

De panopticar

Een trade-off tussen privacy en surveillance door Tesla?

Marc Schuilenburg, Yarin Eski, Quinty van Anen & Jolijn de Waard

1. Inleiding

Na de Hitlergroet van Tesla-CEO Elon Musk tijdens de inauguratie van de Amerikaanse president Donald Trump in 2025 zijn Tesla-auto's en fabrieken doelwit geworden van maatschappelijk protest en vernieling in met name de Verenigde Staten, maar ook in Nederland (Funnekotter, 2025; RTL Nieuws, 2025). De Amerikaanse FBI omschrijft de Teslavernieling als 'gewelddadige criminaliteit' en roept Tesla-eigenaren op waakzaam te zijn (FBI, 2025). Ook op Nederlandse online Tesla-fora wordt opgeroepen alert te zijn. Tips worden gegeven voor wat je kunt doen 'om te voorkomen dat jouw geliefde auto het doelwit wordt van vandalisme' (Kraaijvanger, 2025). Daarbij wordt gewezen op het voordeel van de ingebouwde Sentry Mode-functie, die 'de camera's van je auto gebruikt om de omgeving in de gaten te houden en opnames te maken zodra er iets verdachts gebeurt. Vandalen die aan je auto komen, worden gefilmd, wat hen hopelijk afschrikt' (ibid.).

De Sentry Mode-functie is een geavanceerd veiligheidssysteem ('smart control') dat – met camera's van Tesla – alles wat er buiten de auto gebeurt, monitort om inbraak en vandalisme te voorkomen. Wanneer de camera's een verdachte situatie detecteren, gaan de koplampen knipperen en ontvangt de eigenaar van de auto een waarschuwing op zijn Tesla-app. Daarbij wordt het incident opgenomen en vastgelegd via de camera's van de auto. Gebruikers hebben op afstand toegang tot de live-feeds van de ingebouwde camera's, zodat ze hun auto in real-time kunnen volgen. Maar de Sentry Mode is meer dan een slim autoalarm om alleen criminaliteit tegen te gaan. De camera's registreren ook het gedrag van de bestuurder, waaronder hoe hard wordt gereden, hoe bochten worden genomen, het remgedrag en de geschiedenis van het opladen van de elektrische auto ('superchargen') (Harris, 2022; Tesla, 2025). Een belangrijke rol is hierbij weggelegd voor de cabinecamera – de camera in de achteruitkijkspiegel die tijdens de rit het gedrag van de bestuurder monitort én handelt wanneer de bestuurder niet oplet. Deze camera staat standaard uit, behalve als de bestuurder gebruik maakt van veiligheids- of comfortfuncties, zoals de Autopilot. De cabinecamera kan dan bepalen of de bestuurder niet goed oplet en deze via een geluidssignaal waarschuwen om zijn ogen op de weg te houden. In de literatuur wordt gesproken van een 'panopticar', waarbij de 'slimme controle' door Tesla en de 'zelfdisciplinerende' van de bestuurder naadloos in elkaar overlopen (Eski & Schuilenburg, 2022; Schuilenburg, 2024).

De belangstelling in de culturele en kritische criminologie voor het fenomeen 'auto' richt zich vooral op aspecten als jeugdcultuur, snelheid en transgressie ('joyriding') (o.a. Muzzatti, 2010; Lumsden, 2013; Menoret, 2014; Thalia & Tranter, 2018). Nauwelijks tot geen empirisch onderzoek vindt plaats naar de digitale surveillance

in en rond de auto. Dat is opmerkelijk, omdat in het geval van de elektrische auto's van Tesla er sprake is van een opvallende paradox. Enerzijds is de Tesla voor veel personen een object van betekenisgeving en staat de auto symbool voor 'personal freedom, efficacy, pleasure, and social status' (Loader, 2025: 217). Anderzijds is de Tesla onderworpen aan publieke regelgeving en steeds geavanceerdere vormen van digitale surveillance door het Amerikaanse techbedrijf (Eski & Schuilenburg, 2022; Headworth, 2023; Schuilenburg, 2024). Daarbij scoort Tesla het slechtst van alle automerken als het gaat om de bescherming van publieke waarden als respect voor het privéleven van de bestuurders.¹ Rondom de Tesla vinden met andere woorden tal van spanningen plaats, wat de vraag relevant maakt: hoe navigeren Tesla-gebruikers tussen autonomie en surveillance in hun dagelijkse rijervaringen?

Het antwoord hierop wordt gezocht in een casestudy waarin de ervaringen van eigenaren van auto's van Tesla centraal staan. Daarmee bouwen wij voort op eerder werk naar hoe Tesla persoonlijke gegevens binnen en buiten het voertuig verzamelt en vastlegt in een uniek eigenarenprofiel om zo de veiligheid in en rondom de auto te verbeteren (Eski & Schuilenburg, 2022; Schuilenburg, 2024). Hiervoor gebruiken wij het concept 'luxe surveillance'. Na de bespreking van de methodologie van het onderzoek worden op basis van de interviews en observaties twee soorten van ervaringen van Tesla-eigenaren onderscheiden. In de conclusie en discussie wordt stilgestaan bij de implicaties van de uitkomsten van het onderzoek en worden suggesties gedaan voor verder onderzoek naar de auto als cultureel criminologisch fenomeen.

2. Luxe surveillance

Tesla's Sentry Mode-functie is een voorbeeld van 'luxe surveillance' – consumentengoederen waarvoor personen veel geld willen betalen omdat de vermeende voordelen die deze producten bieden, van het voorkomen van criminaliteit tot de monitoring van jezelf, worden gezien als positieve eigenschappen ervan (Gilliard & Golombia, 2021; Schuilenburg, 2023; 2024; Benjamin, 2024). Met de vrijwillige aankoop van deze producten zijn grote bedragen gemoeid, waardoor ze niet voor iedereen zijn weggelegd. Ze zijn sterk verbonden met een exclusieve levensstijl en de doelgroep van deze luxeproducten bestaat vaak uit 'jonge mensen' met een 'hoge opleiding' die het bezit ervan, van een Tesla-auto bijvoorbeeld, zien als een 'statussymbool' (Li et al., 2021; Eski & Schuilenburg, 2022). Luxe surveillance verschilt daarmee van extern opgelegde surveillance, waar personen niet vrijwillig aan deelnemen, denk aan publieke bewakingscamera's (CCTV) (Minnaar, 2007; Hempel & Töpfer, 2009; Lippert & Wilkinson, 2010; Goold, Loader & Thumula, 2013), bodycams voor politiewerk (White, Gaub & Todak, 2018; St. Louis, Saulnier & Walby, 2019; McKay & Lee, 2020), bodyscanners op luchthavens (Andreas, 2003; Leese, 2015) en elektronisch toezicht (Daems, 2020; Gacek, 2022).

1 Onderzoek van de Mozilla-organisatie spreekt van een 'privacy-nachtmerrie'. Zie: <https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/> (bezoekdatum: 30 maart 2025).

De opkomst van luxe surveillance past binnen bredere socio-technische ontwikkelingen, waaronder (1) de versplintering van de politiefunctie en (2) de platformisering van de samenleving. Het 'veilig maken' van de samenleving door digitale manieren van surveillance gebeurt tegenwoordig door veel meer partijen dan alleen de politie, in dit geval: door burgers ('onder' de politie) en techbedrijven ('naast' de politie) (Schuilenburg, 2023; 2024; Schuilenburg & Soudijn, 2023; Khalfa et al., 2024). Brayne (2017) spreekt van 'non-police databases' en deze data komen onder meer van apps (Waze navigatie), slimme apparaten (intelligente lantaarnpalen), sensoren die op het lichaam worden gedragen (Apple Watch, Fitbit, Ray-Ban Stories bril) of die zijn bevestigd op objecten als toegangspoortjes, woningen (Amazon Ring deurbel) en auto's (Tesla). Je kunt ook zeggen dat digitale surveillance een alledaags en 'banaal product' (Goold, Loader & Thumala, 2013) is en nauw hiermee verbonden zijn maatschappelijke veranderingen rondom surveillance als 'softening' (Marx, 2006; 2016), 'commodificering' (Gandy, 1993; Kienscherf, 2022) en 'normalisering' (Lyon, 2001; 2007; Eley & Rampton, 2020).

'Surveillance-kapitalisten' zoals Facebook, Amazon en Google spelen een belangrijke rol in de 'platformisering' van de samenleving (Bratton, 2015; Srnicek, 2017; Zuboff, 2019). Kenmerkend voor deze nieuwe vorm van kapitalisme is dat bedrijven hun verdienmodel hebben gemaakt van het zo veel mogelijk verzamelen van data, om deze data vervolgens te vermarkten in verhandelbare producten en diensten waarop eigendomsrechten drukken. Srnicek stelt dat digitale platforms de technologische, economische en sociaal-culturele infrastructuur zijn 'to monopolise, extract, analyse, and use the increasingly large amounts of data that were recorded' (2017: 43). De notie 'platform' omvat samenwerking tussen bedrijven over product- en industriegrenzen heen. Dit betekent dat een product als een Tesla-auto 'can be itself a platform and a component of other platforms at the same time' (Alaimo & Kallinikos, 2024: 134-136). Zo kunnen de opgenomen beelden van de Sentry Mode worden gedeeld met andere personen op de online-platforms van Tesla en worden persoonlijke data door Tesla verkocht aan externe partijen, waaronder verzekeringsbedrijven waarbij Tesla-eigenaren een autoverzekering kunnen afsluiten die is gebaseerd op hun rijgedrag.²

Kortom, met luxe surveillance komt een andere verhouding tot stand tussen degenen die kijkt en de persoon die wordt bekeken dan bij 'klassieke surveillance' (Marx, 2016). Niet alleen graaft deze digitale manier van surveillance dieper in het privéleven van burgers, ook is er sprake van een bevoorrechte klasse die zich juist wil laten surveilleren en bereid is daarvoor te betalen en hun privacy in te leveren. West (2019) spreekt in dit verband van 'surveillance as a service'. Meer kennis over de manier waarop dit gebeurt en de onderliggende motieven van Tesla-gebruikers die hierbij een rol spelen, is nodig omdat het onder meer kan gaan om gegevens die personen juist liever niet willen delen of waarvan personen niet weten wat ermee

2 Zie: www.tesla.com/support/insurance/tesla-real-time-insurance (bezoekdatum: 30 maart 2025). Bij deze 'real time driving' verzekering wordt een 'safety score' gevormd door de sensoren in de auto. De 'safety score' gaat omlaag (en daarmee de premie omhoog) als de bestuurder hard remt, agressief een bocht neemt, te dicht op de voorligger rijdt, te lang geen handen op het stuur heeft of als de bestuurder waarschuwingen krijgt voor een botsing.

gebeurt en wat de consequenties hiervan zijn voor de veiligheid in en rondom hun Tesla. In dat opzicht volgen wij de oproep van surveillance-auteurs (Marx, 2006; Monahan, 2010; Lutz, Hoffmann & Ranzini, 2020) om het begrip 'trade-off' nader te onderzoeken.

In de volgende paragraaf bespreken wij de methodologische verantwoording van het empirische onderzoek, waarna we dieper ingaan op de resultaten hiervan.

3. Methodologie

In antwoord op de vraag hoe Tesla-gebruikers navigeren tussen autonomie en digitale surveillance in hun dagelijkse rijervaringen, is kwalitatief onderzoek verricht door (a) online deelname in Facebookgroepen van Tesla-eigenaren en (b) semi-structureerde interviews met Tesla-eigenaren.³ Met deze methoden hebben wij onszelf kunnen verdiepen in de perspectieven, overtuigingen en ervaringen van deze personen met betrekking tot de spanning tussen autonome autonomie en digitale surveillance door Tesla (zie ook: Tracy, 2019; Diphooorn, 2021).

Er zijn tussen februari en augustus 2022 wekelijks online-observaties gedaan in 14 verschillende Facebookgroepen van Tesla-eigenaren om zo inzicht te krijgen in de onderwerpen die zij belangrijk vinden wat betreft hun voertuigen en over welke zaken zij persoonlijke gegevens willen delen met Tesla. Dergelijke observaties zijn een vorm van virtuele etnografie, waarbij etnografische onderzoeksprincipes worden toegepast om publiekelijk gedeelde gegevens op het internet te observeren (Kozinets, 2002; Trottier, 2012; Costello et al., 2017). Op deze manier konden wij de gesprekken in de groepen volgen en zo de Tesla-eigenaren in hun 'eigen' online omgeving bestuderen, waardoor het Hawthorne-effect (waarbij individuen hun gedrag veranderen als ze weten dat ze geobserveerd worden) minimaal effect heeft (Levitt & List, 2011). Aan de hand van 'purposive sampling' zijn relevante groepen geselecteerd en werd toegang mogelijk gemaakt door zelf lidmaatschap aan te vragen, waarbij uitleg is gegeven over het onderzoeksdoel. In besloten groepen is om toestemming gevraagd aan de beheerders van de betreffende Facebookgroep.

Naarmate het onderzoek vorderde, werden de onderwerpen die de eigenaren belangrijk vonden geïdentificeerd en gecategoriseerd in de volgende zes thema's: 1) Auto-onderdelen, 2) Opladen, 3) Kopen, 4) Service, 5) Bewaking en 6) Overig. Het aantal berichten (N = 8.449) zorgde voor een kwantitatief inzicht in de belangrijkste onderwerpen.

Vervolgens zijn semistruktuurde (online) interviews afgenomen voor het kwalitatief inzicht in de ervaringen van Nederlandse Tesla-eigenaren (N = 43) met de digitale surveillance en welke betekenis zij geven aan hun autonomie en het delen van persoonlijke gegevens met Tesla. Alleen interviewdata van personen die een Tesla-auto zakelijk of privé hebben aangeschaft, zijn meegenomen in de analyse (leaserijders zijn dus buiten dit onderzoek gehouden). De geïnterviewde respondenten zijn op twee manieren benaderd, via een oproep in de Facebookgroepen en fysiek op de Tesla's supercharger-locaties Hotel Van der Valk in Akersloot en Hotel

3 Voor een uitgebreidere bespreking van de methodologie, zie: Schuilenburg & Eski, 2025.

Van der Valk in Hoorn. De interviewdata en Facebook-observaties werden geanalyseerd in ATLAS.ti met een deductief-inductieve aanpak, waarbij een coderings-schema werd opgesteld.

Te allen tijde hebben de onderzoekers zich gehouden aan ethische en privacyrichtlijnen (o.a. geïnformeerde consent, data-beveiliging en anonimisering). Ondanks onze pogingen een zo divers mogelijke groep respondenten te bereiken, waren slechts vier van de 43 respondenten vrouw. Dit komt wel overeen met de algemene kenmerken van een Tesla-eigenaar, gelet op het feit dat Tesla-eigenaren overwegend mannelijk en gemiddeld 48 jaar oud zijn (Hedges & Company, 2024).

4. Resultaten

Uit het empirische onderzoek komen twee op elkaar inwerkende ervaringen naar voren met betrekking tot de spanning tussen de digitale surveillance en de gevoelens van autonomie van Tesla-eigenaren, namelijk: 1) branding en vrijwillige datadeling, en 2) onvoorspelbaarheid en privacy-zorgen.⁴

De panopticar: branding en vrijwillige datadeling

Hoewel rond digitale surveillance het beeld hangt dat steeds meer data anoniem worden vastgelegd ('waar we zijn, met wie we zijn, en wat we doen') zonder dat personen het weten of hiervoor toestemming hebben gegeven, blijkt dat de respondenten ook actief participeren en meedoen rondom alle ins en outs van Tesla-auto's en de surveillance door het bedrijf. Opvallend is dat zij hierbij zowel zichzelf als het bedrijf verheerlijken, wat duidelijk wordt aan de hand van het fenomeen van branding, oftewel het aanprijzen van het merk 'Tesla'. Dit gebeurt allereerst door de Tesla te vergelijken met andere automerken, in het bijzonder modellen als de Polestar 2, Porsche Taycan, XPeng P7 en Mercedes-Benz EQS:

'Vandaag een proefrit gemaakt met de XPeng P7! Erg gave auto met de nodige technische snufjes aan boord. Naar mijn mening rijdt mijn Model 3 Performance vele malen sportiever en is hij sneller, dus ik laat het lekker bij deze rit.' (FR18)

Een aspect van branding is dat eigenaren advies bij elkaar inwinnen over waar zij auto-onderdelen kunnen kopen, over het uiterlijk van de auto (bijvoorbeeld tips voor reinigingsproducten voor het interieur, stoelen, deuren en dashboards) en of andere eigenaren soortgelijke problemen hebben ondervonden. Ook bespreken eigenaren met elkaar welke autoverzekering het beste en goedkoopste is, evenals informatie over hoe beginnersfouten te vermijden wanneer ze hun Tesla hebben gekocht. Bovendien willen zij weten of er ook een specifieke Tesla-etiquette is. Zo schrijft FR31: 'Gisteren onze eerste Tesla gekocht! Hebben Tesla-eigenaren een bepaalde groet als we elkaars Tesla's op de weg zien?'

4 Een deelnemer van Facebook wordt aangegeven met F(acebook)R(espondent)# en een deelnemer aan een interview wordt aangegeven met I(nterview)R(espondent)#.

Ook het onderwerp ‘opladen’ is belangrijk voor Tesla-eigenaren, door elkaar op de hoogte te houden over, bijvoorbeeld, de oplaadcapaciteit van oplaadstations en Tesla-superchargers, problemen met opladen, kindvriendelijke oplaadplekken of plekken met unieke diensten, zoals de aanwezigheid van een pizza-automaat, de beschikbaarheid van oplaadpunten, speciale vereisten als zij naar het buitenland reizen, en de kosten die gepaard gaan met thuis- en openbare oplaadstations. Daarbij worden ook frustraties onderling gedeeld, vooral over andere (merken) auto’s die de supercharger-plaatsen bezetten of deze stations ontoegankelijk maken. In dit verband wordt onder meer gepleit voor voorrang voor Tesla’s bij oplaadpunten. Een argument voor een voorkeursbehandeling bij de supercharger-plaatsen is dat de respondenten stellen dat zij deel uitmaken van het merk ‘Tesla’ en rijden in een ‘duurzame auto’. Uit het empirische onderzoek blijkt dat hierbij een gemeenschapsgevoel wordt gecreëerd rondom ‘groen-leven’, iets wat kenmerkend is voor de ‘aspirationele klasse’ (Currid-Halkett, 2017). Zo slaan eigenaren zichzelf op de ‘groene’ borst, omdat de elektrische auto’s geen CO₂ uitstoten en daarmee de overgang naar een duurzame samenleving versnellen. Als het ware internaliseren zij daarmee Tesla’s narratief van ‘lean & green’:

‘Zakelijk gezien is elektrisch rijden [goedkoper] en uiteindelijk ook, ja, het milieu ook. De vorige auto was afgeschreven, dus de volgende stap naar een beter milieu is elektrisch rijden.’ (IR16)

Of:

‘Daarnaast ben ik bezorgd over het milieu, in de zin dat ik het belangrijk vind dat iedereen er alles aan doet om het milieu te sparen.’ (IR19)

In hun branding verheerlijken de respondenten ook Elon Musk, eigenaar van de bedrijven Tesla, SpaceX en X, en zijn ambities om van de mens een interplanetaire soort te maken die ook buiten de planeet Aarde kan voortleven.⁵

‘Dankbaar om hier te zijn [in de Tesla Facebookgroep]. Ik vind het geweldig om alles over Elon te volgen. Van SpaceX tot Tesla, tot zijn familie. Hij verandert de wereld en ik zie hem als mijn mentor.’ (FR45)

De branding van het merk ‘Tesla’ loopt naadloos over in het vrijwillig delen van persoonlijke data met het Amerikaanse techbedrijf. Wood en Ball (2013) spreken in dit verband van ‘brandscapes of control’ – een landschap waar eigenaren voor Tesla aan een vorm van marketing doen (aan elkaar) en waarin surveillance vertroebelt met een positieve ervaring rondom het merk, i.c. privileges eraan ontnemen. Zo wordt de Sentry Mode door de respondenten gezien als een prettige en plezierige vorm van controle in hun dagelijks leven:

5 Inmiddels wordt duidelijk dat Tesla-eigenaren anders beginnen te denken over Elon Musk naar aanleiding van zijn Hitlergroet en zijn rol in de regering van Trump.

‘Ik kan mij voorstellen dat zij [het bedrijf Tesla] wat verzamelen, ja. Dat zie je ook op de display. Wij gingen laatst naar een onderhoudsbeurt en omdat je dat via een app moet inplannen, zagen zij hoeveel kilometer wij hadden gereden. Ik vind dit soort dingen fijn [...] het maakt je leven wat makkelijker en alles heel soepeltjes.’ (IR22)

‘Het [Sentry Mode] houdt continu de omgeving in de gaten terwijl je rijdt, en als je geparkeerd staat, hangt het ervan af of je de beveiligingsmodus hebt ingeschakeld. Maar in dat geval staan de camera’s eigenlijk altijd aan. [...] Ik vind het heel geruststellend. [...] Het is gewoon omdat, als er ooit een kras op je auto komt of als er iets gebeurt, je er visueel bewijs van hebt, zelfs als je er niet bij was.’ (IR4)

Het verkrijgen van bewijs van inbraak of vandalisme door de digitale Tesla-surveillance, zoals duidelijk wordt uit het laatste citaat, zorgt in de Facebookgroepen voor veel interactie via posts en commentaren. Regelmatig worden video’s gedeeld die zijn opgenomen met de Sentry Mode van gevaarlijke situaties op de weg of van incidenten rond geparkeerde auto’s. Ook wordt onderling besproken hoe de camerabeelden van Tesla kunnen worden gebruikt als bewijs om gestolen Tesla’s terug te vinden, boetes aan te vechten, of om verzekeringstechnische redenen.

Respondenten waarderen niet alleen hoe de beelden als bewijs kunnen worden gebruikt door de eigenaren zelf, maar ook als bewijs kunnen dienen voor de politie. Zo wordt gesproken over een dodelijk tramongeluk in oktober 2021, waarbij een geparkeerde Tesla het incident vastlegde en de beschuldigde tieners door de beelden van de Tesla werden vrijgesproken:

‘Ik geloof dat in Rotterdam dat voorvalletje was met de tram, er was iemand voor de tram geduwd. Het bleek dat een opname van de dashcam van een Tesla het beeld kon schetsen van wat er echt gebeurd was. [...] Daarom denk ik dat ik dat [Sentry Mode] heb ingeschakeld omdat ik me persoonlijk niet veel zorgen maak over mijn privacy, omdat ik niets te verbergen heb. [...] Wat ik belangrijk vind is dat ik gegevens deel om het zo veilig te maken dat andere leveranciers en mensen, gebruikers, eigenaren, gaan vertrouwen op de techniek.’ (IR33)

De beelden van de Sentry Mode dienen ook andere doelen, zo blijkt uit gesprekken op Facebook. Zo worden de ingebouwde camera’s door de eigenaren onder meer gebruikt om te kijken of er een laadstation of parkeerplaats vrijkomt.

‘Ik heb iets wilds en geks gedaan. [Ik] was deze week in een hotel voor een conferentie en hun garage heeft twee Tesla-laders, maar ze waren allebei in gebruik toen ik daar aankwam. Ik parkeerde waar Sentry Mode ze kon zien. Ik controleerde de volgende paar dagen een paar keer de Sentry cams op de telefoon, dezelfde twee auto’s stonden er nog, maar één keer was er een slot leeg. Ik rende erheen en pakte hem!’ (FR7)

De software-updates door Tesla worden door de respondenten gezien als 'kleine cadeautjes' waarmee Tesla zich zou onderscheiden van andere autofabrikanten. Dit wederkerige proces van 'het geven', om de klassieke term van de Franse antropoloog Mauss (2002 [1923-1924]; zie ook: Schuilenburg & Peeters, 2017; Schuilenburg, 2024) te gebruiken, zorgt ervoor dat eigenaren reikhalzend uitkijken naar nieuwe updates, wat voor hen een belangrijke reden is om vrijwillig hun persoonlijke data af te staan aan het Amerikaanse techbedrijf:

'Ik zie het echt als big data, en volgens mij is het belangrijk voor Tesla en voor die Autopilot, voor de navigatie, om uiteindelijk helemaal zelfstandig te kunnen rijden. Dat is het doel van Tesla. [...] Hoe meer data, hoe beter die navigatie elke keer wordt. En dat vind ik wel leuk. Je krijgt om de zoveel tijd een update, net zoals je iPad, en dan zitten er ook nieuwe functies in. Dan wordt dit even verbeterd, weet je? Het is dus net alsof je in de nieuwste auto rondrijdt.' (IR14)

De branding en het (willen) bestendigen van de slimme controle via vrijwillige datadeling staat in schril contrast met de andere kant van luxe surveillance, namelijk dat de gedeelde data ook tegen de respondenten kunnen worden gebruikt, een aspect waar wij in de volgende subparagraaf op ingaan.

De panopticar: onvoorspelbaarheid en privacy-zorgen

De ervaring van de gift – gedragsdata en software-updates als kleine geschenken in retour – heeft als keerzijde dat dit proces ook leidt tot verwarring, irritatie en zelfs angst bij verschillende eigenaren. Als er nieuwe software-updates beschikbaar komen, moeten eigenaren vaak hun verwachtingen bijstellen:

'Deze nieuwe update voor zelf rijden is verschrikkelijk. Ik moet elke tien seconden het stuur aanraken. Het is vervelender om het nu aan te hebben staan.' (FR3)

Ook stellen eigenaren soms een update uit als zij daardoor een favoriete functie kunnen kwijtraken, zoals de optie om scheetgeluiden binnen en buiten de auto af te spelen via de Boombox-functie van de Tesla.

Naast kleine irritaties rondom triviale zaken maken eigenaren zich zorgen over de veiligheidstools die niet (goed) werken. Zo wordt gesproken over de (over)gevoeligheid van de Sentry Mode – zodra de auto een beweging detecteert, gaan de koplampen aan. Dit gebeurt namelijk ook bij niet-bedreigende bewegingen, zoals bewegende bomen. Daarnaast kan de Tesla de hele nacht met zijn lichten knipperen, wat leidt tot klachten van burens, aldus de respondenten.

Kortom, terwijl de updates een gevoel van comfort kunnen geven, treedt er ook onvoorspelbaarheid op, iets waar de eigenaren juist niet op zitten te wachten en wat het tegenovergestelde is van surveillancegenot. Sterker nog, in plaats van het gevoel van controle te hebben, leidt de Autopilot – het systeem waarmee de auto's deels zelfstandig kunnen rijden – tot meer (en te veel) alertheid bij respondenten, waardoor zij juist het gevoel hebben de controle te verliezen:

‘Net terug van wintersport. Lekker rustig aangedaan, maar ik werd helemaal gek van het gezwalk van de Autopilot!!! Het lijkt wel of hij van de Schnaps heeft gesnoept. Hij slingert van links naar rechts op de baan, maar wel binnen de lijntjes. Zijn er nog meer mensen die hier last van hebben?’ (FR26)

‘Je hebt wel van dat *ghost breaking* gehoord? [...] Dat zijn van die dingen die hij zomaar kan doen en waarvan je denkt: Waarom doe je dat? Je moet dus alert blijven, anders ga je rare dingen krijgen.’ [IR37]

Uit het feit dat sommige Tesla-eigenaren aangeven dat zij door de surveillance van het techbedrijf voorzichtiger zijn gaan rijden, blijkt dat de vrijwillige datadeling met Tesla een performatieve kracht heeft. Het gaat in dit geval onder meer om respondenten die een verzekering bij Tesla hebben afgesloten. De verzekering van Tesla werkt met een ‘veiligheidsscore’. Om een hoge score te bereiken, moeten eigenaren onberispelijk rijgedrag vertonen, wat als negatief wordt ervaren omdat het rijden met de auto daardoor minder plezierig wordt. In plaats van een voorkeursbehandeling te krijgen, voelen zij zich daardoor geperst in een keurslijf:

‘Vindt iemand dat de veiligheidsscore een beetje gevoelig is? Ik ben overgestapt op een Tesla-verzekering en ik begin het gevoel te krijgen dat je als een oma moet rijden om de scores boven de 95 te houden. Het is niet leuk om een snelle, sportieve auto te hebben.’ (FR28)

Tot slot zijn sommige eigenaren kritisch over privacy-gerelateerde onderwerpen rondom datadeling en de ontvangen updates. Eigenaren maken zich onder meer zorgen over hoe hun gegevens worden gebruikt of zelfs misbruikt, bijvoorbeeld in de rechtbank tegen henzelf of wanneer bedrijfsinformatie door Tesla wordt verkocht aan externe partijen, zoals verzekeringsmaatschappijen en adverteerders:

‘Ik zou Tesla niet zo snel aansprakelijk stellen. Ik heb een keer een heel klein aanrijdinkje gehad in de file. Ik dacht dat ik hem op automatisch rijden had gezet, want dat is altijd wel lekker. Ik zat een kieswijzer of zo in te vullen achter het stuur en hij reed toen tegen de auto voor me aan. Heel langzaam, dus ik had maar een klein beetje schade en de auto voor me had ook een beetje schade, maar bij elkaar wel 1.000 euro of zo. En toen dacht ik: Hoe kan dat nou? Want Tesla moet voor mij zorgen. Tesla moet zorgen dat ik niet tegen die auto rij, want ik had hem op Autopilot staan. Maar ik twijfelde wel of ik toch niet met mijn voet op het gaspedaal had gezeten, heel licht. Dan remt hij niet meer automatisch. Ik geloof nooit dat ik slimmer ben dan Tesla. Dus ik heb daar toen niks mee gedaan, anderen misschien wel. In dat geval had Tesla die data tegen mij kunnen gebruiken. Dat is hun recht ook.’ (IR39)

Privacy-zorgen worden ook gedeeld op de Facebookgroepen, met name over hoeveel gedragsdata de Sentry Mode verzamelt en de deling daarvan door Tesla met andere partijen. Een respondent omschrijft dit gevoel als volgt:

‘We zijn inmiddels al gewend aan gepersonaliseerde berichten op bijvoorbeeld X of Facebook [...] Het is elke keer een klein stapje. Het is elke keer een klein beetje meer informatie die in je profiel komt. Als het wordt toegevoegd aan een compleet profiel om je helemaal te profileren, dan vind ik dat eng. Als het los van de positiegegevens wordt gebruikt, dan is het op zich niet zo ernstig, maar je kunt al die data combineren natuurlijk en iemand helemaal gaan profileren. Ook als onderdeel van een bepaald reclametraject, waar je niet bewust om hebt gevraagd.’ (IR41)

Maar ondanks dat tal van eigenaren zich zorgen maken over de digitale surveillance en gevaren voor hun privacy, accepteren zij op een vrij laconieke, zelfs lollige wijze hun lot als Tesla-eigenaar, zoals deze respondent grapte op Facebook: ‘Je elektrische auto start 48 uur lang niet, omdat je status op sociale media te aanstootgevend wordt gevonden.’ (FR24)

5. Conclusie en discussie

Dit onderzoek heeft zich gericht op de vraag hoe Nederlandse Tesla-gebruikers navigeren tussen autonomie en digitale surveillance in hun dagelijkse rijervaringen. In antwoord hierop is beschreven hoe Tesla binnen en buiten het voertuig data verzamelt en vastlegt in een uniek bestuurdersprofiel om zo de veiligheid in de auto te verbeteren en criminaliteit als inbraak en vandalisme te voorkomen. Dergelijke gedragsdata worden door Tesla als immateriële grondstoffen gebruikt om de prestaties te verbeteren, problemen op te lossen, maar ook om nieuwe functies toe te voegen aan de abonnementen met hun klanten. Eigenaren van Tesla-auto's geven actief toestemming voor deze dataverzameling door de Sentry Mode in te schakelen op het touchscreen van hun Tesla.

Wij hebben de Tesla benaderd als een luxe surveillance-product waarvoor personen veel geld willen betalen en waar zij hun identiteit en ‘groene status’ mee uitdrukken. Een aspect van luxe surveillance is de indringende manier van ‘smart control’ door het techbedrijf van het handelen van de bestuurders. Bij het actief delen van persoonlijke gegevens met Tesla is er ogenschijnlijk sprake van een bewuste trade-off tussen privacy enerzijds en de voordelen van de digitale surveillance anderzijds, in de zin van meer veiligheid en comfort. Maar in tegenstelling tot onderzoek naar vrijwillige datadeling in andere gebieden, denk bijvoorbeeld aan de medische wereld, is er weinig bekend wat auto-eigenaren motiveert om hun gegevens te delen met commerciële partijen, een ontwikkeling die in een breder verband ‘platform-kapitalisme’ (Srnicsek, 2017) en ‘surveillance-kapitalisme’ (Zuboff, 2019) wordt genoemd.

Uit het empirische onderzoek komen twee sets van ervaringen naar voren als het gaat om de spanning tussen autonomie en de surveillance door het Amerikaanse techbedrijf, namelijk: (1) branding en vrijwillige datadeling en (2) onvoorspelbaarheid en privacy-zorgen. Wat betreft de motieven voor datadeling met Tesla blijkt er een verschil te bestaan met donatie en datadeling in de medische wereld (o.a. Verheggen, Nieman & Jonkers, 1998; Kurt et al., 2017; Kostkova, 2018; Skatova &

Goulding, 2019) en het openbaar bestuur (o.a. Hotz et al., 1998; Duran, Wilson & Carroll, 2005; Trein & Varone, 2023). Het sterkste motief om persoonlijke gegevens met Tesla te delen is de behoefte van direct voordeel, terwijl dat bij datadeling (maar ook bij orgaandonatie) met de overheid minder centraal staat en – naast een eigenbelang – vooral een algemeen belang dient.

Naast individuele belangen als betere dienstverlening en extra functies in de elektrische auto, hebben wij laten zien dat een gemeenschapsleven zich vormt rondom het automerk – mede door het online delen van persoonlijke ervaringen in Facebookgroepen. Daarbij ontstaat een gevoel van verbondenheid tussen de eigenaren, wat onder meer leidt tot branding van het merk ‘Tesla’ en eigenaar Musk. Dit alles werpt een bijzonder licht op de trade-off tussen de auto-eigenaren en het bedrijf – tussen privacy enerzijds en surveillance anderzijds. Zo blijkt in dit onderzoek dat het thema ‘surveillance’ meer behelst dan louter negatieve noties als controle of dwang. Dat zullen vaak kenmerken zijn van surveillance, maar surveillance hiertoe reduceren, schiet in deze casestudy tekort. Uit het empirische onderzoek komt ook een andere kant van surveillance naar voren, namelijk die van plezier, spel en ontspanning (zie ook: Albrechtslund, 2008; Ball, 2009). Privacy, hier in de betekenis van controle over je gegevens en databescherming tegen misbruik door derden, wordt – ondanks zorgen hierover – door deze groep personen bewust losgelaten in ruil voor zelfverheerlijking en gevoelens van gemak en genot.

Bij dit alles moet worden gerealiseerd dat in het geval van de datadeling er geen sprake is van een gelijkwaardige relatie tussen Tesla en de eigenaren van de auto's. Antropologische en surveillanceliteratuur wijst erop dat in het geval van de ‘gift’ altijd asymmetrische machtsverhoudingen een rol spelen (Gouldner, 1960; Zuboff, 2019). Deze asymmetrische machtsverhoudingen komen vooral naar voren in de tweede set van ervaringen. Hoewel Tesla beweert persoonlijke gegevens – in principe – anoniem te houden, kunnen ze alsnog worden gedeeld voor ‘fleet learning’ en andere verbeteringen van de elektrische auto's. De software van de auto maakt immers deel uit van een netwerk van software in andere Tesla-auto's. De gepresenteerde balans tussen genot en privacy lijkt dus niet daadwerkelijk gebalanceerd, gelet op hoe de enorme hoeveelheid verzamelde informatie persoonlijke patronen kan onthullen, wat juist de privacy van de eigenaren in gevaar kan brengen, ondanks de beloofde anonimiteit door Tesla (Harris, 2022; Tofel, 2023).

Met betrekking tot de slimme controle door Tesla hebben wij laten zien dat met de datadeling een uniek eigenaarsprofiel wordt opgesteld. In de surveillanceliteratuur wordt in dit verband verwezen naar termen als ‘data double’ (Haggerty & Ericson, 2000), ‘digital persona’ (Clarke, 1994), ‘data shadow’ (Stalder, 2002) en ‘data derivative’ (Amoore, 2011). Een nadeel van deze termen – die duiden op een virtuele representatie van fysieke personen – is de suggestie die erin ligt besloten dat personen passieve subjecten zijn, wachtend om digitaal geclassificeerd te worden door private bedrijven en publieke organisaties. Deze suggestie gaat eraan voorbij dat – zoals deze casestudy laat zien – Tesla-eigenaren zich juist willen laten surveilleren, omdat de uitruil tussen hun persoonlijke data en nieuwe updates als iets positiefs wordt gezien en onderdeel is van een luxe levensstijl.

Dit schrille contrast tussen Tesla's bedrijfsmodel enerzijds en anderzijds de eigenaren die genieten van de digitale surveillance en daarbij een ‘ignorance is bliss’-hou-

ding erop na houden, is een onderwerp dat verder onderzoek verdient in de culturele en kritische criminologie.

Literatuur

- Alaimo, C. & J. Kallinikos (2024). *Data Rules: Reinventing the Market Economy*. Cambridge MA: The MIT Press.
- Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*. <https://doi.org/10.5210/fm.v13i3.2142>
- Amoore, L. (2011). Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times. *Theory, Culture & Society*, 28(6), 24-43.
- Andreas, P. (2003). Redrawing the Line: Borders and Security in the Twenty-First Century. *International Security*, 28(2), 78-111.
- Ball, K. (2009). Exposure: Exploring the subject of surveillance. *Information, Communications and Society*, 12(5), 630-657.
- Benjamins, (2024). Squeeveillance: Performing Cuteness to Normalise Surveillance Power. *Surveillance & Society*, 22(4), 350-363.
- Bratton, B. (2015). *The Stack: On Software and Sovereignty*. Cambridge: MIT Press.
- Brayne, S. (2017). Big Data Surveillance: 'The Case of Policing', *American Sociological Review*, 82(5), 977-1008.
- Clarke, R. (1994). The Digital Persona and its Application to Data Surveillance. *The Information Society*, 10(2), 77-92.
- Costello, L., McDermott, M.L., & R. Wallace (2017). Netnography: range of practices, misperceptions and missed opportunities. *International Journal of Qualitative Methods*, 16(1), 1-6.
- Currid-Halkett, E. (2017). *The sum of small things: A theory of the aspirational class*. Princeton, NJ: Princeton University Press.
- Daems, T. (2020). *Electronic monitoring. Tagging offenders in a culture of surveillance*. Cham, Switzerland: Palgrave Macmillan.
- Diphorn, T. (2021). Emic Security: An Anthropological Approach to Security. In S. Biecker & K. Schlichte (eds.), *The Political Anthropology of Internationalized Politics* (pp. 97-114). Rowman & Littlefield.
- Duran F., Wilson, S., & Carroll, D. (2005). *Putting administrative data to work: A toolkit for state agencies on advancing data integration and data sharing efforts to support sound policy and program development*. Farmington: Child Health and Development Institute of Connecticut.
- Eley, L., & Rampton, B. (2020). Everyday Surveillance, Goffman, and Unfocused Interaction. *Surveillance & Society*, 18(2), 199-215.
- Eski, Y., & Schuilenburg, M. (2022). On Tesla: Balancing sustainable car connectivity, silent lethality and luxury surveillance. *Criminological Encounters*, 5(1), 234-251.
- Federal Bureau of Investigation (2025). Public service announcement: Attacks on Tesla infrastructure. *Internet Crime Complaint Center (IC3)*. www.ic3.gov/PSA/2025/PSA250321
- Funnekotter, B. (2025). Musk stak zijn rechterarm in de lucht. Was het een Hitlergroet? www.nrc.nl/nieuws/2025/01/21/musk-stak-zijn-rechterarm-in-de-lucht-was-het-een-hitlergroet-a4880327
- Gacek, J. (2022). *Portable prisons: Electronic monitoring and the creation of carceral territory*. Canada: McGill-Queens University Press.

- Gandy, O. (1993). *The panoptic sort: A political economy of personal information*. Boulder, CO: Westview.
- Gilliard, C., & D. Golombia (2021). Luxury Surveillance: People pay a premium for tracking technologies that get imposed unwillingly on others. *Real Life Magazine*, July 6.
- Gould, G., Loader, I., & Thumala, A. (2013). The Banality of Security: The Curious Case of Surveillance Cameras. *The British Journal of Criminology*, 53(6), 977-996.
- Gouldner, A. (1960). The Norm of Reciprocity: A Preliminary Statement. *American Sociological Review*, 25(2), 161-178.
- Haggerty, K., & Ericson, R. (2000). The surveillant assemblage. *British Journal of Sociology*, 51(4), 605-622.
- Harris, M. (2022). The Radical Scope of Tesla's Data Hoard. Logs and records of its customers' journeys fill out petabytes – and court case dockets. <https://spectrum.ieee.org/tesla-autopilot-data-scope>
- Headworth S. (2023). *Rules of the Road: The Automobile and the Transformation of American Criminal Justice*. Stanford: Stanford Univ. Press.
- Hedges & Company (Automotive Market Research) (2024). Tesla owner demographics: Income, age, gender, and more. <https://hedgescompany.com/blog/2018/11/tesla-owner-demographics/>
- Hempel, L., & Töpfer, E. (2009). The Surveillance Consensus: Reviewing the Politics of CCTV in Three European Countries. *European Journal of Criminology*, 6(2), 157-177.
- Hotz V.J., Goerge, R., Balzekas, J., & Margolin, R. (1998). *Administrative data for policy-relevant research: Assessment of current utility and recommendations for development*. Chicago, IL: Joint Center for Poverty Research.
- Khalfa, R., Snaphaan, T., Wijsman, O. et al. (2024). Big data policing: de implicaties van digitalisering en maatschappelijke dataficatie voor de politiefunctie en het politiewerk. *Tijdschrift voor Veiligheid*, 23(1-2), 31-52.
- Kienscherf, M. (2022). Surveillance Capital and Post-Fordist Accumulation: Towards a Critical Political Economy of Surveillance-for-Profit. *Surveillance & Society*, 20(1), 18-29.
- Kostkova, P. (2018). Disease surveillance data sharing for public health: the next ethical frontiers. *Life Sciences, Society and Policy*, 14, 16-21.
- Kozinets, R. (2002). The field behind the screen: using netnography for marketing research in online communities. *Journal of Marketing Research*, 39(1), 61-72.
- Kraaijvanger, T. (2025) Hoe voorkom ik Tesla-vandalisme? <https://tesla360.nl/hoe-voorkom-ik-tesla-vandalisme>
- Kurt, A. et al. (2017). Factors Influencing Participation in Clinical Trials: Emergency Medicine vs. Other Specialties. *Western Journal of Emergency Medicine: Integrating Emergency Care with Population Health*, 18(5), 846-855.
- Leese, M. (2015). 'We were taken by surprise': Body scanners, technology adjustment, and the eradication of failure. *Critical Studies on Security*, 3(3), 269-282.
- Levitt, S.D., & List, J.A. (2011). Was There Really a Hawthorne Effect at the Hawthorne Plant? An Analysis of the Original Illumination Experiments. *American Economic Journal: Applied Economics*, 3(1), 224-238.
- Lippert, R., & Wilkinson, B. (2010). Capturing crime, criminals and the public's imagination: Assembling Crime Stoppers and CCTV surveillance. *Crime, Media, Culture*, 6(2), 131-152.
- Li, Y., Lin, J., & Xu, S. (2021). *Analysis of Tesla's Business Model: A Comparison with Toyota*. 2021 International Conference on Financial Management and Economic Transition (FMET 2021), Guangzhou: China.

- Loader, I. (2025). Concerning Cars: Automobility and the Contours of Control, Order, and Harm. *Annual Review of Criminology*, 8(1), 215-237.
- Lumsden, K. (2013). *Boy Racer Culture: Youth, Masculinity and Deviance*. Abingdon, UK: Routledge.
- Lutz, C., Hoffmann, P., & Ranzini, G. (2020). Data Capitalism and the User: An Exploration of Privacy Cynicism in Germany. *New Media & Society*, 22(7), 1168-1187.
- Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.
- Lyon, D. (2007). *Surveillance Studies: An Overview*, Cambridge: Polity Press.
- Marx, G. (2006). Soft surveillance: The growth of mandatory volunteerism in collecting personal information – ‘Hey Buddy can you spare a DNA?’ In: T. Monahan (ed.), *Surveillance and Security* (pp. 37-56). New York: Routledge.
- Marx, G. (2016). *Windows into the soul, Surveillance and society in an age of high technology*. Chicago: University of Chicago Press.
- Mauss, M. (2002 [1923-1924]). *The Gift: The Form and Reason for Exchange in Archaic Societies*. London: Routledge.
- McKay, C. & Lee, M. (2020). Body-worn images: Point-of-view and the new aesthetics of policing. *Crime, Media, Culture*, 16(3), 431-450.
- Menoret, P. (2014). *Joyriding in Riyadh: Oil, Urbanism and Road Revolt*. Cambridge, UK: Cambridge University Press.
- Minnaar, A. (2007). The implementation and impact of crime prevention / crime control open street Closed-Circuit Television surveillance in South African Central Business Districts. *Surveillance and Society*, 4(3), 174-207.
- Monahan, T. (2010). *Surveillance in the Time of Insecurity*. New Brunswick, NJ: Rutgers University Press.
- Murakami Wood, D. & Ball, K. (2013). Brandscapes of Control: Surveillance, marketing and the co-construction of subjectivity and space in neo-liberal capitalism. *Marketing Theory*, 13(2), 47-67.
- Muzzatti, S. (2010). ‘Drive it like you stole it’: A Cultural Criminology of Car Commercials. In: K. Hayward & M. Presdee (Eds.), *Framing Crime: Cultural Criminology and the Image* (pp. 138-155), London: Routledge.
- RTL Nieuws (2025). Nederlandse Tesla-bezitters slachtoffer van vandalisme: ‘Ik ben ook geen fan van Musk.’ www.rtl.nl/nieuws/binnenland/artikel/5500252/ook-nederlandse-teslas-doelwit-van-vandalisme-ik-ben-ook-geen-fan
- Schuilenburg, M. (2023). Big data policing: Schets van de belangrijkste vraagstukken, partijen en nieuwste trends in de praktijk. In: T. Snaphaan et al. (Eds.), *Cahiers Politiestudies 66: Big data policing* (pp. 53-70). Oud-Turnhout: Gompel & Svacian.
- Schuilenburg, M. (2024). *Making Surveillance Public: Why You Should Be More Woke About AI and Algorithms*. The Hague: Eleven International Publishing.
- Schuilenburg M., & Eski, Y. (2025). Data Sharing: A Case-Study of Luxury Surveillance by Tesla. *Surveillance & Society*, 23(2), 199-217.
- Schuilenburg, M., & Peeters, R. (2017). Gift Politics: Exposure and Surveillance in the Anthropocene. *Crime, Law and Social Change*, 68(5), 563-578.
- Schuilenburg, M., & Soudijn, M. (2023). Big Data Policing: The Use of Big Data and Algorithms by the Netherlands Police. *Policing: A Journal of Policy and Practice*, 17, paad061.
- Skatova, A., & Goulding, J. (2019). Psychology of personal data donation. *Plos One*, 14(11), e0224240.
- Srnicek, N. (2017). *Platform Capitalism*. Cambridge: Polity Press.

- St. Louis, E., Saulnier, A., & Walby, K. (2019). Police Use of Body-Worn Cameras: Challenges of Visibility, Procedural Justice, and Legitimacy, *Surveillance and Society*, 17(3/4), 305-321.
- Stalder, F. (2002). Privacy is not the Antidote to Surveillance. *Surveillance and Society*, 1(1), 120-124.
- Tesla (2025). Customer Privacy Notice. www.tesla.com/legal/privacy#:~:text=Energy%20diagnostic%20logs&text=There%20are%20four%20categories%20of,System%20Data%2C%20and%20Autopilot%20Data
- Thalia, A., & Tranter, K. (2018). Car crimes and the cultural imagination. In: N. Rafter & M. Brown (Eds.), *The Oxford Research Encyclopedia of Crime, Media and Popular Culture* (pp. 468-488). Oxford, UK: Oxford University Press.
- Tofel, K.C. (2023). Tesla: The ultimate example of data privacy vs convenience. <https://staceyoniot.com/tesla-the-ultimate-example-of-data-privacy-vs-convenience/>
- Tracy, S.J. (2019). *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact*. Wiley: John Wiley & Sons.
- Trein, P., & Varone, F. (2023). Citizens' agreement to share personal data for public policies: trust and issue importance. *Journal of European Public Policy*. <http://dx.doi.org/10.1080/13501763.2023.2205434>
- Trottier, D. (2012). Policing social media. *Canadian Review of Sociology*, 49(4), 411-425.
- Verheggen, F.W.S.M, Nieman, F., & Jonkers, R. (1998). Determinants of patient participation in clinical studies requiring informed consent: Why patients enter a clinical trial. *Patient Education and Counseling*, 35(2), 111-125.
- West, E. (2019). Amazon: Surveillance as a Service. *Surveillance & Society*, 17(1/2), 27-33.
- White, M., Gaub, J., & Todak, N. (2018). Exploring the Potential for Body-Worn Cameras to Reduce Violence in Police–Citizen Encounters. *Policing: A Journal of Policy and Practice*, 12(1), 66-76.
- Wood, D.M., & Ball, K. (2013). Brandscapes of control? Surveillance, marketing and the co-construction of subjectivity and space in neo-liberal capitalism. *Marketing Theory*, 13(1), 47–67.
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY: Public Affairs.