheten och den personliga integriteten så accepterar vi inte ett binärt val mellan cybersäkerhet eller personlig integritet å ena sidan, och den allmänna säkerheten å andra sidan. Absolutism hjälper inte någon av sidorna.”

Det var som om Ylva Johanssons knarkhund fått upp vittringen igen. I frånvaro av expertis försökte Going Dark-initiativet trixa bort det faktum att end-to-end-kryptering är absolut – antingen har man säker kommunikation eller så har man det inte.

Trots att FN klassar kryptering som en mänsklig rättighet gick Going Dark-initiativet och den samlade europeiska poliskåren ut till strid för att knäcka end-to-end-kryptering.

De samlade polischeferna pekade ut två nyckelfaktorer för att uppnå onlinesäkerhet[282], vilka var direkta upprepningar av resonemang i Going Dark-diskussionerna. Nummer 1: så kallad laglig tillgång till techbolagens lagrade data. Nummer 2: scanning i realtid av olaglig aktivitet i techbolagens tjänster. Allt skulle givetvis ske under starka skyddsåtgärder och tillsyn.

Representant för den svenska polismyndigheten var Stefan Hector som gick ut och sa att ”ett samhälle kan inte acceptera att kriminella idag har ett utrymme att kommunicera säkert i syfte att begå grova brott.” En vecka senare avslöjades det att den svenska polisen infiltrerats och läckt till kriminella[283].

Trots att FN klassar kryptering som en mänsklig rättighet gick Going Dark-initiativet och den samlade europeiska poliskåren ut till strid för att knäcka end-to-end-kryptering. Deras första utspel var rentav en reaktion på att Meta rullade ut just end-to-end-kryptering.

Europols utspel var dock bara en första fingervisning. I slutet av maj 2024 mynnade Going Dark-initiativet ut i 42 rekommendationer[290] som EU-kommissionen ska ha med sig i sitt arbete för framtida lagförslag. I dokumentet går det bland annat att läsa att kryptering gör det svårare för myndigheter att få tillgång till innehållsdata i realtid, inte minst gällande meddelandetjänster som använder sig av end-to-end-encryption. I dokumentet går det också att läsa att myndigheter behöver ha tillgång till data en clair (alltså i klartext) via ”lawfull access without weakening privacy”. Going Dark-initiativet pratar om principen “security through encryption and security despite encryption” som en central grundsten.

Going Dark-initiativet visar alltså upp samma tendenser som chat control-förslaget. Experter har än en gång stängts ute från diskussionerna och ministrar och polisrepresentanter har återigen missat huvudpoängen: antingen är end-to-end-krypterad kommunikation privat och säker – eller så är den inte det.

Lösningen som Going Dark-initiativet (precis som chat control) är ute efter är scanning som sker innan kommunikationen skickas iväg. Med det argumentet menar de att krypteringen inte har brutits. Men det skulle innebära att hela poängen med krypteringen har brutits. Om kommunikation scannas av innan den skickas är den inte privat och säker.

Going Dark-initiativets 42 rekommendationer pratar om hårdare konsekvenser mot de meddelandetjänster som inte ger ”laglig tillgång” till deras data. Och om de ska upprätthålla sin princip om “security through encryption and security despite encryption” återstår egentligen bara två uppenbara metoder för sådan access.

Antingen genom så kallade bakdörrar till systemen – där myndigheter har tillgång att ta sig in i tjänsternas system för att ta en titt på datan, alternativt via ”extranycklar” till de end-to-end-krypterade konversationerna. Eller så är det en så kallad klientscanning, en scanning som sker i användarens app på själva datorn eller telefonen. Klientscanningen skulle också kunna ske på själva operativsystemet – vilket skulle göra det enklare för myndigheterna; för då skulle allt som händer på telefonen kunna avlyssnas i ett svep. Ungefär som när Microsoft börjat utveckla sin feature Recall[291] som är tänkt att köra en printscreen av skärmen varannan sekund.

Att införa den här typen av statliga spionverktyg på EU-invånarnas telefoner skulle inte bara innebära att allas personliga integritet är förlorad. Det skulle också innebära stora säkerhetsrisker. Det här borde massövervakningsförespråkarna veta vid det här laget. Ekona från chat control-debatten är bokstavliga. Men det är också ett eko från en äldre strid.

Going Dark-initiativet är ute efter lagförslag som dömts som olagliga och som bryter mot mänskliga rättigheter. De är en sen svallvåg efter Snowdens avslöjande, som i mångt och mycket förändrade internet.

Going Dark-initiativet är egentligen bara en förlängning av det så kallade kryptokriget (kriget mot kryptering) som amerikanska myndigheter deltagit i sedan internets intåg. Som Signals vd Meredith Whittaker uttrycker det i ett föredrag[284]:

”Kryptering var avgörande för att kunna ha ett kommersiellt internet. Men brottsbekämpningen och säkerhetstjänsterna såg alla

nätverk som är resistenta mot statlig övervakning som ett hot och ett problem."

De amerikanska myndigheterna har redan testat bakdörrarna som det europeiska Going Dark-initiativet nu är ute efter. De har redan fått bevis på att det inte går att införa dem på ett säkert sätt utan att fientliga stater eller hackare kan nyttja dem. Edward Snowden avslöjade att NSA la 250 miljoner dollar varje år[285] på att få techbolag att installera bakdörrar i sina tjänster, vilket också blottade riskerna med just bakdörrar. 2010 lyckades kinesiska hackare att använda en bakdörr hos Google[286] för att ta sig in i Gmail. Samma sak 2005 när statlig övervakning av Vodafone[287] utnyttjades av utomstående för att bugga den grekiska premiärminister och hans utrikesminister, justitieminister och hundra andra regeringsmedlemmar.

Going Dark-initiativet kanske väljer att gå på så kallad client-side scanning istället; för att scanna direkt i apparna på användarnas telefoner, eller till och med scanna hela operativsystemet. Det här är också en övervakningsmetod som, förutom att innebära statlig spionvara på allas telefoner, också skulle misslyckas ur ett säkerhetsperspektiv. Det skulle inte gå att hålla privat och säkert. Detta vet vi eftersom Apple, som är ett av världens mest tekniska och förmögna företag, har slängt otroliga resurser på att reda ut om det går att göra på ett säkert sätt. När Apple gjorde sin satsning publik tog det hackare två veckor att ta sig in. Apple gav upp försöket och säger nej till alla som ber dem att testa igen – eftersom det är för enkelt att hacka system där klientscanning förekommer[288].

Going Dark-initiativets ambitioner att införa bakdörrar och klientscanning är inte förenligt med EU-lagar och mänskliga rättigheter. Men istället för att arbeta på lagförslag som inte bryter mot mänskliga rättigheter har Going Dark-initiativet fokuserat på propaganda för att få igenom sina kommande lagförslag. I läckta dokument[292] framgår vikten av att ”sätta rätt narrativ” och att man ska

ta fram en ”communication strategy that underlines that the recommendations aim to protect fundamental rights”. Ett snabbt tips från Mullvad VPN: ta fram lagförslag som inte bryter mot mänskliga rättigheter – sen är det bara att gå ut och visa upp dem.

Going Dark-initiativet är ute efter lagförslag som dömts som olagliga och som bryter mot mänskliga rättigheter. De är en sen svallvåg efter Snowdens avslöjande, som i mångt och mycket förändrade internet. Efter Snowdens visselblåsning fick end-to-end-krypterade meddelandetjänster som Signal ett allmänt uppsving. Apple började använda stark kryptering i sina operativsystem. Från att ha haft i princip fri tillgång till människors internettrafik (om de inte använde en trovärdig vpn vill säga) och från att ha kunnat läsa människors meddelande sinsemellan i klartext blev nu internet svårare för amerikanska myndigheter att massövervaka.

I sitt föredrag pekar Meredith Whittaker på en viktig poäng: ”Stark kryptering var en viktig vinst. Men resultatet av vinsten blev inte integritet. Arvet från kryptokrigen var att vi klev in i den kommersiella massövervakningens tidsålder. Makten att möjliggöra – eller kränka – den personliga integriteten lämnades i händerna på företag, inte i händerna på de som förlitar sig på deras tjänster. Företag som gavs incitament att implementera övervakning i form av reklam och kommersiell handel.”

I mer än tjugo år har den så kallade kommersiella massövervakningen skapat några av världshistoriens rikaste företag. Att Meta rullar ut end-to-end-kryptering innebär inte att de övergett sin affärsmodell. Men det var tillräckligt för att de europeiska polischeferna, påhejade av amerikanska myndigheter, skulle gå ut i samlad trupp och kräva laglig tillgång till innehållet i säker och privat kommunikation. Meredith Whittaker igen:

”Våldsamheten i den attack som nu sker mot end-to-end-krypteringen, och andra integritetsbevarande tekniker, är relaterat till

önskan från vissa i den amerikanska regeringen att återvända till den mindre begränsade tillgång till övervakning som de ser att de har förlorat efter Snowdens avslöjanden."

Vi ser attacken komma i Europa nu. Men rörelsen har sin bas i USA. Redan 2014, bara ett år efter Snowdens avslöjanden, gick FBI-chefen James Comey[289] ut och pratade om "det växande problem som kryptering innebär för brottsbekämpande myndigheter som vill ha laglig tillgång till elektronisk kommunikation."

De amerikanska myndigheterna som 2014 nyligen blivit påkomna att spionera på precis hela världen använde sig av ett speciellt uttryck när de började lobba för att åter få tillgång till att kontrollera allt och alla utan större ansträngning. FBI-chefen Comey pratade om "Going Dark".

”Våldsamheten i den attack som nu sker mot end-to-end-krypteringen, och andra integritetsbevarande tekniker, är relaterat till önskan från vissa i den amerikanska regeringen att återvända till den mindre begränsade tillgång till övervakning som de ser att de har förlorat efter Snowdens avslöjanden.”

Meredith Whittaker, vd Signal.

KONSEKVENSERNA AV MASSÖVERVAKNINGEN: SÅ ANVÄNDS DATAN SOM SAMLAS IN

Övervakningen av ditt internetbeteende får konsekvenser, du kanske inte bara ser dem än.

Kommersiella och statliga massövervakare samlar in absurda mängder data om människor över hela världen. Men vad används all data till? När ditt internetbeteende kartlagts, vad riskerar det att leda till?

Ganska ofta stöter vi på personer som säger ungefär: ”jaja, de samlar in massor av data, men varför ska jag bry mig?”. Det finns flera svar på den frågan, men ett av dem är kort och gott att datan kan läcka. Den ”vanliga internetanvändaren” kanske inte bryr sig om att personlig data finns lagrad på något av världens största företag eller hos en myndighet, men har kanske större problem om den personliga informationen hamnar i det som brukar kallas ”fel händer”. Du kanske inte har problem med att ett apotek lagrar vilka mediciner du köper, men tycker att det känns olustigt när rubrikerna om dataintrång kommer[151]. För så enkelt är det: Insamlad data är lika med data som kan läcka. Om en stat eller ett företag eller en organisation sitter

på känslig data är de ansvariga för att hålla den säker i en oöverskådlig framtid. Det är en svår uppgift, speciellt när tekniken utvecklas snabbt och företag och myndigheter (vanliga myndigheter, inte de som sysslar med massövervakning) har svårt att hålla takten. Historien har gång på gång visat hur databaser använts på sämsta tänkta sätt när nya ledare kommer till makten. Vi har alldeles för ofta sett hur hackare och fientliga makter kommit över uppgifter som de absolut inte ska. Eller hur slarv, dåliga strukturer och mänskliga faktorer lett till läckage. Vår inställning till detta är oerhört enkel och vårt budskap till de som lagrar data är tydligt: minimera er datalagring, data som ni inte har riskerar inte att läcka.

Men nu är ju de återkommande skandalrubrikerna om dataläckor tyvärr det lilla problemet. Det stora problemet är att det praktiskt taget pågår ett konstant läckage, när kommersiella och statliga massövervakare medvetet samlar in data. Men vad händer sen? Bortsett från att du får störiga annonser riktade till dig, hur används egentligen datan?

Det korta svaret när det gäller de statliga massövervakarna: flera av världens länder har kapaciteten att när som helst ta en titt på ditt samlade internetbeteende. Beroende på var du bor kan det få ödesdigra konsekvenser för dig.

Du kanske tänker: vem bryr sig om vilka sidor jag klickar på? Ett exempel om du bor i USA: försäkringsbolag, som använt köphistorik för att skruva upp priserna på folks premier.

När det gäller de kommersiella massövervakarna finns det också ett kort och enkelt svar på frågan vad de gör med din data: de säljer den.

2021 avslöjades det att så kallade data brokers hade köpt location data från Life360[152], en app där 33 miljoner föräldrar håller koll på var deras barn befinner sig genom att spåra barnens telefoner. Året därpå stämdes bolaget Kochava, en annan så kallad data broker, för att de spårat hundratals miljoner människor och sålt känslig data om var de befunnit sig[153].

Beroende på vilket land du bor i kan också din internetleverantör logga din trafik och dela med sig av den i olika affärsuppgörelser. I en rapport från amerikanska Federal Trade Commission (FDT)[154] visade det sig att minst sex stora amerikanska internetleverantörer delat sina kunders location data med tredjepartsbolag. I rapporten konstaterade man att "även om internetleverantörerna lovar att inte sälja personlig data, så framgår det i deras privacy policy att datan kan delas och nyttjas i affärsuppgörelser med andra"

Det här är ett upplägg som även de största techbolagen sysslar med. Meta och Google kanske inte säljer sin (din) data, men de byter den fram och tillbaka hej vilt[155]. Men framförallt använder de stora techbolagen datainsamlingen för att optimera sina annonsverktyg. Meta och Google har blivit två av världshistoriens högst värderade bolag tack vare intäkterna från sina annonsnätverk och deras affärsidé är uppenbar; den handlar om att kartlägga ditt beteende och förutse vad du kommer att efterfråga i framtiden för att kunna skräddarsy annonser så pricksäkert som möjligt.

Data på sjukdomshistorik och sexuell läggning säljs och utnyttjas.

Du kanske ställer dig frågan: vem bryr sig om Facebook har koll på vilka sidor jag klickar på? Du kanske dessutom gillar att få skräddarsydd reklam till dig. Men det kanske inte känns lika lustigt när dataköparen är till exempel ett försäkringsbolag.

Amerikanska FDT har rapporterat om hur data säljs till försäkringsbolag som i sin tur använt köphistorik för att höja premierna på par som betalat för parterapi[156].

Andra exempel: hälsoappar som delat med sig data till hundra olika samarbetspartners om användares herpes, hiv och diabetes[157] och data brokers som lätt kan sätta ihop profiler under kategorier som ”deprimerade”. Frågan är vad som händer med människor som katalogiseras så; har deras försäkringspremier gått upp, har de fått riktad information och reklam till sig som gjort dem pillerberoende, har deras ränta på bolån gått upp?

Ytterligare ett: den katolska prästen som blev uthängd som homosexuell på grund av location data som sålts av en data broker[158].

Det är otroligt enkelt att köpa data från data brokers och den innehåller tillräckligt med information för att den ska gå att av-anonymisera. Konsekvensen av det är till exempel att utsatta kvinnor fått sin ”real-time location data” utlämnad till stalkers[159]. Och redan 2013 gick det att köpa uppgifter om människor som våldtagits och listor på människor med drog- och alkoholberoenden[160]. Återigen: vilka är köparna och hur utnyttjas informationen? Det är svårt att spekulera i några positiva utkomster ur den typen av datalistor.

Idag är det ett faktum att socialt utsatta personer far illa på grund av datainsamlingen och försäljningen av densamma. Men om man vill fundera lite på slutstationen för den här utvecklingen kan man rikta blicken mot Kina och landets så kallade social credit score system.

Kinas social credit score-system ger dig minuspoäng om du spelar för mycket tv-spel.

Det finns en rad missuppfattningar om det kinesiska social credit score-systemet. Den absolut vanligaste syntes redan i den förra meningen; det finns nämligen inte ett kinesiskt social credit score-system. Som forskaren Mareike Ohlberg, på the Mercator Institute for

”Det finns inte ett kinesiskt social credit score-system. Det finns flera. Om de lyckas med sin vision att sammankoppla dem alla kommer de att skapa något väldigt unikt. Men det är en del av en global trend.”

Mareike Ohlberg

China Studies, uttryckte det i en artikel i Wired[161].

”Till att börja med är detta inte ett kinesiskt fenomen, vilket inte heller användningen och missbrukandet av insamlad data och beteendeanalyser är. Det handlar inte heller om ett nationellt samlat system, utan om flera olika pilotprojekt som inte fungerar på exakt samma sätt. Men om de lyckas samla ihop dem, vilket visionen är, då kommer det att skapa något väldigt unikt. På det sättet är de kinesiska social credit score-programmen unika, men också en del av en global trend.”

De kinesiska social credit score-programmen registrerar alltså lite olika grejer, men innefattar totalt sett allt från sena betalningar av dina räkningar och att du kört mot rött ljus till att du betett dig illa på ett tåg eller i en taxi. Den här typen av poängsystem känns igen från västvärldens kreditvärdighet och betygsystem i tjänster som Uber. Det som gör att Kina sticker ut är kanske ambitionen att samla ihop allt. Mareike Ohlberg berättar till exempel om den kinesiska staden Rongcheng som gett alla invånare tusen poäng att börja med, och där avdrag sker när du till exempel beter dig dåligt i trafiken men där du kan plussa på poäng om du skänker pengar till välgörenhet.

Flera av pilotprojekten drivs av stora techbolag som Alibaba. Sesame Credit driver ett av dem och har gjort sig kända för att ha samlat in data om sina 400 miljoner kunder och delat ut betyg utifrån hur mycket tid de spenderat på tv-spel och om de är föräldrar eller ej[162]. I bolagets dejtingapp har social credit score funnits med som en parameter.

Ett annat känt exempel är hur den granskande journalisten Liu Hu nekades att köpa en flygbiljett för att han fått statusen ”not qualified”[163].

Jämförelserna med den fiktiva serien Black Mirror[164] är påtagliga. Man kan skämta om parodin i att din social score skulle komma att sänkas när du hängt på fel fester eller tappat humöret i matbuti-

ken. Problemet är bara att det här händer i verkligheten, här och nu, och att slutstationen för den här typen av massövervakning är total kontroll över människor. Allra värst blir det förstås för de socialt utsatta i samhället. Men man behöver inte vända blickarna mot Kina för att ge riktigt skrämmande exempel ur nutiden.

Du kanske säger att du ”inte har något att dölja”. Men vad händer när lagarna ändras?

När människor rättfärdigar massövervakning med ”jag har inget att dölja” finns det flera argument som motbevisar deras resonemang. Men inget har väl slagit hål på det lika bra som den samtida utvecklingen i USA. Ett stort problem med ”jag har inget att dölja” är ju att det inte är oföränderligt. Du kanske ändrar politisk uppfattning, blir aktivist och plötsligt får finna dig i att dina sökningar på internet får extra uppmärksamhet från myndigheterna. Du kanske blir deprimerad, köper mycket skräpmat och får se dina försäkringspremier skjuta i höjden. Du kanske är homosexuell och hittar en partner i ett land där det är förbjudet enligt lag.

Kanske lever du i villfarelsen av att ”du inte har något att dölja” men så ändras lagen och så är du kriminell. 2022 förändrades livet för miljontals amerikanska kvinnor som plötsligt inte längre kunde googla på abortläkare, köpa abortpiller online eller besöka abortkliniker (med telefonen i fickan) utan att det riskerade att bli bevis i ett potentiellt åtal mot dem. Plötsligt hade de något att dölja, och så som den digitala infrastrukturen ser ut i USA är det ingen enkel match. Har man som samhälle under lång tid förvandlat internet till en plats där både statliga och kommersiella aktörer kan kartlägga människors liv, då blir det tufft för de människorna den dagen en lag tar en ny riktning.

Direkt efter att Roe mot Wade upphävdes i juni 2022 kom nyhet efter nyhet om kvinnor som raderade sina graviditetsappar (åtmins-

tone de kvinnor som använde dem som hjälpmedel för att inte bli gravida) och det ett vettigt beslut av dem alla med tanke på att forskare rapporterat om att majoriteten av graviditetsappar delar stora mängder personlig data med andra bolag[165].

Tonen i diskussionerna om location data förändrades också. 2019 släppte New York Times sitt Privacy Project[166]. Tidningen hade kommit över en databas som innehöll location data på mer än tolv miljoner amerikaner. Datan innehöll mer än 50 miljoner så kallade location pings som påstods vara anonyma. Ändå tog det bara några minuter innan tidningen hade lyckats lista ut vilket av rörelsemönstren som tillhörde Donald Trump[167]. När det kommer till location data är det förstås hur enkelt som helst att avanonymisera den; eftersom det inte är många personer som sover på samma ställe som du och sen går till samma arbetsplats som du.

Ta nu den typen av databaser och plocka ut alla location pings som finns kopplade till en abortklinik och följ sedan deras resväg därifrån. Det här är inte en hypotetisk tankeövning. Vice har rapporterat[168] om att det för ynka 160 dollar går att köpa en hel veckas register över vilka människor som besökt en specifik klinik kopplat till graviditet – och att det även går att se var besökarna kom från och var de tog vägen efteråt. Det här är data som vem som helst kan köpa.

Vi har redan sett hur det blåst upp en perfekt storm på en mix av data brokers och deras tvivelaktiga dataregister, amerikanska delstaters vilja att sätta dit kvinnor som gör abort och giriga prisjägare. I Texas och Oklahoma kan invånarna, vem som helst, få upp till tio tusen dollar i belöning om de rapporterar kvinnor som brutit mot abortlagarna[169].

Det har byggts en digital infrastruktur som går ut på att kartlägga människors liv för att räkna ut vad de kommer att göra härnäst. Och i ett land som USA har myndigheterna inte bara sina egna verktyg, utan även i princip fri tillgång till de kommersiella bolag som följer

”Nu är vi oroliga för att kvinnor som söker efter abort ska bli övervakade. Samma apparat kan användas för att rikta in sig på vilken grupp som helst, när som helst, av vilken anledning som helst.”

Shoshana Zuboff

varenda steg vi tar. När man väl har ett sådant system på plats är det enkelt att rikta strålkastarljuset dit man vill. Som en artikel i New York Times uttrycker det[171]: ”Tänk er en kvinna som vanligtvis äter sushi regelbundet och plötsligt slutar med det och börjar ta vitamin B6 istället, hon kan enkelt bli identifierad som gravid. Om hon sedan inte föder ett barn är det inte otroligt att hon kommer att bli utfrågad av polisen.”

Det har till och med tagits fram AI-system för att räkna ut sannolikheten att unga tjejer ska bli gravida[172]. I ett samarbetsprojekt mellan Microsoft och en argentinsk organisation tog man 2018 fram algoritmer som de påstod hade en 86-procentig träffsäkerhet i att räkna ut vilka tjejer som skulle bli gravida inom en 6-årsperiod. Bakom den argentinska organisationen stod en känd abortmotståndare.

Abortfrågan är ett tydligt exempel på hur ”jag har inget att dölja” kan förändras. Men den är ”bara” ett exempel på en mycket bredare fenomen. Som Shoshana Zuboff sa i en intervju i Washington Post[173]:

”Den krassa verkligheten är att vi nu är oroliga för att kvinnor som söker efter abort ska bli övervakade; och samtidigt kan samma apparat användas för att rikta in sig på vilken grupp som helst, vilken liten del av en befolkning som helst – eller vår hela befolkning – när som helst, av vilken anledning som helst. Ingen går säker i det här.”

KONSEKVENSERNA AV MASSÖVERVAKNINGEN: SÅ HOTAR DATAINSAMLINGEN ETT FRITT SAMHÄLLE

Både den statliga och den kommersiella massövervakningen riskerar att förvandla fria demokratier till rena kontrollstater.

Auktoritära stater använder massövervakningen för att kontrollera befolkningen. Även i demokratiska länder ser vi direkta konsekvenser av en absurd datainsamling. Men det finns också mindre synliga effekter: både den statliga och kommersiella massövervakningen visar tecken på att kunna förvandla fria samhällen till den totala motsatsen.

Massövervakning är lika med kontroll. De mest uppenbara exemplen hittar vi i länder som Iran där internet censureras, invånarnas beteende online kontrolleras[174] och där så kallade smartcameras identifierar kvinnor som inte bär hijab[175].

Eller som i Ryssland där makten kombinerar massövervakning online[176] med en absurd mängd övervakningskameror med ansiktsigenkänning för att sätta dit journalister och regimkritiker[177].

Ännu värre: Kina med sin totala övervakning av invånarnas liv online[178], censurverktyget the great firewall of China[179] och förföljelse

av människor som deltar i protester[180]. Och inte minst landets övervakningskameror med teknik som påstås kunna avgöra människors etnicitet[181]. 2018 ansökte Huawei och the China Academy of Sciences om patent för just den typen av AI-kameror.

Den här övervakningstekniken använder Kina bland annat för att förfölja uigurerna i regionen Xinjiang. De registreras via tekniken som fått smeknamnet ras-AI och Human Rights Watch har rapporterat[182] om att staten under nio månader gjorde elva miljoner sökningar på närmare hälften av Urumqis 3,5 miljoner invånares telefoner. Resultatet av den massiva massövervakningen? Dokument som CNN kom över 2020 visade att miljontals uigurer först övervakats och sen fängslats[183] i arbetsläger på helt absurda grunder. Samtidigt har det rapporterats om att Kina testat en annan sorts ny teknik på uigurerna, där AI-kameror med så kallad ”emotion detection” använts för att registrera om en person är orolig eller inte[184]. Den kinesiska staten förnekar förstås detta och svarade BBC i en intervju att ”i Kina lever människor i harmoni oavsett vilken etnisk bakgrund de har, de lever ett stabilt och lugnt liv utan begränsningar i sin personliga frihet”.

Den granskande journalisten Liu Hu, som nekades att färdas med kollektivtrafiken för att han scorat dåligt i ett av Kinas social credit score-system, är av en annan uppfattning. För BBC berättade han[185]: ”Flera gånger har jag träffat vänner och direkt efteråt har regeringen kontaktat mig, varnat mig och sagt att jag inte ska träffa den och den personen, att jag inte ska göra det ena och det andra. Med artificiell intelligens har vi ingenstans att gömma oss.”

Undrar du hur Kina rättfärdigade det nya övervakningssystemet som nu förföljer hela folkgrupper? Det infördes efter att fem personer mördats 2016 i vad som staten beskrev som en terroristattack.

De här länderna har nått botten. Det kan alltid bli värre för befolkningen, men vi pratar inte om fria samhällen här. Frågan är hur mycket världens demokratier ska ta efter dem.

”2019 var mer än 70 länder utsatta för politiska manipulations-kampanjer via sociala medier. Antalet demokratier har rasat sedan den kommersiella datainsamlingen slog igenom på allvar runt 2010.”

Center for Humane Technology

Det finns massor med skräckexempel även i demokratiskt klassade länder. I både Europa och andra delar av världen har vi sett hur spionverktyget Pegasus använts för att övervaka meningsmotståndare, politiska aktivister och journalister[186]. Massövervakningen i USA är ett kapitel för sig och Snowdens avslöjanden visade hur extrema landets myndigheter är på området.

Den här typen av övervakning för tankarna till George Orwells 1984-dystopi med teleskärmar och en Storebror som alltid ser dig[187], tankepoliser och brist på yttrandefrihet. Men det finns andra element i de gamla dystopiböckerna, som pricksäkert förutsåg andra delar av vår samtid. Som propagandan och uppenbara fake news i 1984. Eller som i Aldous Huxleys Brave New World[188] där människorna knaprar lyckopiller (sociala medier och dopamin någon?), är uppenbart anti-intellektuella (Tikok någon?) och tror att de lever la dolce vita trots att deras frihet de facto glidit dem ur händerna.

Stora delar av världen har redan halkat in i någon sorts blandning av de två dystopierna. Och länderna som fortfarande klassas som fria demokratier står nu inför ett val: antingen samhällen som bygger på kontroll eller samhällen som bygger på kultur.

Redan idag ser vi hur massövervakningen kommer med ödesdigra konsekvenser i länder som är klassade som demokratier. Men massövervakningen är inte bara ett symptom. Den används också för att styra utvecklingen och putta fria länder åt fel håll. Hand i hand riskerar den statliga och den kommersiella massövervakningen att urvattna demokratiska samhällen. Det här är något som händer här och nu. 2019 var mer än 70 länder utsatta för politiska manipulationskampanjer[189] via sociala medier. Antalet globala demokratier har rasat[190] sedan den kommersiella massövervakningen slog igenom på allvar runt 2010.

”Vi har skapat en global generation av människor som uppfostrats i en miljö där själva meningen med kommunikation är manipulation.”

Meta och Google har blivit två av världshistoriens högst värderade bolag tack vare intäkterna från sina annonsnätverk och deras affärsidé är uppenbar. Den handlar om att kartlägga ditt beteende och förutse vad du kommer att efterfråga i framtiden för att kunna skräddarsy annonser så pricksäkert som möjligt. Ännu bättre: om de till och med kan styra ditt beteende i önskvärd riktning. Som Harvardprofessorn Shoshana Zuboff skriver i sin bok The Age of Surveillance Capitalism:

”Automatiserade maskinprocesser inte bara känner till våra beteenden utan också formar våra beteenden. I de tusentals transaktioner vi gör, så betalar vi för vår egen underkastelse.”

Det Zuboff pratar om är till exempel Metas AI-system som redan 2018, enligt läckta dokument[191,] hade kapaciteten att samla in tusen miljarder datapunkter varje dag för att producera sex miljoner beteendeförutsägelser per sekund.

Tristan Harris, tidigare design ethicist på Google och senare grundare för The Center of Humane Technology[192], är inne på samma spår som Zuboff i dokumentärfilmen Social Dilemma[193]:

”Vi riktar de här AI-motorerna mot oss själva för att demontera vad som framkallar reaktioner från oss. Det är som ett fängelseexperiment där vi drar in folk i Matrix och skördar alla pengar och all data från deras aktivitet för att göra vinst. Och vi är inte ens medvetna om det.”

I samma dokumentär menar Sean Parker, Facebooks första president, att bolagen från start var medvetna om vad de gjorde.

”Det är precis en sån sak en hackare som jag själv skulle komma på. För man exploaterar en sårbarhet i mänsklig psykologi. Jag tror att vi … ni vet, uppfinnarna, skaparna; jag själv och Mark (Zuckerberg) och Kevin Systrom på Instagram, alla de här människorna … vi var medvetna om det här och vi gjorde det ändå.”

”Vi letar efter ögonblicket då tekniken ska överträffa mänskligheten styrkor. Men det kommer ett ögonblick innan dess. När tekniken utnyttjar mänsklighetens svagheter. Och då är det schackmatt.”

Tristan Harris

Skaparna (åtminstone de som lämnat) av de största techbolagen spekulerar i att datainsamlingen och de AI-motorer som analyserar miljardtals internetanvändare kan bli slutet för oss. Som Tristan Harris säger:

”Vi letade alla efter ögonblicket då tekniken skulle överträffa mänskligheten styrkor och intelligens. Men det finns något som kommer innan dess och det är när tekniken utnyttjar mänsklighetens svagheter. När den hittar roten till missbruk, polarisering, radikalisering, upprördhet och fåfänga … hela grejen. När den gör det, det är då den överträffar den mänskliga naturen. Och då är det schackmatt på mänskligheten.”

Jaron Lanier är en av skaparna av virtual reality, men nu förespråkar han att vi borde lägga ner sociala medier för gott[194].

”Sociala medier manipulerar mänskligt beteende och hotar vår fria vilja. De bidrar till massproduktion av missinformation. Det är dags att lägga ner.”

I Social Dilemma[195] säger han:

”Vi har skapat en värld där online-anslutning blivit primärt, särskilt för yngre generationer. I den världen, när än två människor knyter an, är allt finansierat genom en lömsk tredje person som betalar för att manipulera dem. Så vi har skapat en global generation av människor som uppfostrats i en miljö där själva meningen med kommunikation, själva meningen med kultur, är manipulation. Vi har satt bedrägeri och lömskhet i centrum av allt vi gör.”

Eller som Shoshana Zuboff resonerar i dokumentären The Big Data Robbery[196]:

”När Chris Wiley (visselblåsaren som avslöjade Cambridge Analytica-skandalen) berättade sin historia för the Guardian 2018 sa han att de visste så mycket om så många människor att vi kunde förstå deras inre demoner och vi kunde räkna ut hur vi skulle rikta in oss på de demonerna, vi förstod hur vi skulle rikta in oss på deras rädsla,

deras ilska, deras paranoia och när vi riktat in oss på dem kunde vi trigga deras känslor och genom att trigga deras känslor kunde vi manipulera dem att klicka på en hemsida, gå med i en grupp, få dem att läsa vad vi ville, få dem att välja vilka personer de skulle hänga med, och till och med få dem att rösta i valet så som vi ville."

Absurd datainsamling och AI-system som attackerar människors rädslor hjälpte Trump att vinna valet. Idag används massövervakningen för att övervaka kvinnor som vill göra abort.

Var och en som lever med sociala medier och i dagens digitala värld borde fundera på personprofilerna som AI-systemen tar fram: används de på ett bra eller dåligt sätt? Om någon klassas som deprimerad, får den personen då riktat innehåll till sig som handlar om att gå ut och springa i skogen eller reklam för mängder med läkemedel? En person som köper ohälsosamt mycket läsk; innebär det förslag på en alternativ livsstil eller rabatt på Coca-Cola? För någon som börjat läsa på om konspirationsteorier; reklam för böcker utgivna av universitet eller förslag på sidor om fejkade månlandningar och att jorden är platt?

I ett läckt dokument till The Australian[197] har det visat sig att Meta erbjudit annonsköpare möjligheten att rikta sin reklam till mer än sex miljoner unga användare (barn) baserat på tillfällen då de känner sig (och här citerar vi kategorierna): värdelösa, osäkra, stressade, slagna, oroliga och misslyckade.

”Låt oss inte vara naiva. Makthavare kommer att frestas att använda de här systemen över våra huvud och emot oss. När vi gör motstånd idag, då kämpar vi för att för att samhället ska vara fritt för kommande generation.”

Shoshana Zuboff

Samma taktik som används för att sälja produkter och tjänster används för att tilta användare i politisk riktning. Shoshana Zuboff igen[198]:

”Cambridge Analytica-skandalen var helt enkelt en mimik på den kommersiella massövervakningen. Men istället för att manipulera människor i kommersiellt syfte gjorde man det för politisk vinning. Istället för ett köp, en röst. Demokratin i Storbritannien, USA och många andra länder hänger i en lös tråd, tack vare den kommersiella massövervakningen.”

Tristan Harris, alltså han som tidigare var design ethicist på Google men som nu driver The Center of Humane Technology, använder siffror för att tydliggöra hur dagens datainsamling och den rådande sociala medier-världen påverkar politiken[199]: 19 procent av alla tweets om det amerikanska presidentvalet 2016 gjordes av bottar. Inför valet 2020 var Facebooks mest besökta sidor för kristna och svarta amerikaner administrerade av trollfabriker.

Och algoritmerna som de sociala medierna bygger på är skapade för att främja kaos: ord som accelererar polarisering ökar mängden retweets med 17 procent. Varje negativt ord om en politisk motståndare ger en skjuts med 67 procent.

MIT har i sin tur siffror[200] på hur fake news sprids snabbare än riktiga nyheter. Och ytterligare forskning har visat att Facebooks algoritmer knuffat användare ner i konspiratoriska kaninhål, att Meta vetat om det men ändå inte gjort något åt det[201].

Vi har alltså en digital infrastruktur som samlar in precis allt vi gör och som främjar radikalt och osant innehåll. Har man ett sådant system på plats är det klart att det kommer att utnyttjas. Som när bolaget Cambridge Analytica[202] (där Donald Trumps chefsstrateg Steve Bannon var inblandad) fick tillgång till 87 miljoner Facebookanvändares personliga data (inklusive privata meddelanden) som de sedan stoppade in i egna AI-system. Ut kom personprofiler som Cambridge Analytica använde för att skräddarsy digitalt innehåll

som riktades till invånare som stod och vägde mellan hur de skulle rösta i presidentvalet mellan Donald Trump och Hillary Clinton. De sponsrade inläggen byggde på mottagarnas rädslor, de var utformade på ett radikalt sätt för att trigga algoritmerna[203] och innehöll rena fake news[204].

I en intervju berättade visselblåsaren Christopher Wylie[205] om konsekvenserna:

”Sättet som vi viskade olika saker till olika människor riskerar att fragmentera samhället på ett sätt som gör att vi inte längre har någon gemensam och delad upplevelse, som gör att vi inte har någon delad förståelse. Och om vi inte har en gemensam och delad förståelse av samhället, hur ska vi då kunna fungera som samhälle?”

I Netflix-dokumentären The Great Hack[206] berättar Cambridge Analyticas vd att de inte var det enda bolaget inblandade i valet på det här sättet. Plussa på det faktum att ryska trollfabrikerna är inne och härjar inför amerikanska val[207] och uppgifterna om att Cambridge Analytica sägs ha varit insyltade i tvåhundra valrörelser[208] runt om i världen. Fram växer en bild av hur den kommersiella datainsamlingen får konsekvenser långt bortom riktade annonser för den där tröjan som du tittat på en gång.

Vi har alltså sett bevis på hur insamlad data, tillsammans med algoritmer och AI-system som bygger på människors rädslor och osäkerhet, använts för att sprida fejkade nyheter och bidra till att Donald Trump kunde vinna presidentvalet. Vid makten förändrade Trump abortlagarna och nu används massövervakningen för att övervaka kvinnor, som står inför det plötsliga faktum att deras önskade abort är olaglig.

I dokumentären The Big Data Robbery[209] uppmanar Shoshana Zuboff invånarna i demokratier att inte vara naiva.

“Vår personliga integritet försakas för den här marknadslogikens skull. Det är inte acceptabelt. Och låt oss inte vara naiva. När vi har

fel makthavare på plats så kommer de att titta på de ofantliga kontrollmöjligheter som det här systemet erbjuder. Det kommer en tid då vi, även i västvärlden, även i våra demokratiska samhällen, kommer att få se en regering som frestas av att använda de här systemen över våra huvud och emot oss. Låt oss inte vara naiva gällande det. När vi bestämmer oss för att göra motstånd mot övervakningskapitalismen här och nu, då kämpar vi också för vår demokratiska framtid, då kämpar vi för den typen av kontrollfunktioner som vi kommer att behöva för att vårt informationssamhälle ska förbli fritt och demokratiskt i ytterligare en generation."

"Personlig integritet är grunden för alla andra rättigheter. Yttrandefrihet betyder inte mycket om du inte har personlig integritet."

Det Shoshana Zuboff pratar om är ett motstånd som måste komma nu, innan det är för sent. Det är en viktig poäng. Eftersom infrastrukturen som byggs idag kommer att användas av framtida regeringar. Eftersom vi inte vet vilka som kommer till makten. Och eftersom den här typen av övervakningssamhällen tenderar att komma smygandes dolt inför den stora massan. Ändamålsglidningen är total på det här området. Vägen till helvetet är, som känt, kantat av goda intentioner och det är svårt att upptäcka den större bilden när den läggs en liten pusselbit i taget. Varje obskyr liten lag som införs innebär kanske inte en katastrof, men tillsammans tar de oss i fel riktning. Och slutstationen är solklar: när ett land infört total massövervakning börjar folket självcensurera sig. När de inte kan vara säkra på om de är övervakade eller ej kommer de att vakta sin tunga. I ett Ted Talk berättar Glenn Greenwald, en av journalisterna som träffade Edward Snowden på det där hotellrummet i Hongkong och som hjälpte honom med visselblåsningen, om hur just självcensuren är en utstuderad kontrollmetod med flera hundra år på nacken[210].

”Under 1700-talet fick filosofen Jeremy Bentham uppgiften att klura på ett problem: ett fängelse hade blivit så stort att de inte hade möjligheten att kontrollera var och en av de intagna. Han kallade sin lösning för panoptikonen; ett enormt torn i mitten av fängelset där man när som helst kan ta en titt på vem som helst av fångarna. Det gick inte att titta på alla fångarna samtidigt, men den avgörande designen var att fångarna inte kunde se in i panoptikonen. De kunde aldrig veta om de var iakttagna eller inte. Det här gjorde Bentham väldigt upphetsad; fångarna skulle behöva anta att de övervakades vid varje givet ögonblick, vilket var det ultimata sättet att upprätthålla lydnad och efterlevnad. Den franske 1900-talsfilosofen Michel Foucault insåg att den här modellen kunde användas inte bara för fängelser utan för varje institution som försöker kontrollera mänskligt beteende: skolor, sjukhus, fabriker, arbetsplatser. Han sa att detta tankesätt, detta ramverk som upptäcktes av Bentham, var nyckeln till samhällskontroll i moderna, västerländska samhällen, som inte längre behövde tyrannens vapen – att straffa eller fängsla eller döda eller tvinga lojalitet till ett visst parti – eftersom massövervakning skapar ett fängelse i sinnet som är mer subtilt men mycket effektivare när det kommer till att främja efterlevnad av sociala normer eller social ortodoxi, betydligt mer effektivt än vad brutalt våld någonsin kan bli.”

I samma Ted Talk pratade Greenwald även om den nedkylande effekt som massövervakning har på samhällen:

“När vi vet att vi kan bli övervakade, när vi vet att vi kan bli iakttagna, då förändras vårt beteende dramatiskt. Bredden av möjliga beteenden som vi överväger krymper kraftigt när vi tror att vi blir observerade. Det är helt enkelt så den mänskliga naturen ser ut och det har erkänts inom samhällsvetenskap och i litteratur och inom religion och inom i princip varenda disciplin som finns. Det finns dussintals psykologiska studier som bevisar detta.”

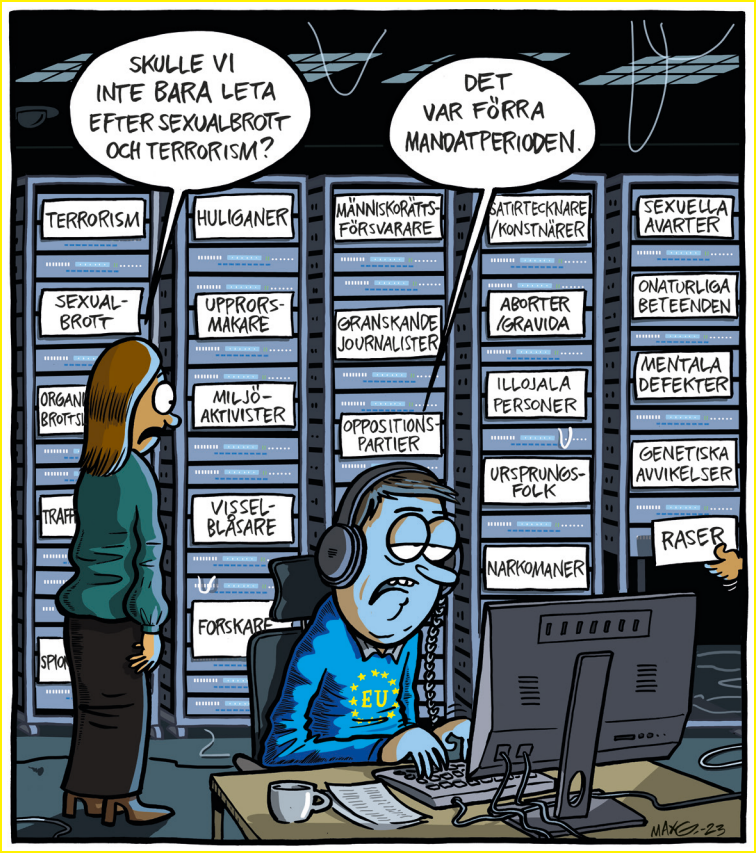
Shoshana Zuboff [211]:

"Personlig integritet innebär att vi kan bestämma vad vi vill hålla privat och vad vi vill dela med andra. De här massövervakningssystemen är ett direkt angrepp på den mänskliga handlingsfriheten, på den individuella suveräniteten, och de utmanar de mest grundläggande rättigheterna till autonom handling. Utan mänsklig handlingsfrihet finns det ingen frihet, och utan frihet finns det ingen demokrati."

Edward Snowden [212]:

"Personlig integritet är det som ger dig möjligheten att berätta för världen vem du är, på dina egna villkor, att berätta för världen vem du försöker att vara, och att du samtidigt kan skydda de delarna av dig själv som du inte är säker på, som du fortfarande utforskar. Om vi inte har personlig integritet förlorar vi möjligheten att göra misstag, vi förlorar möjligheten att vara oss själva. Personlig integritet är grunden för alla andra rättigheter. Yttrandefrihet betyder inte mycket om du inte får ha en fri plats inom dig själv, i dina tankar, bland dina vänner, i ditt hem … där du kan bestämma vad du faktiskt vill säga."

Egentligen är det ganska enkelt. Antingen har vi ett samhälle där människor har rätt till sina egna tankar, sina privata samtal och ett utrymme att testa sina idéer. Ett fritt samhälle där utveckling och förändring är möjlig. Där makten kan utmanas, granskas och bytas ut. Eller så har vi ett stängt samhälle där du aldrig vet om du är övervakad eller ej. Antingen fortsätter vi ta steg för steg mot odemokratiska samhällen. Eller så försöker vi istället hålla fast vid artikel 12 i den allmänna förklaringen om de mänskliga rättigheterna: "Ingen får utsättas för godtyckligt ingripande i fråga om privatliv."


SKULLE VI INTE BARA LETA EFTER SEXUALBROTT OCH TERRORISM?
DET VAR FÖRRA MANDATPERIODEN.
TERRORISM
SEXUAL-BROTT
HULIGANER
UPPRORS-MAKARE
MILJÖ-AKTIVISTER
VISSEL-BLÅSARE
FORSKARE
MÄNNISKORÄTTS-FÖRSVARARE
GRANSKANDE JOURNALISTER
OPPOSITIONS-PARTIER
SATIRTECKNARE /KONSTNÄRER
ABORTER /GRAVIDA
ILLOJALA PERSONER
URSPRUNGS-FOLK
NARKOMANER
SEXUELLA AVARTER
ONATURLIGA BETEENDEN
MENTALA DEFEKTER
GENETISKA AVVIKELSER
RASER
EU

KONSEKVENSERNA AV MASSÖVERVAKNINGEN: VI HAR ALLA NÅGOT ATT DÖLJA

Till dig som inte har något att dölja:

En dag kanske du har det. Eftersom det inte är du som sätter reglerna.

Det absolut vanligaste försvarstalet för massövervakning är ”om du inte har något att dölja har du inget att frukta”. Säg det till kvinnorna i stater där abort plötsligt förbjudits. Säg det till granskande journalister i auktoritära länder. Att säga ”jag har inget att dölja” är att sluta bry sig om alla de som kämpar för sin frihet. Och en dag kanske du är en av dem.

Den här texten är till dig som säger att du inte har något att dölja. Vi har skrivit den eftersom det är det absolut vanligaste argumentet från människor som är likgiltiga inför massövervakning eller till och med förespråkar den. Den långa versionen av uttrycket lyder ”har du inget att dölja har du inget att frukta” och den har praktiserats av myndigheter i hundra år. Något remixade versioner av den har också använts av de kommersiella massövervakarna. Av Mark Zuckerberg och av Googles tidigare vd Eric Smith[213] som sagt: ”Om du gör något som du inte vill att andra ska veta om, då kanske du inte skulle ha gjort det från första början.”

Till att börja med är det här en fras som ter sig väldigt olika beroende på vilket land du befinner dig. På väldigt många platser i världen finns det mängder med människor som faktiskt har något att dölja. Som granskande journalister som förföljs i auktoritära länder. Som homosexuella i länder där det är förbjudet. Som politiska motståndare som övervakas av totalitära stater. Som kvinnor som söker efter abort i stater som gjort det olagligt. Som människor som lever under skyddad identitet och inte vill riskera att den läcker.

Att säga att ”den som inte har något att dölja har inget att frukta” är världsfrånvänt och det är lika med att inte bry sig om alla de här människorna som faktiskt har något att frukta – många av dem riskerar sitt liv om de inte kan dölja vilka de är, vad de tror på och vad de kämpar för.

”Har du rent mjöl i påsen har du inget att oroa dig för” är ett tankemönster som är så otroligt ogenomtänkt. I en värld där bara brottslingar anses vara de som har något att dölja är det slut på företagshemligheter. I en sådan värld riskerar känslig hälsodata att läcka varje dag. För att inte prata om politiker som bär på information som inte får hamna i främmande händer – eller är det helt enkelt så att de styrande inte ska leva under samma regler som folket?

Argumentet ”har du inget att dölja har du inget att frukta” är i grunden bakvänt. Medborgare ska inte behöva förklara för staten (eller företag) varför de inte vill bli övervakade. Tvärtom, staten ska kunna förklara varför de rotar i någons privatliv.

För det är ju så, vi har faktiskt alla något att dölja: vårt privatliv, som ingen annan har att göra med, så länge du inte är misstänkt för brott och en oberoende, fri och demokratisk domstol utfärdat en order om att en proportionerlig övervakning behövs.

Från politiker och myndigheter kommer uttrycket ofta med tillägget: ”för att hålla oss alla säkra måste vi offra lite av vår integritet”. Men som Benjamin Franklin en gång sa[214]: ”De som är redo att

offra frihet för att få lite tillfällig säkerhet tillbaka, förtjänar varken frihet eller säkerhet." Eller som den amerikanske kryptografen och säkerhetsexperten Bruce Schneier beskriver det[215]:

"Alldeles för många kategoriserar debatten fel. Som om det handlar om ett val mellan 'säkerhet eller privacy'. Men det verkliga valet är mellan frihet och kontroll. Frihet kräver säkerhet utan intrång, friheten kräver säkerhet plus personlig integritet. En utbredd polisövervakning är själva definitionen av en polisstat. Och det är därför vi bör kämpa för personlig integritet även när vi inte har något att dölja."

Bruce Schneier är inne på något viktigt, som handlar om att en stat inte ska ha total makt[216].

"Absolut makt korrumperar. Och vem övervakar övervakarna? Privacy handlar om att skydda folket mot de som sitter på makten och potentiellt kan missbruka den."

Edward Snowden argumenterar för samma sak under parollen: Privacy is for the powerless. Transparency is for the powerful[217].

"Du ska inte behöva förklara varför du vill att staten ska lämna dig ifred. Det naturliga tillståndet i ett fritt samhälle är att vi får vara fria. Om de vill begränsa oss och övervaka oss, då förändras själva naturen av ett mänskligt samhälle."

"När du säger att du inte har något att dölja bettar du på att du aldrig kommer att ha något att dölja i ett system som förändras men som aldrig glömmer."

Grunden för ett demokratiskt samhälle är att invånarna har rätt till personlig integritet. Men låt oss säga att du fortfarande tycker att det är okej med massövervakning för att "du inte har något att dölja"; problemet med "nothing to hide" är att det inte är ett tillstånd som är oförändbart. Fråga bara de kvinnor som levt i amerikanska delstater under föreställningen att de inte haft något att dölja, men så ändra-

des lagen över en natt och så var det inte längre lagligt för dem att göra abort.

Glenn Greenwald var en av journalisterna som hjälpte Edward Snowden att visselblåsa. I ett Ted Talk under titeln Why Privacy Matters[218] illustrerade han hur massövervakning inte tar hänsyn till förändring varken hos makthavarna eller hos de som övervakas.

”När du säger ’någon som gör dåliga saker’ så menar du förmodligen saker som att planera en terroristattack eller delta i någon grov brottslighet. Men det är en mycket snävare beskrivning än vad makthavarna menar när de säger ’någon som gör dåliga saker’. Hos människorna som köper detta tankesätt finns det en underförstådd acceptans: att du är villig att göra dig själv tillräckligt harmlös och tillräckligt ohotad, inför de som utöver den politiska makten, och då och först då kan du bli fri från farorna med massövervakningen. Det är bara de som är oliktänkande, som utmanar makten, som har något att oroa sig för. Och det finns alla möjliga anledningar till att vilja undvika detta. Du kanske är en person som just nu inte vill engagera dig, men någon gång i framtiden kanske du ändrar dig. Och även om du aldrig skulle vilja engagera dig, så är det faktum att det finns andra människor som är villiga och har möjligheten att göra motstånd – journalister och aktivister och en hel bunt andra – något som är gott för oss alla och något som vi skulle borde vilja bevara.”

Edward Snowden, i ett samtal anordnat av the Tor Project[219]:

”Den här typen av spårning och övervakning av hela befolkningar som vi ser idag … du kommer inte att se konsekvenserna av det idag. När vi pratar om internet, när vi pratar om övervakning, då pratar vi om makt. De spionerar inte på oss och de övervakar inte oss för att de tycker att det är intressant. De gör det inte för att det är kul. De är inte intresserade av data för data, de är inte akademiker, de jobbar inte på en studie. De gör det för att det ger dem inflytande. Det tillåter dem att forma vårt beteende, det tillåter dem att visa dig något som du

”Att säga att man inte bryr sig om integritet för att man inte har något att dölja är som att säga att man inte bryr sig om yttrandefrihet för att man inte har något att säga. Eller att man inte bryr sig om pressfrihet för att man inte tycker om att läsa.”

Edward Snowden

inte annars skulle ha sett, som de tror att du kommer att klicka på och som de hoppas kommer att leda eller missleda dig i framtiden. Det kommer inte att fungera varje gång, det kommer inte att fungera på tusen försök, men sen när de försökt ett tusen och en gång, då funkar det plötsligt och steg för steg börjar de kontrollera individer och via individer börjar de kontrollera grupper och via grupper kommer de att börja kontrollera samhället. Och sen är vi fast. Och när jag säger att du inte kommer att känna av konsekvenserna idag, då menar jag att människor som säger ’jag bryr mig inte, det där betyder inget för mig och du vet, jag kollar ändå inte på något intressant på internet’, då har du gjort dig sårbar för ett system som aldrig glömmer. Det du gör är att du bettar på följande: om du inte har något intressant att säga idag, om du inte har något provokativt eller kontroversiellt att säga idag, om du inte tillhör en minoritet idag, så kommer du heller aldrig att göra det. Men du vet inte hur morgondagen ser ut, du

vet inte hur samhället kommer att se ut imorgon. Den här typen av system, både de statliga och de kommersiella, försöker skapa vad de kallar friktionslösa system. Vad de menar med det är att de på ytan laddas med glädje; bilderna du vill se, konversationerna du vill åt, de där endorfinerna och dopaminkickarna som du vill ha. Tillbaka får de konsekvenserna. De gömmer det, de gör det dolt, och det kommer inte att gå upp för dig förrän om fem år, om tio år, om tjugo år. Men när du väl förstår det, då är det för sent att backa bandet, då är det för sent att skydda sig själv."

I grund och botten är "jag har inget att dölja" helt irrelevant i diskussionen om massövervakning. För det handlar inte om just dig. Personlig integritet är en mänsklig rättighet och det finns människor över hela världen som inte har lyxen att resonera i termer huruvida de har något att dölja eller inte, eftersom de lever under konstant förtryck. Att kämpa för privacy handlar om att kämpa för dem, här och nu. Och för att alla som inte lever under totalitära makter inte själva ska hamna där en dag. Som Edward Snowden skriver i sin bok Permanent Record:

"Eftersom en befolknings friheter är ömsesidigt beroende av varandra innebär det att du ger upp allas rätt om du ger upp din egen. Du kan välja att ge upp den av bekvämlighet, eller under den populära förevändningen att privatliv endast är ett krav för dem som har något att dölja. Men att säga att du inte behöver eller vill ha integritet för att du inte har något att dölja är att anta att ingen bör ha, eller kan ha, något att dölja, inklusive sin invandrarstatus, arbetslöshetshistoria, finansiella historia eller sjukjournal. Du antar att ingen, inklusive du själv, kan ha något emot att avslöja någon information om sina religiösa övertygelser, sin politiska tillhörighet eller sina sexuella aktiviteter, lika lättsinnigt som en del väljer att avslöja sina preferenser inom film, musik eller litteratur.

Att säga att man inte bryr sig om integritet för att man inte har något att dölja är ytterst detsamma som att säga att man inte bryr sig om yttrandefrihet för att man inte har något att säga. Eller att man inte bryr sig om pressfrihet för att man inte tycker om att läsa. Eller att man inte bryr sig om religionsfrihet för att man inte tror på gud. Eller att man inte bryr sig om mötesfrihet för att man är en lat, antisocial agorafob. Bara för att den ena eller den andra friheten kanske inte har betydelse för dig idag behöver den inte sakna mening imorgon, för dig eller din granne, eller för de massor av principfasta dissidenter som jag följde på min telefon och som protesterade halvvägs runt planeten i hopp om att vinna bara en bråkdel av de friheter som mitt land var i fulla färd med att montera ned.”

”Bara för att den ena eller andra friheten kanske inte har betydelse för dig idag behöver den inte sakna mening imorgon, för dig eller din granne, eller för de som protesterar halvvägs runt jorden i hopp om att vinna bara en bråkdel av de friheter som mitt land var i full färd med att montera ned.”

Edward Snowden

KÄLLOR

Klickbara källor finns på mullvad.net

[1] Wired: Cambridge Analytica Could Have Also Accessed Private Facebook Messages

[2] BBC: Facebook's data-sharing deals exposed

[3] The New York Times: As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants.

[4] The Guardian: The Cambridge Analytica Files

[5] The New York Times: Facebook's Data Sharing and Privacy Rules: 5 Takeaways From Our Investigation.

[6] Signal.org

[7] The New York Review: "We Kill People Based on Metadata"

[8] Johns Hopkins University: The Price of Privacy: Re-Evaluating the NSA

[9] Contrachrome.com

[10] VPRO Documentary: Shoshana Zuboff on surveillance capitalism

[11] Contagious: Shoshana Zuboff on the age of surveillance capitalism

[12] The intercept: Facebook Engineers: We Have No Idea Where We Keep All Your Personal Data

[13] The Guardian: Privacy no longer a social norm, says Facebook founder

[14] EFF: Google CEO Eric Schmidt Dismisses the Importance of Privacy

[15] Gawker.com: Google CEO: Secrets Are for Filthy People

[16] Business Insider: Google CEO: "We Know Where You Are. We Know Where You've Been. We Can More Or Less Know What You're Thinking About."

[17] Humanetech.com

[18] Thesocialdilemma.com

[19] The Harvard Gazette: High tech is watching you

[20] Vice: Internet Service Providers Collect, Sell Horrifying Amount of Sensitive Data, Government Study Concludes.

[21] Vice: Internet Service Providers Collect, Sell Horrifying Amount of Sensitive Data, Government Study Concludes.

[22] Vice: Internet Service Providers Collect, Sell Horrifying Amount of Sensitive Data, Government Study Concludes.

[23] Daily Mail: To read, or not to read... the terms and conditions: PayPal agreement is longer than Hamlet, while iTunes beats Macbeth.

[24] The Washington Post: I tried to read all my app privacy policies. It was 1 million words.

[25] FTC: FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations.

[26] Time: The Most Important Things to Know About Apps That Track Your Location

[27] Bloomberg: Meta Signs $37.5 Million Deal Over Facebook Location Tracking

[28] Politico: Facebook parent company to settle Cambridge Analytica scandal lawsuit for $725M

[29] The Guardian: The Cambridge Analytica Files

[30] The Intercept: Facebook Engineers: We Have No Idea Where We Keep All Your Personal Data

[31] Vice: Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document

[32] ProPublica: Facebook Doesn't Tell Users Everything It Really Knows About Them

[33] The Markup: Facebook Is Receiving Sensitive Medical Information from Hospital Websites

[34] Bleeping Computer: Misconfigured Meta Pixel exposed healthcare data of 1.3M patients

[35] CNBC: Meta fined over $400 million by top EU regulator for forcing users to accept targeted ads

[36] The Markup: How We Built a Real-time Privacy Inspector

[37] Bloomberg: Zuckerberg Says Facebook Collects Internet Data on Non-Users

[38] Sveriges Radio: Facebook collects intimate customer data from over 100 European pharmacies

[39] ProPublica: Facebook Doesn't Tell Users Everything It Really Knows About Them

[40] The Intercept: Facebook Uses Artificial Intelligence to Predict Your Future Actions for Advertisers, Says Confidential Document

[41] Google Patents: US10149111B1

[42] Buzzfeed News: Facebook Filed A Patent To Calculate Your Future Location

[43] Bloomberg: Meta Sued for Skirting Apple Privacy Rules to Snoop on Users

[44] Techradar: Facebook reveals it can track users location even if they turn off location services

[45] The Guardian: The Cambridge Analytica Files

[46] Buzzfeed News: Here Are 18 Things You Might Not Have Realized Facebook Tracks About You

[47] Forbes: Security Researcher Finds Facebook App Tracking iPhone Movements

[48] The Guardian: Boot up: Facebook self-censorship, Tufte in brief, developer intention, and more.

[49] Daily Mail: Facebook can predict when you'll get married, change jobs and even DIE: Patents reveal the shocking algorithms the firm runs on its users

[50] The Markup: How We Built a Real-time Privacy Inspector

[51] Daily Mail: How Google is using fonts to track what you do online and sell data to advertisers - and what you can do about it

[52] Statista: Google's Search Dominance

[53] Statista: Global market share held by leading desktop internet browsers from January 2015 to December 2022

[54] Contrachrome.com

[55] The Guardian: Google will pay $392m to 40 states in largest ever US privacy settlement

[56] Chromeunboxed.com: Google Analytics banned in several European countries due to GDPR violations

[57] Politico: Washington wants to break up Google. But Europe is way ahead.

[59] EFF: Google's FLoC Is a Terrible Idea

[60] Time: Europe Is Saving Democracy From Big Tech, Says the Author of Surveillance Capitalism

[61] Wired: Google Will Delete Your Data by Default—in 18 Months

[62] The Washington Post: Okay, Google: To protect women, collect less data about everyone.

[63] The Washington Post: Google promised to delete sensitive data. It logged my abortion clinic visit.

[64] The Guardian: Google under scrutiny over pledge to protect abortion location data

[65] The Guardian: TikTok has been accused of 'aggressive' data harvesting. Is your information at risk?

[66] TikTok.com: Privacy Policy

[67] Wired: All the ways Amazon tracks you and how to stop it

[68] Business Insider: Amazon is introducing new tech to monitor shoppers in its grocery stores and share data with advertisers

[69] Forbes: Mastercard, AmEx And Envestnet Profit From $400M Business Of Selling Transaction Data

[70] Wired: Forget Facebook, mysterious data brokers are facing GDPR trouble.

[71] The Markup: The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users

[72] FTC: FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations.

[73] Vice: Data Broker Is Selling Location Data of People Who Visit Abortion Clinics

[74] Time: The Most Important Things to Know About Apps That Track Your Location

[75] Worldprivacyforum.org: Congressional Testimony: What Information Do Data Brokers Have on Consumers?

[76] CBS News: The Data Brokers: Selling your personal information

[77] ProPublica: Facebook Doesn't Tell Users Everything It Really Knows About Them

[78] Wired: It's time to ditch Chrome

[79] Reuters: Google faces $5 billion lawsuit in U.S. for tracking 'private' internet use

[80] Vice: Internet Service Providers Collect, Sell Horrifying Amount of Sensitive Data, Government Study Concludes.

[81] The Tor Project: Browser Fingerprinting: An Introduction and the Challenges Ahead

[82] The Guardian: Boot up: Facebook self-censorship, Tufte in brief, developer intention, and more.

[83] Arvind Narayanan and Vitaly Shmatikov, The University of Texas at Austin: Robust De-anonymization of Large Sparse Datasets.

[84] Latanya Sweeney, Harvard University: Matching Known Patients to Health Records in Washington State Data.

[85] Techcrunch: Researchers spotlight the lie of 'anonymous' data

[86] Nature.com: Unique in the Crowd: The privacy bounds of human mobility

[87] Science.org: Unique in the shopping mall: On the reidentifiability of credit card metadata

[88] United Nations: Universal Declaration of Human Rights

[89] LeakSourcetv: CIA's Chief Tech Officer on Big Data: We Try to Collect Everything and Hang Onto It Forever

[90] The Guardian: Welcome to Utah, the NSA's desert home for eavesdropping on America

[91] Center for democracy & technology: Section 702: What It Is & How It Works

[92] The Guardian: NSA collecting phone records of millions of Verizon customers daily

[93] The Guardian: NSA collects millions of text messages daily in 'untargeted' global sweep

[94] The Guardian: XKeyscore: NSA tool collects 'nearly everything a user does on the internet'

[95] The Guardian: XKeyscore presentation from 2008 – read in full

[96] The Guardian: All the data about your data

[97] The Washington Post: U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program

[98] ABC News: Dissecting Big Tech's Denial of Involvement in NSA's PRISM Spying Program

[99] EFF: Upstream vs. PRISM

[100] The New York Times: AT&T Helped U.S. Spy on Internet on a Vast Scale

[101] The Guardian: Glenn Greenwald: how the NSA tampers with US-made internet routers

[102] The New York Review: 'We Kill People Based on Metadata'

[103] Citizenfourfilm.com

[104] Theintercept.com/staff/glenn-greenwald/

[105] Reuters: Snowden says NSA engages in industrial espionage: TV

[106] The Guardian: Edward Snowden: US government spied on human rights workers

[107] Le Monde: France in the NSA's crosshair : phone networks under surveillance

[108] The Guardian: NSA monitored calls of 35 world leaders after US official handed over contacts

[109] Wikipedia: Global surveillance disclosures (2013–present)

[110] WikiLeaks: Vault 7: CIA Hacking Tools Revealed

[111] Vice: The CIA Spied on People Through Their Smart TVs, Leaked Documents Reveal

[112] The Guardian: 'No regrets,' says Edward Snowden, after 10 years in exile

[113] The Guardian: States haven't stopped spying on their citizens, post-Snowden – they've just got sneakier.

[114] Wired: A simple guide to GCHQ's internet surveillance programme Tempora

[115] Amnesty: Why we're taking the UK government to court over mass spying

[116] The Guardian: GCHQ taps fibre-optic cables for secret access to world's communications

[117] The Guardian: GCHQ taps fibre-optic cables for secret access to world's communications

[118] Forbes: NSA Responds To Snowden Claim That Intercepted Nude Pics 'Routinely' Passed Around By Employees

[119] The Guardian: GCHQ's mass data interception violated right to privacy, court rules

[120] The Guardian: NSA surveillance exposed by Snowden was illegal, court rules seven years on.

[121] Politico: Europe's state of mass surveillance

[122] Noyb: CJEU declares Meta's GDPR approach illegal.

[123] France24: Critics claim Paris using 2024 Games to introduce Big Brother video surveillance

[124] Freedom House: Hungary

[125] Mullvad.net/chatcontrol

[126] The Verge: The UK's tortured attempt to remake the internet, explained.

[127] The Guardian: The Pegasus Project

[128] The Guardian: A data 'black hole': Europol ordered to delete vast store of personal data

[129] Freedom House: Countering an Authoritarian Overhaul of the Internet

[130] The Intercept: Hacked Documents: How Iran Can Track and Control Protesters' Phones

[132] The New York Times: When Nokia Pulled Out of Russia, a Vast Surveillance System Remained

[133] Wired: Inside Safe City, Moscow's AI Surveillance Dystopia

[134] The Washington Post: Russia's surveillance state still doesn't match China. But Putin is racing to catch up.

[135] The New York Times: How Investigative Journalism Flourished in Hostile Russia

[136] Wikipedia: Mass surveillance

[137] Freedom House: Explore the map

[138] South China Morning Post: How China's surveillance state was a mirror to the US for whistle-blower Edward Snowden

[139] CNBC: China has launched another crackdown on the internet — but it's different this time

[140] The Verge: Chinese authorities admit they're able to retrieve deleted WeChat messages

[141] Time: These Are the Countries Where Twitter, Facebook and TikTok Are Banned

[142] The New York Times: China's Surveillance State Is Growing. These Documents Reveal How.

[143] The Guardian: The great firewall of China: Xi Jinping's internet shutdown

[144] The Guardian: The great firewall of China: Xi Jinping's internet shutdown

[145] The Washington Post: China harvests masses of data on Western targets, documents show

[146] Freedom House: China

[147] Human Rights Watch: China: Police 'Big Data' Systems Violate Privacy, Target Dissent

[148] The New York Times: Four Takeaways From a Times Investigation Into China's Expanding Surveillance State

[149] The New York Times: China's Surveillance State Is Growing. These Documents Reveal How.

[150] BBC: AI emotion-detection software tested on Uyghurs

[151] Sveriges Radio: Facebook collects intimate customer data from over 100 European pharmacies

[152] The Markup: The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users

[153] FTC: FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations

[154] FTC: A Look At What ISPs Know About You.

[155] BBC: Facebook's data-sharing deals exposed

[156] FTC: Big Data. A tool for inclusion or exclusion?

[157] The Washington Post: Health apps share your concerns with advertisers. HIPAA can't stop it.

[158] The Washington Post: Top U.S. Catholic Church official resigns after cellphone data used to track him on Grindr and to gay bars

[159] Vice: Internet Service Providers Collect, Sell Horrifying Amount of Sensitive Data, Government Study Concludes.

[160] World Privacy Forum: Congressional Testimony: What Information Do Data Brokers Have on Consumers?

[161] Wired: The complicated truth about China's social credit system

[162] Wired: The complicated truth about China's social credit system

[163] Newsweek: 'Black Mirror' in China? 1.4 Billion Citizens to Be Monitored Through Social Credit System

[164] Wikipedia: Nosedive (Black Mirror)

[165] The Guardian: How private is your period-tracking app? Not very, study reveals

[166] The New York Times: The Privacy Project

[167] The New York Times: How to Track President Trump

[168] Vice: Data Broker Is Selling Location Data of People Who Visit Abortion Clinics

[169] Time: Supreme Court Allows Texas Abortion Law to Stand, But Says Abortion Providers Can Challenge It.

[171] The New York Times: We Need to Take Back Our Privacy

[172] Wired: The Case of the Creepy Algorithm That 'Predicted' Teen Pregnancy

[173] The Washington Post: Okay, Google: To protect women, collect less data about everyone.

[174] The Intercept: Hacked Documents: How Iran Can Track and Control Protesters' Phones

[175] BBC: Iran installs cameras to find women not wearing hijab

[176] The New York Times: When Nokia Pulled Out of Russia, a Vast Surveillance System Remained

[177] Wired: Inside Safe City, Moscow's AI Surveillance Dystopia.

[178] CNBC: China has launched another crackdown on the internet — but it's different this time.

[179] The Guardian: The great firewall of China: Xi Jinping's internet shutdown

[180] The New York Times: How China's Police Used Phones and Faces to Track Protesters

[181] Technology Review: This huge Chinese company is selling video surveillance systems to Iran

[182] Human Rights Watch: China: Phone Search Program Tramples Uyghur Rights

[183] CNN: Watched, judged, detained.

[184] BBC: AI emotion-detection software tested on Uyghurs

[185] BBC: AI emotion-detection software tested on Uyghurs

[186] The Guardian: The Pegasus Project

[187] Wikipedia: Nineteen Eighty-Four

[188] Wikipedia: Brave New World

[189] Humanetech.com: democratic functioning

[190] Humanetech.com: democratic functioning

[191] The Intercept: Facebook Uses Artificial Intelligence to Predict Your Future Actions for Advertisers, Says Confidential Document.

[192] Humanetech.com

[193] Thesocialdilemma.com

[194] Jordanharbinger.com: 156: Why You Should Unplug from Social Media for Good

[195] Thesocialdilemma.com

[196] VPRO documentary: Shoshana Zuboff on surveillance capitalism

[197] Wired: Get Ready for the Next Big Privacy Backlash Against Facebook

[198] The Guardian: Shoshana Zuboff: 'Surveillance capitalism is an assault on human autonomy'

[199] Humanetech.com: democratic functioning

[200] Massachusetts Institute of Technology: Study: On Twitter, false news travels faster than true stories.

[201] NBC News: 'Carol's Journey': What Facebook knew about how it radicalized users

[202] Amnesty: 'The Great Hack': Cambridge Analytica is just the tip of the iceberg

[203] The Guardian: Cambridge Analytica: how did it turn clicks into votes?

[204] BBC: 'Cambridge Analytica planted fake news'

[205] The Guardian: Cambridge Analytica whistleblower: 'We spent $1m harvesting millions of Facebook profiles'

[206] Amnesty: 'The Great Hack': Cambridge Analytica is just the tip of the iceberg

[207] The New York Times: Russians Again Targeting Americans With Disinformation, Facebook and Twitter Say

[208] Wikipedia: Cambridge Analytica

[209] VPRO Documentary: Shoshana Zuboff on surveillance capitalism

[210] Ted Talks: Why privacy matters

[211] Cigionline: Shoshana Zuboff on the Undetectable, Indecipherable World of Surveillance Capitalism.

[212] Universal Pictures All-Access: Snowden - Nothing To Hide, Nothing To Fear

[213] Ted Talks: Why privacy matters

[214] Npr.org: Ben Franklin's Famous 'Liberty, Safety' Quote Lost Its Context In 21st Century

[215] Wired: The Eternal Value of Privacy

[216] Schneier.com: The Eternal Value of Privacy

[217] Amnesty: Edward Snowden: 'Privacy is for the powerless'

[218] Ted Talks: Why privacy matters

[219] The Tor Project: PrivChat #3 - Advancing Human Rights with Tor

[221] The Register: Egyptian government caught tracking opponents and activists through phone apps

[222] Amnesty: Morocco: Human Rights Defenders Targeted with NSO Group's Spyware

[223] Wired: The FBI just admitted it bought US location data

[224] Wired: How the Pentagon learned to use targeted ads to find its targets – and Vladimir Putin

[225] Wall Street Journal: U.S. Spy Agencies Know Your Secrets. They Bought Them.

[226] Senator Ron Wyden: Wyden Releases Documents Confirming the NSA Buys Americans' Internet Browsing Records

[227] Electronic Frontier Foundation: Bad Amendments to Section 702 Have Failed

[228] Zwillgen: House Intelligence Committee FISA "Reform" Bill Would Greatly Expand the Class of Businesses and Other Entities Required to Assist in FISA 702 Surveillance

[229] The New York Times: Secret Rift Over Data Center Fueled Push to Expand Reach of Surveillance Program

[230] Senator Ron Wyden: "I Will Do Everything In My Power" to Stop Bill Expanding Government Surveillance Under FISA 702

[231] Edward Snowden on X/Twitter: The NSA is just days from taking over the internet, and it's not on the front page of any newspaper--because no one has noticed.

[236] IMDB: Total Trust

[237] Wikipedia: 709 Crackdown

[238] Wikipedia: Huang Xueqin

[239] IMDB: Total Trust

[240] Reuters: Google hit with 150 mln euro French fine for cookie breaches

[241] The Verge: Google will turn off third-party tracking for some Chrome users soon

[242] The Verge: Google abandons FLoC, introduces Topics API to replace tracking cookies

[243] Techradar: Facebook's Onavo VPN used to wiretap competitor data, court filings reveal

[244] patrick-breyer.de

[245] edps.europa.eu

[246] patrick-breyer.de

[247] patrick-breyer.de

[248] edri.org: Joint statement of scientists and researchers

[249] mullvad.net: The European Commission does not understand what is written in its own chat control bill

[250] Politico: Pegasus used by at least 5 EU countries, NSO Group tells lawmakers

[251] about.fb.com: Preventing child exploitation on our apps.

[252] Fokus: Chat Control: Så ska techjättarna skanna allt du skickar

[253] Fedpol 2021: Kampf gegen pädokriminalität

[254] edri.org: Uphold privacy, security and free expression by withdrawing new law

[255] patrick-breyer.de: Manipulative EU opinion poll no justification for indiscriminate chat control

[256] Balkaninsight: 'Who Benefits?' Inside the EU's Fight over Scanning for Child Sex Content

[257] Politico: The Qatargate files

[258] blog.cryptographyengineering.com

[259] The Intercept: New Group Attacking iPhone Encryption Backed by U.S. Political Dark-Money Network

[260] Engadget: Sex, lies, and surveillance: Something's wrong with the war on sex trafficking

[261] The Intercept: How Peter Thiel's Palantir Helped the NSA Spy on the Whole World

[262] The New York Times: Spy Contractor's Idea Helped Cambridge Analytica Harvest Facebook Data

[263] Netzpolitik: How the security apparatus shapes chat control

[264] Netzpolitik: Thorn also brought chat control into play for other topics

[265] Follow the money: Ashton Kutcher's anti childabuse software below par

[266] Balkaninsight: Europol Sought Unlimited Data Access in Online Child Sexual Abuse Regulation

[267] Wired: A Controversial Plan to Scan Private Messages for Child Abuse Meets Fresh Scandal

[268] europarl.europa.eu

[269] Fortune: Privacy-busting 'chat control' plans rejected by European Parliament as CSAM law heads into final stretch

[270] European court of human rights: case of podchasov v. Russia

[271] Reclaim the net: EU Officials Dodge Their Own Surveillance Law

[272] Netzpolitik: Behind closed doors

[273] data.consilium.europa.eu

[274] riksdagen.se

[275] patrick-breyer.de

[276] Netzpolitik: Why chat control is so dangerous

[277] Svenska Dagbladet: Expertkritik mot omstritt nätförslag i EU

[278] euractiv.com

[279] Aftonbladet: Mörkade allt för riksdagen

[280] europol.europa.eu: European Police Chiefs call for industry and governments to take action against end-to-end encryption roll-out

[281] polisen.se: Europas polischefer går samman mot grov brottslighet i en digital värld

[282] europol.europa.eu

[283] Svenska Dagbladet: Granskning: Poliser läcker till gängen

[284] Signal.org: AI, Encryption, and the Sins of the 90s

[285] The New York Times: Secret Documents Reveal N.S.A. Campaign Against Encryption

[286] CNN: U.S. enables Chinese hacking of Google

[287] IEEE: The Athens Affair

[288] blog.cryptographyengineering.com: remarks on “chat control”

[289] fbi.gov: Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?

[290] EU Commission: Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement

[291] Wired: Microsoft’s Recall Feature Is Even More Hackable Than You Thought

[292] Netzpolitik: Going Dark – EU states want access to encrypted data and more surveillance

Vi lever i en värld där allt vi gör på internet spåras och sparas. Stora techbolag säger det själva rakt ut: deras målsättning är inte bara att övervaka allt du gör, utan även att kunna förutse ditt beteende men också styra det. Statliga myndigheter är inte bättre. Istället för att rikta sina insatser massövervakar de hela befolkningar. Utan konsekvenser bryter de mot grundläggande lagar, gång på gång ertappas de med att övervaka journalister, aktivister och meningsmotståndare.

Redan idag ser vi hur auktoritära länder använder massövervakningen för att kontrollera sina invånare. I demokratier har insamlingen av högst personlig data använts i påverkanskampanjer för att vinna val. Vi kan känna av konsekvenserna här och nu. Men den stora frågan är var vi hamnar om vi inte får stopp på utvecklingen.

Till dig som säger att du inte har något att dölja: det handlar inte om dig. Det handlar om allas vår framtid, om de utsatta och om våra samhällen. Det handlar om kommande generationer, och om de ska växa upp i ett fritt eller kontrollerande samhälle.

MULLVAD VPN