SIGNIFICANT OTHERS

Interview met Chris Gilliard (aka Hypervisible)

‘Als het gaat om technologieën die fundamenteel discriminerend zijn, moet het doel altijd abolitionisme zijn’

Marc Schuilenburg & Yarin Eski

Chris Gilliard wordt gerekend tot een van de meest invloedrijke stemmen op het gebied van digitale surveillance. Hij doceert aan het Macomb Community College, een openbare school voor middelbaar beroepsonderwijs, in de Verenigde Staten en neemt vaak en stevig stelling in het debat over de (on)mogelijkheden van nieuwe vormen van surveillance. Als publiek wetenschapper benadrukt Gilliard hoe historische vooroordelen hun weg vinden naar digitale systemen vanwege de manier waarop algoritmes worden gemaakt en getraind. Zo getuigde hij in 2019 voor het Amerikaanse House Financial Services Committee over de manier waarop in de bancaire wereld big data en algoritmes leiden tot een verdere versterking van reeds

Tijdschrift over Cultuur & Criminaliteit 2023 (13) 2
doi: 10.5553/TCC/221195072023013002009

bestaande vormen van discriminatie.[1] Met zijn collega Hugh Culik muntte hij hiervoor de term 'digital redlining' om daarmee aandacht te vragen voor internettools die verschillende vormen van inhoud blokkeren, waardoor gemarginaliseerde groepen in de samenleving verder worden gediscrimineerd.[2] Een goed voorbeeld van deze nieuwe vorm van segregatie is de manier waarop de advertentietargeting van Facebook werkt. Journalisten van ProPublica ontdekten dat zwarte mensen niet alle advertenties voor huisvesting kregen te zien, waardoor ze van een deel van de huizenmarkt werden buitengesloten, ondanks dat juridische regels als de Fair Housing Act dergelijk gedrag verbieden. 'Luxury surveillance' is een ander concept van Gilliard dat tot veel weerklank leidt. Dit zijn producten waarvoor personen bereid zijn veel geld te betalen en waarvan de mogelijkheden – zoals tracking en monitoring van jezelf en van andere personen – worden gezien als positieve eigenschappen. Denk hierbij aan de slimme videodeurbel Ring van Amazon of de Apple Watch en Fitbit waarmee je je gezondheid kunt meten.
Opvallend is dat Gilliards invloed niet is gebaseerd op vuistdikke boeken of peer-reviewed artikelen over de wijze waarop we voortdurend worden bekeken en kijken naar andere personen. Zijn faam dankt hij aan korte essays over digitale surveillance in techbladen als *Wired*, *Real Life*, *The Atlantic* en *Vice*, met aansprekende titels als 'Friction-free racism' en 'There are no guardrails on our privacy dystopia'. Hij lijkt zich hiermee te verzetten tegen de impact-publicatiecultuur op universiteiten wereldwijd. Zo is hij zeer actief op X (voorheen Twitter) onder de gebruikersnaam 'Hypervisible', die volgens Gilliard staat voor 'blackness being seen and not understood'. Volgens een profielschets van Gilliard in *The Washington Post* uit 2021 maakt hij deel uit van een bredere beweging in de Verenigde Staten die probeert bloot te leggen hoe de technologie-industrie, die van oudsher wordt gedomineerd door witte en Aziatische mannen, haar eigen vooroordelen heeft ingebouwd in producten die nu door miljoenen mensen worden gebruikt. Andere bekende schrijvers en academici die tot deze beweging behoren, zijn Safiya Umoja Noble en Ruha Benjamin.[3]

Voor dit special issue over digitale surveillance spreken we met Gilliard over onderwerpen zoals zijn jeugd, zijn interesse in en kritiek op surveillancetechnologie, en over de soms inherente discriminatoire aard van nieuwe big data-toepassingen en algoritmes.

ToCC: Kun je ons iets vertellen over je persoonlijke achtergrond?

CG: Ik woon in Dearborn, Michigan, een stad met de grootste populatie moslims in de Verenigde Staten. Ik ben opgegroeid in een gezin van acht kinderen in Detroit in de jaren 1970 en 1980. Dat gebeurde toen onder, wat ik in interviews en artikelen geregeld noem, het spook van de Detroitse politie-eenheid STRESS, wat een acroniem is voor 'Stop the Robberies, Enjoy Safe Streets'. Deze eenheid richtte zich

1 Zie www.congress.gov/116/meeting/house/110251/witnesses/HHRG-116-BA00-Wstate-GillardC-20191121.pdf.
2 Zie www.commonsense.org/education/articles/digital-redlining-access-and-privacy.
3 Zie www.washingtonpost.com/technology/2021/09/16/chris-gilliard-sees-digital-redlining-in-surveillance-tech/.

vooral op de zwarte gemeenschappen in Detroit, in gebieden met veel criminaliteit. Destijds heb ik vaak geweerlopen op mij gericht gehad door de politie. In de 3,5 jaar dat de eenheid actief was, doodde STRESS 24 mensen, van wie er 21 zwart waren. Pas in 1974 werd onder druk van de publieke opinie en talloze rechtszaken de eenheid eindelijk opgeheven. Die gebeurtenissen zijn bepalend geweest voor hoe ik nu denk over de inzet van surveillance om de samenleving veiliger te maken.
In mijn werk houd ik me bezig met hoe surveillancemiddelen onevenredig worden ingezet tegen de zwarte bevolking. Denk bijvoorbeeld aan gezichtsherkenningssystemen die zwarte personen ten onrechte beschuldigen van allerlei zaken, waaronder fraude en andere vormen van criminaliteit. Maar denk ook aan de politie van Los Angeles, die de beelden van de Amazon Ring-deurbel heeft opgevraagd van Black Lives Matter-protesten.
Op dit moment is Detroit nog steeds een van de strengst bewaakte steden in de Verenigde Staten. De alom aanwezige bewakingsdrang blijkt onder meer uit het 'Project Green Light Detroit', dat een aantal jaren geleden is ingevoerd. Het gaat hierbij om een publiek-private samenwerking om de criminaliteit terug te dringen, waarbij gebruik wordt gemaakt van een web aan veiligheidscamera's en de inzet van ShotSpotters. Hierbij wordt microfoontechnologie ingezet waarmee de locatie van geweerschoten kan worden gedetecteerd, zodat de politie kan reageren zónder dat er een 911-oproep is geweest.
Mijn stelling is dat bijna alles wat we tegenwoordig meemaken in termen van toezicht en onderdrukking slechts uitbreidingen zijn van al langer bestaande praktijken, maar dat die praktijken in reikwijdte en schaal worden vergroot door nieuwe surveillancetechnologieën, waarbij het vooral gaat om het gebruik van big data en AI. Deze nieuwe technologieën worden als het ware witgewassen met termen als 'objectiviteit' en 'nauwkeurigheid'.

ToCC: Wanneer raakte je professioneel geïnteresseerd in surveillance?

CG: Persoonlijk ben ik altijd al geïnteresseerd geweest in dit onderwerp, maar sinds de laatste vijf jaar heeft mijn interesse steeds meer een publieke uiting gekregen. Het is lastig een lijst van favoriete wetenschappers te noemen die mij hierbij hebben beïnvloed, maar als er een boek uit springt, dan is het *Dark matters. On the surveillance of blackness* van Simone Browne uit 2015. Wat mijn denken ook heeft getriggerd, is de weerstand tegen en de collectieve schade die wordt veroorzaakt door surveillancesystemen. Ik denk hierbij aan het verzet van de bewoners van de Atlantic Towers in Brooklyn, New York, tegen het ophangen van gezichtsherkenningssystemen door hun huurbaas. Of aan de commotie rondom het project van Googles zusterbedrijf Sidewalk om het industriegebied Waterfront in Toronto te veranderen in een zogenoemde 'slimme wijk' door alle data van de bewoners te verzamelen.

ToCC: In je werk wijs je op de negatieve uitwerkingen van surveillance. Maar aan surveillance zijn ook positieve aspecten verbonden, denk bijvoorbeeld aan de zorg van ouders voor hun kinderen of die van dokters voor hun patiënten. Op dit moment helpen commerciële drones Oekraïne bijvoorbeeld in de oorlog tegen Rusland. Herken je deze spanning in surveillance, en hoe is die spanning te adresseren?

doi: 10.5553/TCC/221195072023013002009

CG: In sommige opzichten denk ik dat jullie vraag al een antwoord is. Dat surveillance in oorlogstijd een aantal 'nuttige' toepassingen heeft, helpt precies te verklaren waarom ze niet – onder normale omstandigheden – tegen de burgerbevolking zou moeten worden ingezet. Vergis je niet, er is in de Verenigde Staten altijd sprake geweest van een duidelijke route die oorlogstechnologieën afleggen: van oorlogen die we voeren in andere landen naar lokale handhavingsinstanties in Amerikaanse steden, en zelfs naar particuliere bedrijven. Ik durf zelfs te spreken van een heuse 'surveillancestroom'. Ik vind het daarom moeilijk, zo niet onmogelijk, om afstand te nemen van het dystopische aspect van surveillance. Juist omdat er machtige instellingen, autoritaire regeringen en technologiebedrijven zijn met onbeperkte fondsen die ons allemaal consequent in de richting van meer surveillance proberen te duwen. Zelfs in de gevallen waarin surveillancetechnologie nuttig zou kunnen zijn, zoals spraakondersteuning of een mobiel gezondheidsapparaat, zorgen data-extractie en exploitatie van gegevens dat de utopische elementen, het helpen van mensen bijvoorbeeld, dikwijls op de achtergrond raken, waardoor die technologieën steevast leiden tot een vorm van totaalcontrole van de bevolking.

ToCC: Leidt zo'n zienswijze niet tot een vorm van technologisch determinisme?

CG: Pas op, ik wil niet zeggen dat surveillancetechnologieën altijd het menselijke element elimineren. Ik denk eerder dat het bijna onmogelijk wordt om er weerstand aan te bieden, juist omdat veel personen niet weten wat er allemaal gaande is en hoe die technologieën in de praktijk werken. Ik aarzel om termen zoals determinisme te gebruiken, maar ik vind het lastig om met een andere term te komen om de invloed van digitale technologieën in ons dagelijkse leven goed te duiden en te bediscussiëren.

ToCC: Data-ethiek wint snel aan belang bij het ontwerp en de inzet van digitale surveillance, waaronder benaderingen als Value Sensitive Design en ethisch pluralisme. Wat is je mening over deze ontwikkeling?

CG: Ik ben hierover erg sceptisch. Ik heb vaak geschreven dat surveillance altijd haar weg vindt in de samenleving. Ruha Benjamin zegt het fraai: 'Ons uitgangspunt zou moeten zijn dat geautomatiseerde systemen ongelijkheid zullen vergroten, tenzij het tegendeel wordt bewezen.' Dat betekent dat in een antizwarte samenleving transfobische en carcerale surveillancestructuren altijd zullen worden ingezet om machtsverhoudingen in stand te houden en te bestendigen, tégen de zwarte bevolking. Met dat in gedachte, denk ik dat er te veel pogingen worden ondernomen om bestaande surveillancesystemen te hervormen, terwijl we ze eigenlijk zouden moeten ontmantelen of verbieden. Anders gezegd, er wordt nu vooral nadruk gelegd op de hervorming van negatieve effecten van surveillance zoals discriminatie en etnisch profileren, in plaats van die systemen gewoonweg te elimineren. Als het gaat om technologieën die fundamenteel discriminerend zijn, moet het doel altijd abolitionisme zijn. Vergelijk het met de situatie waarin een hamburgerrestaurant voedsel serveert waardoor 60 procent van de klanten komt te overlijden. Dan wordt dat restaurant toch meteen gesloten? Waarom doen we dat niet

met bedrijven als Facebook en Google, waarvan we weten dat ze technologieën inzetten die racistisch en discriminatoir zijn?

ToCC: Past hierin ook wat je hebt geschreven over 'friction-free racism'?

CG: Ja, het klinkt paradoxaal, maar frictie houdt mij veilig. Zoals het idee dat ik me ervan bewust ben dat er talloze racistische praktijken bestaan, waardoor ik ook weet hoe ik hiermee moet omgaan of waarop ik moet letten. Vaak worden nieuwe technologieën gepromoot onder het mom van efficiëntie en frictieloos, in de zin dat ze vervelende beperkingen in ons leven uit de weg ruimen. Ik geloof daar niet in. We moeten blijven onderzoeken hoe surveillance de meest kwetsbare en meest gemarginaliseerde groepen in de samenleving blijft schaden. Dit alles gaat namelijk veel verder dan wat iemand redelijkerwijs zou mogen verwachten. Zelfs kinderen komen terecht in databases voor gezichtsherkenning, databases die voor allerlei vreselijke dingen worden gebruikt, tot en met militaire toepassingen aan toe.

ToCC: Je geeft aan dat je de machine niet actief wilt voeden, bijvoorbeeld door je profielfoto offline te houden op Twitter. Zou je kunnen uitleggen hoe en waarom andere personen gemotiveerd moeten worden om dit ook te doen?

CG: Ik heb hiervoor een aantal redenen. Veel van de grote Amerikaanse surveillancebedrijven worden vaak – en daar zijn overtuigende argumenten voor te geven – in verband gebracht met extreemrechtse bewegingen en witte suprematie. Daarbij komt dat gezichtsherkenning – en surveillance in het algemeen – een vorm is van controle en macht. Ik probeer daarom waar mogelijk geen afbeeldingen van mijn gezicht op internet te zetten. Ik ben me ervan bewust dat niet iedereen in dezelfde positie verkeert om hetzelfde standpunt in te nemen. Tegelijk ben ik zeer actief op platforms als Twitter, waardoor ik toch een publiek profiel heb. Een van de redenen waarom ik op Twitter belandde, was dat – naast alle rotzooi – ook tal van academische en intellectuele discussies hierop werden gevoerd die niet beschikbaar waren op mijn academische instelling, door personen wier werk ik lees of bewonder, zoals Frank Pasquale, David Golombia, Tressie McMillan en Audrey Watters. Ik had zoiets van: 'Wauw, ik kan met één druk op de knop inzicht krijgen in het denken van al deze personen.' Een tijdje heb ik op Twitter mijn naam veranderd in 'Hypervisible gaat binnenkort weg', of iets dergelijks. Maar ik zou hier niet met jullie praten als ik niet nog steeds actief op Twitter was.

ToCC: In hoeverre denk je dat er een verschil is tussen Europa en de Verenigde Staten met betrekking tot de problematiek van discriminatoire surveillancetechnologie?

CG: Het is nu vrijwel een 'free for all' in de Verenigde Staten. Illinois heeft een privacywet en Californië heeft er een, maar dat zijn uitzonderingen. Er zijn serieuze geruchten over de komst van een federale privacywet, maar op dit moment zijn lobbyen datamakelaars, die naar mijn mening een van de slechtste actoren zijn op dit gebied, druk om privacywetten verder af te zwakken. Dan ontstaat er een wetteloze samenleving. Weliswaar zijn er in de Verenigde Staten tal van beperkingen in het kader van wetshandhaving, maar er gelden bijna geen beperkingen voor bedrij-

doi: 10.5553/TCC/221195072023013002009

ven die over onze data beschikken. Wetshandhavers kunnen die gegevens opvragen of kopen en hiervoor hebben ze vaak geen gerechtelijk bevel nodig.

ToCC: Wat is privacy dan nog, en hoe kan zij beter worden beschermd? Is hiervoor een sterkere overheid nodig?

CG: Een sterkere overheid is niet het volledige antwoord. Er is al veel mogelijk, maar het grote probleem is hoe om te gaan met de misleidende praktijken van techbedrijven over wat hun technologie kan doen. Ik denk veel na over onderwijstechnologieën. Zelfs in het geval van technologieën die veiligheid of beveiliging of dat soort dingen op scholen bevorderen, is er sprake van een vorm van misleiding. De kloof is groot tussen wat bedrijven beweren en wat hun technologie daadwerkelijk kan. Er zijn nu tal van zogeheten 'proctoring-systemen', zoals *room scans*, *eye tracking* en data-analyse om scholieren te monitoren. Onlangs oordeelde een rechter dat zo'n *room scan* ongrondwettelijk is, omdat deze in strijd is met het 4de amendement van de Amerikaanse Grondwet waarin het recht op privacy is vastgelegd. Er zijn dus wel regels en wetten, maar er is weinig wil om ze daadwerkelijk af te dwingen.
Overigens wil ik de pogingen om privacywetgeving te versterken niet kleineren, ze raken namelijk aan de kern van waarom ik zo gepassioneerd ben over dit onderwerp. Zo hoor je steeds vaker dat privacy iets zou zijn uit het verleden of dat ze niet meer belangrijk is. Maar praat met de meest gemarginaliseerde bevolkingsgroepen, praat met gedetineerden, praat met vrouwen die hun uitkering of kinderen dreigen te verliezen, of praat met moslims in Amerika die continu in de gaten worden gehouden door de overheid: zij delen allemaal een zeer scherp gevoel voor de manier waarop hun privacy wordt geschonden. Om dan te beweren dat privacy niet bestaat of niet belangrijk is, is obsceen. De personen die beweren dat privacy onbelangrijk is, of niet meer bestaat, of dat niemand er iets om geeft, zijn vaak mensen in de meest bevoorrechte posities.
Ik sprak onlangs met de omroep NBC en de interviewer zei dat hij dit probleem heeft, dat als hij met zijn vrienden hierover praat, ze zeggen: 'Privacy, who cares?' Ik zei hierop: 'Ik heb een luchthartig antwoord. Dat is: trek al je kleren uit en geef me je sleutels en de wachtwoorden van al je apparaten. Niemand zal dat doen.' Tegelijk denk ik dat een hardnekkig misverstand is dat wanneer digitale systemen een oordeel vellen over personen, die systemen nauwkeurig en eerlijk werken. Dus als een systeem zegt dat je schuldig bent aan een misdaad, dat je kinderen moeten worden afgenomen, of dat je geen baan of lening kunt krijgen, dat zo'n oordeel dan op de een of andere manier nauwkeurig en objectief is. Daarvan is niets waar.

ToCC: Is surveillancetechnologie daarom een noodzakelijk kwaad waarmee we moeten leren leven?

CG: Ik heb hierop een lang antwoord, maar ik zal het beknopt houden. Kan er zoiets bestaan als een digitale spraakassistent die niet al je gegevens aan Amazon weggeeft? Het antwoord is: 'Ja.' Mijn probleem is daarom niet dat mensen bijvoorbeeld beveiligingscamera's ophangen. Ik kan begrijpen waarom burgers denken dat ze die nodig hebben. Mijn probleem is dat die camera's de opgenomen data sturen

naar een centrale locatie en dat die gegevens worden gebruikt voor andere doeleinden. Anders gezegd, we hebben een mythe gecreëerd over het delen van data met technologiebedrijven, namelijk dat die bedrijven deze gegevens ten goede zouden inzetten om consumenten te helpen. Wanneer iemand honderd camera's op zijn terrein heeft opgehangen en een harde schijf in een kast in zijn kelder heeft staan met alle gegevens daarop, en die blijft daar gewoon staan, dan is dat iets heel anders dan hoe de Amazon Ring-videodeurbel werkt, waarvan alle gegevens worden verstrekt aan het moederbedrijf. Kortom, ik denk niet dat surveillance iets is dat we als een noodzakelijk onderdeel van ons leven moeten accepteren om de voordelen ervan te kunnen hebben.

Een van de voorbeelden die ik in dit verband gebruik, is dat van de CEO van Zoom. Toen iedereen aan het begin van de coronapandemie op Zoom overging, zei de CEO: 'Ik had nooit gedacht dat Zoom zou worden gebruikt als doelwit, voor intimidatie, en andere zoom-interrupties.' Als ik vijf minuten met hem aan de telefoon had gezeten, had ik hem dit kunnen vertellen. Je hebt hiervoor geen bijzondere expertise nodig. Er zijn talloze voorbeelden van manieren waarop bedrijven, met een beetje vooruitziende blik of met een beetje zorg, zouden kunnen weten dat dergelijke systemen gaan worden misbruikt. Maar ze doen vaak weinig tot niets om dat te voorkomen.

Facebooks eigen onderzoek toonde aan dat een bepaald segment van Facebook zich bij extremistische groeperingen aansloot. Maar er werd niks tegen gedaan. Of denk aan het gebruik van Instagram, dat vooral schadelijk is voor jonge meisjes en vrouwen. Dat blijkt, opnieuw, uit eigen onderzoek van Instagram. Maar ze doen weinig of niets met die informatie omdat het voordeliger is om het te negeren. Aan de ene kant hebben we dus de kennis dat digitale surveillance niet zo hoeft te werken. Aan de andere kant hebben we bedrijven die zeggen: 'Als je gratis diensten wilt, moet je ons je gegevens geven.' Die twee kanten zijn volgens mij niet goed in balans.

Literatuur

Brown, S. (2015), *Dark matters. On the surveillance of blackness*. Durham, NC: Duke University.

Gilliard, C. (2022, 30 juni). School surveillance will never protect kids from shootings. *Wired*. Geraadpleegd op 7 juli 2023, van www.wired.com/story/school-surveillance-never-protect-kids-shootings.

Gilliard, C. (2022, 18 oktober). The rise of 'luxury surveillance'. *The Atlantic*. Geraadpleegd op 7 juli 2023, van www.theatlantic.com/technology/archive/2022/10/amazon-tracking-devices-surveillance-state/671772.

Gilliard C. & Culik, H. (2016, 24 mei). Digital redlining, access, and privacy. *Common Sense Education*. Geraadpleegd op 7 juli 2023, van www.commonsense.org/education/articles/digital-redlining-access-and-privacy.

Gilliard, C. & Golombia, D. (2018, 9 maart). There are no guardrails on our privacy dystopia. *Vice*. Geraadpleegd op 7 juli 2023, van www.vice.com/en/article/zmwaee/there-are-no-guardrails-on-our-privacy-dystopia.

Gilliard, C. & Golombia, D. (2021, 6 juli). Luxury surveillance: People pay a premium for tracking technologies that get imposed unwillingly on others. *Real Life Magazine*. Geraadpleegd op 7 juli 2023, van https://reallifemag.com/luxury-surveillance.

doi: 10.5553/TCC/221195072023013002009