De wereld buiten je voordeur

Contextual integrity bij slimme deurbellen

Matt ter Steege, 9932003
matttersteege@gmail.com
Universiteit Utrecht
Utrecht, Nederland

1 abstract

Er verschijnen steeds meer videodeurbellen aan de deurposten. Dit roept de vraag op of dit niet een immense inbreuk op privacy is. Het doel van dit onderzoek is om te achterhalen of en hoe privacy in de verdrukking komt door deze nieuwe surveillancetrend. De achterliggende onderzoeksvraag is daarom ook: *Hoe beïnvloedt het constant filmen van slimme deurbellen de privacy van buren en voorbijgangers?* Om op een antwoord te komen wordt er een bronnenonderzoek gedaan en worden de bevindingen op verschillende gebieden **Privacy theorie**, **technische aspecten van slimme deurbellen**, **maatschappelijke en ethische implicaties** en **gebruikerservaringen / gedrag**

Uit de bronnen blijkt dat de bedrijven die achter de videodeurbellen zitten, niet altijd het beste voor hebben met de klanten. Ook is het niet altijd duidelijk wat er met de data gebeurt die wordt opgenomen door de deurbellen en/of ze daadwerkelijk verwijderd worden als dat gevraagd is. Maar niet alles is aan de bedrijven te wijten, want klanten (met name “ervaren gebruikers”) hadden liever gemak en functies over privacy.

2 Introductie

We leven in een tijd waarin zoveel mogelijk onderdelen van iemands leven aan het internet gekoppeld (kunnen) worden. Zo ook je eigen voordeur: de opkomst van zogenaamde videodeurbellen, zoals deurbellen van Ring of Eufy, is een steeds bekender gezicht in de wijken van Nederland. Het plus- (en tevens ook min-)punt van deze producten is dat elke (verdachte) beweging die de deurbel detecteert, wordt opgenomen en doorgestuurd naar de eigenaar. Mogelijke inbrekers worden afgeschrikt door het idee dat ze op video staan bij een inbraakpoging en dat zorgt bij veel mensen voor een veilig gevoel, maar dit heeft ook een keerzijde. De postbode die je krantje komt bezorgen, maar ook voorbijrijdende auto’s, buren die een ommetje maken of kinderen die langsfietsen worden ook opgenomen, terwijl dit niet de doelgroep is waarvoor (of waartegen) deze deurbel ontworpen is. Dit roept de vraag op:

Hoe beïnvloedt het constant filmen van slimme deurbellen de privacy van buren en voorbijgangers?

Deze vraag sluit nauw aan bij het concept contextuele integriteit van Helen Nissenbaum, waarin iemand zo goed mogelijk in zijn of haar persoonlijke vrijheid gelaten wordt en data alleen in een passende context gedeeld mag worden. Videodeurbellen doorbreken deze verwachte informatiestromen, want waar voorbijgangers normaal anoniem over straat liepen, worden zij nu onbewust onderdeel van een digitaal surveillancesysteem.

2.1 Theoretisch kader

(Nissenbaum, 2009) Schreef al over een door haar ontwikkeld privacy theorie: **contextuele integriteit**. Dit schreef zij in haar boek *Privacy In Context: Technology, Policy, and the Integrity of Social Life.*

- Privacy wordt gewaarborgd door passende informatiestromen.
- Passende informatiestromen zijn stromen die voldoen aan contextuele informatienormen.
- Contextuele informatienormen verwijzen naar vijf onafhankelijke parameters: betrokkene, afzender, ontvanger, informatietype en transmissie-principe.
- Concepties van privacy zijn gebaseerd op ethische overwegingen die in de loop der tijd evolueren.

Nissenbaum stelt dat privacy en wat acceptabel is om te delen af hangt van de situatie waarin men op dat moment leeft. Een voorbeeld hiervan is dat het (doorgaans vaak) niet gewenst is om je medische dossier met Jan en alleman te delen, echter met een dokter of huisarts is dit natuurlijk wel wenselijk. Hier komt contextuele integriteit goed naar boven. Want gebaseerd op de situatie deel je (of wil je) wel of niet bepaalde data met bepaalde entiteiten en deze entiteiten deze data ook niet doorgeven aan andere waarvoor de data niet nodig is.

Dit wijkt af van het “traditionele" denkbeeld, oftwel *control over information* waarin een individu zelf zijn data beheert en kiest of data wel of niet gedeeld wordt. Dit is veel meer individu-gecentreerd en contextuele integriteit is meer (je raadt het al) context-gecentreerd.

2.2 Relevantie

Videodeurbellen zijn dus nauw verbonden met het concept contextuele integriteit. Voor eigen veiligheid (of gemoedsrust) schaffen steeds meer mensen een videodeurbel aan, dit gaat echter ten koste van de privacy van voorbijgangers, buren en andere die toevallig langs een huis met een videodeurbel lopen. Daarom wordt in dit onderzoek gekeken naar of de waarde in veiligheidsgevoel opweegt tegen het ongevraagd (en passief) filmen van voorbijgangers en dergelijke.

3 Methode

Dit onderzoek is een kwantitatief onderzoek om de vragen rondom de contextuele integriteit en privacy en Slimme (video) deurbellen te beantwoorden. Hiervoor is uitsluitend literatuuronderzoek gedaan. Er zijn veel verschillende bronnen geraadpleegd, dit is grotendeels via Google Scholar gedaan. Hierbij zijn verschillende zoektermen gebruikt zoals: Slimme deurbel, Ring (video)deurbel, Smart doorbell, Privacy video doorbell.

De gebruikte bronnen zijn afkomstig uit wetenschappelijke publicaties en tijdschriften. Zo vormt het werk van Nissenbaum een theoretisch fundament op het gebied van privacy en contextuele integriteit.

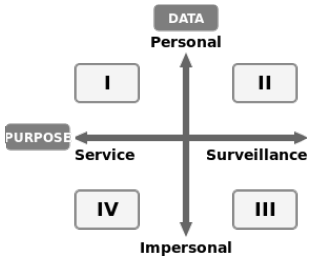
Van Zoonen biedt een bruikbaar framework en Shaffer levert een casestudy over de samenwerking tussen Ring en de politie, wat direct aansluit bij het onderwerp van dit onderzoek (4.1). Daarnaast bieden studies van Liu, Lalitha et al. en Chaudhari et al. een technisch perspectief op slimme deurbellen, waarbij veiligheid en functionaliteit empirisch worden onderzocht (4.2). Tot slot leveren

Selinger and Durant en Kelly kritische beschouwingen over Amazon's Ring en de maatschappelijke gevolgen van consumentgestuurde surveillance (4.3). Artikelen van Shaffer en Tabassum and Lipford bouwen daarop voort met recente analyses van smart home-privacy en gebruikerscontrole, gepubliceerd in peer-reviewed journals (4.4). Samen bieden deze bronnen een goed gebalanceerde mix van theoretische, technische en ethische invalshoeken, afkomstig uit betrouwbare en actuele academische contexten.

4 Beschouwing van literatuur

4.1 Privacy-theorie

(Van Zoonen, 2016) stelt dat data in een privacy framework (Figuur 1) opgedeeld kan worden. Deze is opgedeeld in twee assen: de y-as geeft aan of data wel of niet persoonlijk is, en de x-as geeft aan of data wordt gebruikt om te helpen of om te monitoren.



Figuur 1: Privacy framework (nagemaakt van],][)van2016privacy

In het tweede kwadrant (**II**) gaat het over het verzamelen van persoonlijke data om te monitoren. Dit betreft bijvoorbeeld politiedata of beelden van beveiligingscamera's. Mensen ervaren dit als zeer persoonlijke en gevoelige informatie, wat tot kritiek leidt op toezicht en controle. Zo kreeg de burgemeester van Nice in 2008 een "Big Brother Award" voor het volhangen van de stad met camera's, en Dresden kreeg deze prijs in 2012 voor het volgen van mobiele telefoons tijdens een demonstratie.

Tegelijkertijd hangt hoe bezorgd mensen af van tijd en situatie. Zo werd geschreven: "*Acceptance of the US government monitoring personal communications was high in the immediate aftermath of the 9/11 attacks but declined after about half a year.*" (Van Zoonen, 2016, p. 474)

Het derde kwadrant (**III**) gaat over data die niet direct aan één persoon gekoppeld zijn, maar wél gebruikt worden om gedrag of situaties te controleren. Denk aan verkeersstromen of drukte op stations en evenementen. Op het eerste gezicht lijkt dit onschuldig, omdat het om groepen, patronen of cijfers gaat, en niet om individuen.

Steden gebruiken zulke "anonieme" data vaak om beleid te maken. Rotterdam bijvoorbeeld verzamelt en koppelt diverse datasets, van politiedata tot economische cijfers, om risicowijken te identificeren of criminaliteit te voorspellen[1]. Toch schuilt hier een gevaar: hoe meer datasets worden gekoppeld, hoe makkelijker het wordt om individuen te identificeren. Anonieme data verandert zo in persoonlijke data, wat wantrouwen en zorgen over discriminatie en controle kan veroorzaken.

Een concreet voorbeeld van deze privacyzorgen is de samenwerking tussen Ring en de Long Beach Police Department (LBPD) in augustus 2019 (Shaffer, 2021). Via de app *Neighbors* konden bewoners videobeelden van Ring-deurbellen delen met de politie. Officieel vrijwillig, maar in de praktijk voelde het voor velen als een sluiproute naar burgerlijke surveillance. De reacties waren gemengd: sommigen zagen het als logisch voor criminaliteitsbestrijding, anderen als zorgelijk omdat politie en een commercieel bedrijf (Amazon, het moederbedrijf van Ring) steeds dieper in de privésfeer doordringen. Het ongemak werd versterkt doordat bewoners Amazon veel minder vertrouwen dan de politie.

Uiteindelijk draait de discussie niet om de videodeurbellen zelf, maar om macht en controle: wie kijkt mee, en wie bepaalt wat er met de verzamelde data gebeurt?

4.2 Technische aspecten van slimme deurbellen

Een samengevoegd overzicht van technische, bouwkundige en praktische perspectieven op privacy en beveiliging bij slimme deurbellen. Hieronder volgen de bevindingen en reflecties uit drie studies — elk met hun eigen focus — maar samengebracht onder één overkoepelend thema: wat betekent *privacy* technisch en praktisch in een world-wide-netwerk van videodeurbellen?

Na uitvoerig *threat modeling* en *penetration testing* concludeert (Liu, 2021) dat de onderzochte smart video deurbel over het algemeen degelijk maar niet foutloos is. Er werden geen directe, kritieke zero-days[2] gevonden, maar er zijn meerdere zwakke plekken die in de praktijk misbruikt kunnen worden — met name in de Android-app, de accountbeveiliging en de draadloze communicatie. Belangrijk is dat deze zwaktes vooral aantonen dat privacy geen gegeven is; het is iets dat voortdurend verdedigd moet worden.

Categorie	Belangrijkste bevindingen en verbeterpunten
Android-applicatie	Gevoelige data kan uitlekken doordat de app-data niet goed wordt afgeschermd. Externe opslag moet worden vermeden en verouderde encryptie vervangen, certificaatvalidatie is zwak (zelfondertekende certificaten worden te snel vertrouwd). Positief is dat de code lastig te manipuleren is door de gesegmenteerde .dex-bestanden.
Accountbeveiliging	Wachtwoorden worden gehasht met MD5, wat onveilig is en makkelijk te breken. Sessies worden in URL's doorgegeven in plaats van via veilige cookies of POST-methoden. CAPTCHA's beperken brute-force aanvallen effectief en het wachtwoordbeleid zorgt voor goed genoege wachtwoorden.
Draadloze communicatie	Verkeer tussen app en deurbel verloopt via HTTPS, waardoor afluisteren bemoeilijkt wordt. Toch blijft een MitM-aanval mogelijk als de aanvaller een eigen CA weet te installeren. Replay-aanvallen zijn theoretisch uitvoerbaar bij specifieke verzoeken (zoals uitloggen of gebruikers delen). Deauthenticatie-aanvallen kunnen de deurbel tijdelijk uitschakelen en zelfs helpen bij het kraken van het Wi-Fi-wachtwoord.

Tabel 1: Overzicht van de belangrijkste beveiligingsbevindingen van de smart video deurbel

Liu benadrukt dat beveiligingstesten op IoT-apparaten geen bijzaak zijn — veel producten bevatten nog steeds fouten in encryptie, databeheer en netwerkgedrag. Xiaomi stond dit onderzoek toe onder de voorwaarde dat andere gebruikers of servers niet werden geraakt; alle testen werden op eigen apparaten en accounts uitgevoerd en de gevonden kwetsbaarheden zijn gerapporteerd aan de fabrikant. Hoewel sommige bevindingen door de fabrikant als *"ignored"* zijn bestempeld (omdat ze moeilijk te misbruiken of structureel lastig te voorkomen zouden zijn), blijven ze cruciaal voor productverbetering. De deurbel is niet direct onveilig, maar zeker niet waterdicht, met andere woorden eerder *voldoende* dan *uitstekend*.

[1] Ook wel *predictive policing* genoemd

[2] Een beveiligingsprobleem dat nog geen oplossing heeft en nog niet bekend is bij de ontwikkelaars

(Chaudhari et al., 2020) benaderen het probleem vanuit het design van een slimme deurbel: een integratie van gezichtsherkenning, stemherkenning en bewegingsdetectie (Raspberry Pi + OpenCV + DSP + Speech-to-Text). Hun focus ligt op functionaliteit en automatische besluitvorming — bij het aanbellen wordt een foto gemaakt die vergeleken wordt met een database; onbekende bezoekers genereren een melding met foto en een OTP naar de eigenaar, en alleen met die OTP kan iemand uiteindelijk worden toegevoegd.

Aspect	Beschrijving
Probleemstelling	Bestaande beveiligingssystemen vertrouwen enkel op gezichtsherkenning; onbekende gezichten worden niet gecontroleerd of gemeld.
Doel van het systeem	Ontwikkelen van een slimme deurbel die gebruikmaakt van IoT, gezichtsherkenning, stemherkenning en bewegingsdetectie om bezoekers automatisch te identificeren.
Werking	Bij het aanbellen activeert de Raspberry Pi een camera; de foto wordt vergeleken met een database van geregistreerde gezichten. Onbekende bezoekers leiden tot een e-mailmelding met foto en OTP naar de eigenaar.
Technologieën	Raspberry Pi, OpenCV (beeldverwerking), DSP (stemherkenning), Speech-to-Text, e-mailserver voor OTP-verzending.

Tabel 2: Overzicht van de belangrijkste elementen uit *Smart Doorbell Security System Using IoT*

Technisch interessant (en in bepaalde gevallen nuttig), maar deze aanpak schuurt meteen met privacyprincipes: gezichts- en spraakdata zijn biometrisch en gevoelig. Het systeem lost één tekort op (valse acceptatie door alleen gezichtsherkenning) door meerdere sensorstromen te combineren, maar vergroot tegelijkertijd de hoeveelheid persoonlijke data die wordt vastgelegd en verwerkt. In termen van privacy-theorie is dat een paradox: meer *zekerheid* vergt vaak meer *data*, wat dus meer *risico*.

(Lalitha et al., 2019) tonen hoe eenvoudig het is om zelf een videodeurbel te bouwen met een Raspberry Pi 3[3], een bewegingssensor en een goedkoop cameraatje. Bij beweging wordt automatisch video opgenomen, naar de cloud gestuurd, en ontvangen de eigenaar en diegene zijn apparaten meldingen (email, SMS). De auteurs presenteren dit als een laagdrempelige manier om je veiligheid te verhogen, maar dat is waar het probleem zit, het wordt extreem gemakkelijk om surveillance te democratiseren.

De paper claimt dat het systeem *ook privacy biedt* omdat beelden alleen naar een geregistreerde gebruiker gemaild worden. Maar in dezelfde adem zeggen ze dat alles naar de cloud gaat, wat toch ook wel weer een aardige paradox (privacy door centralisatie) oplevert. Opnames van gezichten, tijdstippen en bewegingen worden ergens opgeslagen, onder de controle van wie precies? Dat is de kern van de privacy-theorie in applicatie: technisch haalbare functionaliteit betekent niet automatisch verantwoord databeheer.

Daarnaast bevat het werk een praktisch stappenplan — waardevol voor makers — maar precies dat stappenplan verlaagt de drempel om lokale gemeenschappen continu te monitoren. Het normaliseert het idee van permanente observatie en creëert een ecosysteem waar *alle* data onderdeel wordt van een netwerk van observatie.

Technisch gezien zijn slimme deurbellen haalbaar, nuttig en vaak voldoende veilig om alledaags gebruik te overleven — mits correcte implementatie. Tegelijkertijd laten de drie bronnen samen zien dat *privacy* niet één enkel technisch probleem is, maar een samenspel van beleid, ontwerpkeuzes en operationele realiteit:

- Verouderde cryptografie en zwakke authenticatie (MD5, sessies in URL's) maken dat **privacy technisch breekbaar** blijft (zie (Liu, 2021)).
- Het toevoegen van extra sensoren en verwerkingslagen (gezicht, stem, beweging) verhoogt herkenningsbetrouwbaarheid maar ook de hoeveelheid opgeslagen biometrische data — een **kwantitatieve privacykost** (zie (Chaudhari et al., 2020)).
- De laagdrempeligheid van DIY-oplossingen (Raspberry Pi-projecten) democratiseert surveillance en creëert een **sociaal-ethische blinde vlek**: wie heeft toegang tot die beelden en voor hoe lang? (zie (Lalitha et al., 2019)).

sterke certificaatvalidatie, moderne hashing, veilige sessiebeheer, encryptie end-to-end en minimale logging zijn noodzakelijk maar niet voldoende: ontwerpkeuzes en maatschappelijke normen (wat is acceptabel toezicht in een buurt?) bepalen in sterke mate of een systeem *privacyvriendelijk* genoemd mag worden.

4.3 Maatschappelijke en ethische implicaties

(Selinger & Durant, 2022) gebruiken Amazon's *Ring-ecosysteem*[4] als voorbeeld van hoe consumententechnologie ons sociale leven langzaam maar zeker kan veranderen. Vanuit Amazon is het een belofte van veiligheid, maar langzamerhand leidt dit tot een samenleving waarin iedereen elkaar in de gaten houdt. "*Amazon drafts social media content and press statements, and provides templates, all designed to help the police [...] make persuasive requests for surveillance data.*" (Selinger and Durant, 2022, p. 98) Hun conclusie is duidelijk: Ring is geen neutraal hulpmiddel dat je beter kunt reguleren, maar dat het politieke technologie is en Amazon heeft er bewust voor gekozen om de grenzen van privacy op te rekken. Bewaken wordt gepresenteerd als zorgzaamheid, en dataverzameling als vriendelijkheid onder buren. Ondertussen verdwijnt de grens tussen bedrijf en staat, en verdwijnt privacy langzaam maar zeker naar de achtergrond.

Het argument leunt op drie belangrijke ideeën:

- **Langdon Winner** - sommige technologieën zijn van zichzelf politiek; ze leggen machtsverhoudingen vast in hoe ze werken.
- **Alan Dafoe** - technologie stuurt de wereld niet met zekerheid, maar wél met grote waarschijnlijkheid; ze beïnvloedt de richting waarin dingen gaan.
- **De glijdende helling** - als bepaalde voorwaarden eenmaal aanwezig zijn, versterkt surveillance zichzelf; het stopt niet meer.

Selinger and Durant laten zien hoe al deze problemen elkaar versterken. Bedrijfswinsten, angst voor criminaliteit, slimme marketing ("voel je veilig, wees een goede buur") en etnische vooroordelen werken allemaal samen in hetzelfde systeem. Samen vormen ze een vicieuze cirkel die het steeds moeilijker maakt om de uitbreiding van surveillance tegen te houden.

(Kelly, 2023) voegt hieraan toe dat de marketing van Ring-deurbellen het probleem versterkt. De reclamecampagnes wekken de indruk dat veiligheid alleen bereikbaar is als je je huis volhangt met (Ring-)camera's. Daarbij worden er subtiele, en soms expliciete, vergelijkingen gemaakt tussen een gewone consument met een videodeurbellen en een professioneel beveiligingsbedrijf. Uit onderzoek van Kelly blijkt bovendien dat het gemak waarmee het Ring-ecosysteem werkt,

[3] Een minicomputer van +/- €40,-

[4] videodeurbellen's, de Neighbors-app en samenwerkingen met de politie

Probleem	Beschrijving
Centralisatie	Amazon verzamelt alle data en beslist wat ermee gebeurt - bedrijfsbelangen en staatsbelangen vloeien samen.
Uitsluiting / "Wie hoort hier?"	Bewaking stimuleert etnische en sociale profilering: wie "past" er wel of niet in de buurt?
Schijninstemming	Mensen lijken toestemming te geven, maar door machtsverschillen en sociale druk is die instemming leeg.
RoboCop-effect	De politie krijgt toegang tot beelden van burgers, waardoor een privaat bewakingssysteem ontstaat.
Vervaging tussen bedrijf en politie	Amazon levert kant-en-klare PR-teksten aan de politie - ze schrijven feitelijk mee aan publieke communicatie.
Technologische laksheid	Onduidelijke regels en weinig toezicht zorgen ervoor dat misbruik makkelijk blijft gebeuren.
Panopticon-effect	Goedkope camera's overal maken het normaal om buren in de gaten te houden en elkaar te corrigeren.

Tabel 3: Overzicht van de zeven sociale problemen rond Amazon Ring volgens Selinger and Durant

met camera's, bewegingssensoren, alarmen en andere slimme snufjes, een belangrijke verkooptroef is. Alles is eenvoudig te koppelen, waardoor het bijna moeiteloos lijkt om je eigen kleine surveillancesysteem op te zetten.
Uiteindelijk draait het Amazon natuurlijk niet om de veiligheid van gebruikers; het gaat om de verkoop van Ring-producten. Mensen eerst bang maken en vervolgens de "oplossing" aanbieden is een effectief commercieel model. Daarnaast promoot Amazon de *Ring's Neighbors App* - een buurtapp die vergelijkbaar werkt met WhatsApp-buurtpreventiegroepen. Uit eerder onderzoek blijkt echter dat dit soort apps "*[will] provoke increased feelings of anxiety and interpersonal surveillance*" (Wang et al., 2018, p. 1) Met andere woorden: mensen voelen zich niet per se veiliger, maar juist meer bekeken.
Opvallend genoeg is er nog maar weinig onderzoek gedaan naar de ervaringen van mensen die daadwerkelijk een Ring-deurbel gebruiken - en nog minder naar mensen die dat bewust níet doen. Dat zorgt voor een scheef beeld, waar Amazon handig op inspeelt in haar marketing. Slimme huisapparaten zoals Ring en Alexa hebben miljoenen mensen ertoe gebracht om vrijwillig surveillancesystemen in hun eigen huis te installeren. Dat levert bedrijven gigantische hoeveelheden data op, maar brengt ook risico's met zich mee: ongelijkheid, etnische profilering en verlies van privacy - vaak juist voor mensen die de technologie niet eens zelf hebben gekocht. Hoewel publieke druk bedrijven soms dwingt tot aanpassingen, blijft de balans tussen gemak en controle wankel.
Als dit doorgaat, leidt het tot:

- Surveillance als normaal onderdeel van huis en buurt.
- Meer macht voor de politie, via prive datastromen.
- Grotere ongelijkheid, omdat kwetsbare groepen vaker worden bekeken of verdacht.
- Minder democratische controle, want niemand houdt toezicht op wat er precies gebeurt.

Het eindoordeel is nogal kritisch. Amazon Ring is een voorbeeld van een technologie die niet te veranderen is. De problemen zitten ingebakken in hoe het werkt en in de logica eromheen. Volgens (Selinger & Durant, 2022) helpt geen privacyinstelling of toestemmingsformulier meer. Sommige technologieën, zeggen ze, zouden gewoon niet moeten bestaan.

4.4 Gebruikerservaring / Gedrag

(Moh et al., 2023) heeft een onderzoek gedaan naar ongeautoriseerd gebruik van smart home devices. Dit gebeurde via twee enquêtes uitgevoerd in de Verenigde Staten. De eerste enquête was open en bedoeld om een breed beeld te krijgen van soorten misbruik en persoonlijke ervaringen met slimme apparaten. Deelnemers kregen open vragen over situaties waarin apparaten onverwacht gedrag vertoonden, iemand anders hun apparaat gebruikte, of zij zelf dat bij een ander deden.

De tweede enquête bestond uit gesloten meerkeuzevragen om te meten hoe vaak de misbruikscenario's uit de eerste enquête voorkwamen. Deelnemers gaven aan of zij in de afgelopen vijf jaar zo'n situatie hadden meegemaakt of zelf hadden veroorzaakt. Bij sommige scenario's volgden extra vragen over toestemming (expliciet, impliciet of geen) en apparaattypes.

Voor dit onderzoek is alleen gekeken naar het apparaattype "smart cameras". Moh et al. onderzochten tien verschillende categorieën, maar slechts drie waren relevant: Monitor activities, Data leakage en Trigger unwanted behavior. Deze categorieën zijn samengevat in Tabel 4.

Expliciet	Impliciet	Geen toestemming
11 + 0 + 0 = 11	11 + 0 + 4 = 15	5 + 2 + 5 = 12
Expliciet	**Impliciet**	**Geen toestemming**
10 + 1 + 0 = 11	2 + 1 + 4 = 7	1 + 0 + 2 = 3

Tabel 4: Aantal mensen die zijn of hebben gemonitord op basis van toestemmingstype (Moh et al., 2023)

(Tabassum & Lipford, 2023) onderzocht hoe mensen hun videodeurbel gebruiken. Zelfs als gebruikers de mogelijkheid hebben privacyinstellingen aan te zetten, blijkt dit vaak niet te gebeuren. De meeste mensen geven meer om functionaliteit dan om privacy. Gemak wint vrijwel altijd van voorzichtigheid.

Wanneer een videodeurbel een persoon detecteert, krijgt de eigenaar direct een melding. Velen vonden dit handig, maar na verloop van tijd begonnen de meldingen te irriteren. Deelnemers wilden ze tijdelijk uitschakelen, bijvoorbeeld 's nachts of tijdens werkuren. Anderen vroegen om "slimmere" meldingen - alleen bij pakketbezorgers of onbekende gezichten. Sommigen wilden meldingen volledig uitzetten. Een enkeling stelde zelfs voor dat het systeem geluiden zoals geweerschoten zou kunnen herkennen.

Bijna niemand realiseerde zich dat beelden in de cloud veel langer bewaard blijven dan verwacht. Vrijwel iedereen had een abonnement op de cloudservice van de fabrikant, waardoor data standaard werd opgeslagen. Slechts twee van de negentien deelnemers verwijderden regelmatig data uit privacyoverwegingen. De rest dacht dat dit weinig zin had, omdat bedrijven "alles bewaren". Zoals één deelnemer zei: "*the problem is that they do keep your recordings, and there are people accessing them regardless of what they tell you*" (Tabassum and Lipford, 2023, p. 576).

Bij het filmen zelf vond bijna iedereen het normaal dat de deurbel de straat filmt. Pas bij doorvragen beseften sommigen dat ook gesprekken of buren werden opgenomen. Nieuwe gebruikers wilden het gezichtsveld beperken of de opname tijdelijk uitzetten, maar ervaren gebruikers deden dat zelden.

Het delen van beelden werd gezien als vanzelfsprekend. Bij verdachte situaties wilden mensen kunnen delen met buren, politie

of sociale media. Toch waren er zorgen over wat er daarna met de beelden gebeurt, en wie de eigenaar is.

Bij slimme sloten gebruikten veel deelnemers logboeken en meldingen niet alleen voor zichzelf, maar ook om anderen te controleren. Ouders volgden hun kinderen, verhuurders hun gasten. Sommigen wilden de logs kunnen filteren op persoon of tijdstip, maar dat bleek niet mogelijk.

Toegang delen met anderen was lastig. De instellingen waren onduidelijk, waardoor sommigen hun hele account deelden "omdat dat makkelijker is". Anderen wilden tijdelijke toegang, maar vonden de interface te ingewikkeld.

Bijna niemand las de helpteksten. Mensen vertrouwden op grote merken en gingen ervan uit dat die het wel goed doen. Echte kennis over wat er met hun data gebeurt ontbrak volledig.

Uiteindelijk beheren zowel nieuwe als ervaren gebruikers hun privacy nauwelijks actief. Nieuwe gebruikers vragen zich nog af hoe iets werkt, terwijl eigenaars het allang geaccepteerd hebben. De technologie wint, en privacy blijft iets wat pas belangrijk lijkt als het te laat is.

5 Conclusie

Uit dit onderzoek blijkt dat slimme deurbellen, hoewel ontworpen vanuit een gevoel van veiligheid en gemak, verschuivingen veroorzaken in hoe we privacy beschermen. Binnen het kader van **contextuele integriteit** van Nissenbaum wordt duidelijk dat de oorspronkelijke informatiestromen worden doorbroken. Waar ooit een publieke anonieme omgeving was, worden nu camera's aan gevels gehangen en langzaam een semi-publiek surveillancelandschap gecreëerd, waarin buren, voorbijgangers en pakketbezorgers (ongewild) onderdeel worden van iemands persoonlijke drang om zich veilig te voelen.

De literatuur laat zien dat deze technologie niet slechts een technisch hulpmiddel is, maar een sociaal-politiek systeem in miniatuur. Amazon's Ring, en vergelijkbare apparaten, vervagen de grenzen tussen particulier en publiek, tussen bedrijf en politie. Dit leidt tot structurele verschuivingen in macht en vertrouwen — met als ironische uitkomst dat het gevoel van veiligheid vooral groeit bij de eigenaar van de camera, terwijl de privacy van de rest juist afbrokkelt.

Tegelijkertijd blijkt dat gebruikers zelf nauwelijks nadenken over die bredere gevolgen. Privacy-instellingen worden zelden aangepast, beelden worden automatisch opgeslagen, en het gemak van de technologie wint steevast van ethische terughoudendheid. Veiligheid en privacy staan dus niet los van elkaar, maar zijn twee zijden van hetzelfde muntstuk.

Zodra technologie buiten haar beoogde context treedt — van huisbeveiliging naar buurtbewaking — verschuift de balans onherroepelijk. De slimme deurbel maakt zichtbaar hoe dun de grens is tussen bescherming en controle. In termen van contextuele integriteit is het duidelijk: niet de intentie van veiligheid, maar de context van gebruik bepaalt of privacy behouden blijft. En precies die context is bij slimme deurbellen structureel uit balans geraakt.

References

Chaudhari, U., Gilbile, S., Bhosale, G., Chavan, N., & Wakhare, P. (2020). Smart doorbell security system using iot. *International Conference on Sciences and Technology*, (4228).

Kelly, K. (2023). The ring video doorbell and the entry of amazon into the smart home: Implications for consumer-initiated surveillance. *Journal of Consumer Policy*, *46*(1), 95–104.

Lalitha, R., Kavitha, K., Rao, N., Mounika, G. R., & Sandhya, V. (2019). Smart surveillance with smart doorbell. *Int. J. Innovative Technol. Explor. Eng.(IJITEE)*, *8*(8), 1841.

Liu, X. (2021). Ethical hacking of a smart video doorbell.

Moh, P., Datta, P., Warford, N., Bates, A., Malkin, N., & Mazurek, M. L. (2023). Characterizing everyday misuse of smart home devices. *2023 IEEE Symposium on Security and Privacy (SP)*, 2835–2849.

Nissenbaum, H. (2009). Privacy in context: Technology, policy, and the integrity of social life. In *Privacy in context*. Stanford University Press.

Selinger, E., & Durant, D. (2022). Amazon's ring: Surveillance as a slippery slope service. *Science as culture*, *31*(1), 92–106.

Shaffer, G. (2021). Applying a contextual integrity framework to privacy policies for smart technologies. *Journal of Information Policy*, *11*, 243–247.

Tabassum, M., & Lipford, H. (2023). Exploring privacy implications of awareness and control mechanisms in smart home devices. *Proceedings on Privacy Enhancing Technologies*.

Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472–480.

Wang, Y., Pridmore, J., & Mols, A. (2018). Keeping an eye on the neighbours: Police, citizens, and communication within mobile neighbourhood crime prevention groups. *The Police Journal*, *online first*. https://doi.org/10.1177/0032258X18768397