De wereld buiten je voordeur

Contextual integrity bij slimme deurbellen

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

1 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 contextual integrity 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.

1.1 Theoretisch kader

(Nissenbaum, 2009) Schreef al over een door haar ontwikkeld privacy theorie: **Contextual integrity**. 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.

1.2 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.

2 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 (2009) een theoretisch fundament op het gebied van privacy en contextual integrity. Artikelen van Shaffer (2021) en Tabassum Lipford (2023) bouwen daarop voort met recente analyses van smart home-privacy en gebruikerscontrole, gepubliceerd in peer-reviewed journals.

Daarnaast bieden studies van Liu (2021), Lalitha et al. (2019) en Chaudhari et al. (2020) een technisch perspectief op slimme deurbellen, waarbij veiligheid en functionaliteit empirisch worden onderzocht. Tot slot leveren Selinger Durant (2022) en Kelly (2023) kritische beschouwingen over Amazon's Ring en de maatschappelijke gevolgen van consumentgestuurde surveillance. Samen bieden deze bronnen een goed gebalanceerde mix van theoretische, technische en ethische invalshoeken, afkomstig uit betrouwbare en actuele academische contexten.

3 Beschouwing van literatuur

3.1

(Moh et al., 2023) heeft een onderzoek gedaan naar ongeautoriseerd gebruik van smart home devices. Dit is gedaan door middel 2 enquêtes die zijn uitgevoerd in de Verengde Staten. Deze eerste, open enquête was 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 gebruikte gesloten meerkeuzevragen om te meten hoe vaak de misbruikscenario's uit Survey 1 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.

Aangezien niet alle gevonden data relevant is voor dit onderzoek (omdat het apparaat type, of het misbruik niet relevant is) wordt er alleen gekeken naar het apparaattype "smart cameras" gedeelte. Er wordt in het onderzoek van Moh et al. naar 10 verschillende categoriën gekeken, maar 3 van die categoriën zijn voor dit onderzoek daadwerkelijk nuttig, de rest is dus buiten beschouwing gelaten. In Tabel 1 is de opsomming van de 3 categorieën die wél nuttig waren. Deze categorieén zijn: Monitor activities, data leakage trigger unwanted behavior (van links naar rechts respectievelijk).

Zijn gemonitord:		
Expliciet	**Implcitiet**	**Geen toestemming**
11 + 0 + 0 = 11	11 + 0 + 4 = 15	5 + 2 + 5 = 12

Hebben gemonitord:

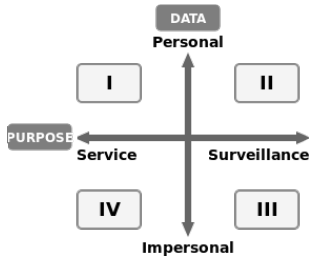
Expliciet	**Implcitiet**	**Geen toestemming**
10 + 1 + 0 = 11	2 + 1 + 4 = 7	1 + 0 + 2 = 3

Tabel 1: Aantal mensen die zijn gemonitord of hebben gemonitord op basis van toestemmingstype (Moh et al., 2023)

3.2

(Van Zoonen, 2016) stelt dat data in een privacy framework (Figuur 1) opgedeeld kan worden. Deze is opgedeeld in 2 assen, de y-as geeft aan of data wel/niet persoonlijk is, de x-as geeft aan of data gebruikt wordt voor helpen of monitoren.

In het tweede kwadrant (**II**) gaat over het verzamelen van data om vervolgens te gebruiken voor monitoren. Dit gaat over persoonlijke data die de overheid verzamelt om mensen in de gaten te houden (denk aan politiedata, of beelden van beveiligingscamera's). Het gaat dus om zeer persoonlijke en gevoelige informatie, en mensen ervaren dat ook zo.



Figuur 1: Privacy framework (nagemaakt van Van Zoonen, 2016)

Precies daardoor ligt dit onderwerp onder een vergrootglas. Er is veel kritiek op hoe zulke data worden gebruikt voor toezicht en controle. Bijvoorbeeld: de burgemeester van Nice kreeg in 2008 een "Big Brother Award" omdat hij de stad vol hing met camera's. Dresden kreeg diezelfde prijs in 2012 voor het volgen van mobiele telefoons tijdens een demonstratie.

Echter zit hier ook een keerpunt aan, het ligt namelijk aan de huidige tijd en situatie of mensen het een probleem vinden om gemonitord te worden. Zo werdt 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 worden gebruikt om gedrag of situaties te controleren. Denk aan verkeersstromen of drukte op stations of evenementen. Op het eerste gezicht lijkt dat onschuldig, want het gaat niet om individuen, maar om groepen, patronen, cijfers.

Steden gebruiken zulke "anonieme" data vaak om beleid te maken. Rotterdam heeft bijvoorbeeld een systeem waarin allerlei data worden samengevoegd (van politiedata tot economische cijfers) om te zien waar problemen dreigen te ontstaan. Zo kan men "risicowijken" aanwijzen of voorspellen waar criminaliteit waarschijnlijk zal oplaaien[1].

Maar ook hier zit een gevaar, want hoe meer je die datasets koppelt, hoe makkelijker het wordt om tóch individuele mensen te herkennen, dan verandert zogenaamd anonieme data ineens in persoonlijke data. Daardoor ontstaat wantrouwen wat kan leiden burgers en organisaties vrezen dat zulke systemen vooroordelen versterken of leiden tot discriminerende controle, zoals in de VS al vaak is gebeurd.

3.3

(Shaffer, 2021) In augustus 2019 sloot Ring een samenwerking met de LBPD[2], waarmee de politie via de app *Neighbors* toegang kreeg tot videobeelden van Ring-deurbellen. Bewoners kunnen via deze app beelden delen van verdachte activiteiten in hun buurt. Officieel is dat volledig vrijwillig, maar in de praktijk voelt het voor velen

[1] Ookwel predictive policing genoemd
[2] Long Beach Police Department

als een sluiproute naar een samenleving waarin iedereen elkaar in de gaten houdt.

De reacties op deze samenwerking zijn gemengd. Sommigen zien het als een logische stap in het bestrijden van criminaliteit, want het is niet heel anders dan het opvragen van beelden bij winkels of bedrijven. Anderen ervaren het juist als een zorgelijke ontwikkeling, als een vorm van burgerlijke surveillance waarbij politie en een (groot) technologiebedrijf samen steeds dieper doordringen in de privésfeer.

Wat het ongemak versterkt, is dat niet alleen de politie, maar ook Amazon (het moederbedrijf van Ring) toegang heeft tot deze beelden. Veel bewoners gaven aan dat ze de politie op zich vertrouwen, maar Amazon veel minder. "Wat doen ze met die data?" is een veelgehoorde vraag. De vrees is dat commerciële belangen en veiligheidsdoelen door elkaar gaan lopen.

Uiteindelijk draait de discussie niet om de camera's zelf, maar om macht en controle: wie kijkt er mee, en wie bepaalt wat er met die beelden gebeurt?

3.4

(Liu, 2021)

Na uitvoerig *threat modeling* en *penetration testing* blijkt dat de beveiliging van de onderzochte smart video deurbel over het algemeen degelijk is, maar beslist niet foutloos. Er zijn geen directe, kritieke kwetsbaarheden gevonden, maar wel meerdere zwakke plekken die in de praktijk kunnen worden misbruikt. De belangrijkste aandachtspunten liggen bij de Android-app, de accountbeveiliging en de draadloze communicatie.

Categorie	Belangrijkste bevindingen en verbeterpunten
Android-applicatie	Gevoelige data kan uitlekken bij een geroot toestel 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) en logging is minimaal. 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 is voldoende streng.
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 2: Overzicht van de belangrijkste beveiligingsbevindingen van de smart video deurbel.

Liu benadrukt dat het uitvoeren van beveiligingstesten op IoT-apparaten essentieel is, omdat veel van deze producten nog altijd basisfouten bevatten in encryptie, databeheer en netwerkverkeer. Xiaomi staat "ethisch hacken" toe zolang andere gebruikers of servers niet worden geraakt — een voorwaarde die in dit onderzoek strikt is nageleefd. Alle testen zijn uitgevoerd op eigen apparaten en accounts, en de kwetsbaarheden zijn gemeld aan de fabrikant.

Hoewel Xiaomi de bevindingen formeel als *"ignored"* heeft bestempeld (omdat ze moeilijk te misbruiken of structureel lastig te voorkomen zijn), blijven ze relevant voor verdere productverbetering (voor zowel Xiaomi, maar ook voor andere bedrijven die slimme deurbellen produceren). De deurbel is bovendien onbeschadigd gebleven en kan nog steeds gebruikt worden, wat bijdraagt aan de duurzaamheid van het project.

De smart video deurbel is niet direct onveilig, maar zeker niet waterdicht. De combinatie van verouderde cryptografie (MD5), beperkte logging en enkele kwetsbare communicatiemechanismen maakt dat de beveiliging vooral *voldoende* is — niet *uitstekend*. De studie toont aan dat zelfs populaire IoT-producten structureel vatbaar blijven voor datalekken en manipulatie, en dat systematische beveiligingsaudits geen luxe maar noodzaak zijn.

3.5

(Lalitha et al., 2019) Dit onderzoek is eigenlijk een beetje eng. Hoe maak je eenvoudig zelf een videodeurbel om jouw veiligheid(sgevoel) te vergroten. Het is de onderzoekers gelukt om met behulp van een Raspberry Pi 3[3], een bewegingssensor en een goedkoop cameraatje een surveillance systeem te maken. Als er dan beweging wordt gedetecteerd wordt er automatisch een video opgenomen en opgeslagen in de cloud, krijgt de eigenaar van de computer een melding, wordt er een Email gestuurd met de desbetreffende beelden én krijgt de gebruiker nog een SMS'je.

Maar waar de onderzoekers spreken over "veiligheid" en "gemak", lijkt wel heel erg op het idee dat elk huis een klein surveillancesysteem moet worden. Alles (van je voordeur tot je telefoon) is onderdeel van een netwerk dat jou observeert, bewaart, en waarschuwt.

In de paper staat dat het systeem "ook privacy biedt", omdat beelden enkel worden gemaild naar de geregistreerde gebruiker. Echter, tegelijk wordt alles naar de cloud gestuurd (alsof dat geen paradox is). Beelden van gezichten, bewegingen, tijdstippen worden allemaal opgeslagen, ergens, door iets.

Ook bieden ze een stappenplan dat (voor iedereen die kabels kan aansluiten) goed te volgen is en volledig is uitgeschreven. Het wordt dus extreem makkelijk gemaakt om je eigen buurt in de gaten te houden.

3.6

(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 andpress 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

[3] Een minicomputer van +/- €40,-

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

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 vervagen de grenzen tussen bedrijf en staat, en verdwijnt privacy stilletjes 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.

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: Tabel van de zeven sociale problemen

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 als motoren in hetzelfde systeem. Samen vormen ze een vicieuze cirkel die het steeds moeilijker maakt om de uitbreiding van surveillance tegen te houden.
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 and Durant helpt geen privacyinstelling of toestemmingsformulier meer. Sommige technologieën, zeggen ze, zouden gewoon niet moeten bestaan.

3.7

(Kelly, 2023) Waar Kelly vooral kritiek op heeft, is de manier waarop Amazon zijn Ring-deurbellen in de markt zet. 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 heel expliciete, vergelijkingen gemaakt tussen een gewone consument met een deurbelcamera en een professioneel beveiligingsbedrijf.

Uit het onderzoek van Kelly blijkt bovendien dat het gemak waarmee het Ring-ecosysteem werkt — 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.

Maar uiteindelijk draait het Amazon natuurlijk niet om de veiligheid van gebruikers; het gaat om de verkoop van Ring-producten. En er is weinig effectiever dan mensen eerst bang maken en ze vervolgens de "oplossing" aanbieden.

Daar komt nog bij dat Amazon de *Ring's Neighbors App* promoot — 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.

3.8

De paper van (Chaudhari et al., 2020) beschrijft een slim deurbelsysteem gebaseerd op Internet of Things (IoT) technologie. Het doel is om huisbeveiliging te automatiseren met behulp van gezichtsherkenning, stemherkenning en bewegingsdetectie via een Raspberry Pi. Wanneer iemand aanbelt, maakt het systeem automatisch een foto, vergelijkt die met een database van bekende gezichten en beslist of toegang wordt verleend. Onbekende bezoekers krijgen geen toegang, maar er wordt een melding gestuurd naar de eigenaar met een foto en een eenmalige code (OTP). Alleen wanneer de eigenaar de code deelt, wordt de bezoeker toegevoegd aan de toegangsdatabase.

Het systeem combineert beeldverwerking, digitale signaalverwerking en spraak-naar-tekst-herkenning in één geïntegreerd beveiligingsplatform. Daarmee wil het de beperkingen van bestaande enkelvoudige gezichtsherkenningssystemen overwinnen.

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 4: Overzicht van de belangrijkste elementen uit *Smart Doorbell Security System Using IoT*.

3.9

(Tabassum & Lipford, 2023)

Zelfs als gebruikers de kans krijgen om privacyinstellingen aan te zetten, lijkt dat vaak niet gebruikt te worden. De meeste mensen geven volgens de studie meer om functionaliteit dan om privacy. Gemak wint het vrijwel altijd van voorzichtigheid.

Als een videodeurbel een persoon detecteert, krijgt de eigenaar direct een melding. Dat vonden velen handig, maar na verloop van tijd begonnen die 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.

De meeste mensen hadden niet bedacht dat de beelden in de cloud veel langer bewaard blijven dan gehoopt. 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 privacy-overwegingen. De rest dacht dat het toch 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 viel op dat bijna iedereen het normaal vond dat de deurbel de straat filmt. Pas bij doorvragen beseften sommigen dat ook gesprekken of buren werden opgenomen. Novices wilden het gezichtsveld beperken of de opname tijdelijk uitzetten, maar ervaren gebruikers deden dat zelden. Men was er simpelweg aan gewend geraakt.

Het delen van beelden werd gezien als iets vanzelfsprekends. Bij verdachte situaties wilden mensen kunnen delen met buren, politie of sociale media. Toch maakte men zich zorgen over wat er daarna met die beelden gebeurt, en wie eigenlijk 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 bleek lastig. De instellingen waren onduidelijk, waardoor sommigen hun hele account deelden "omdat dat makkelijker is". Anderen wilden juist tijdelijke toegang, maar vonden de interface te ingewikkeld.

Opvallend is dat bijna niemand de helpteksten las. Mensen vertrouwden op grote merken en gingen ervan uit dat die het wel goed doen. Maar echte kennis over wat er met hun data gebeurt, ontbrak volledig.

Uiteindelijk beheren zowel nieuwe als ervaren gebruikers hun privacy nauwelijks actief. Novices 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.

4 Conclusie

Duidelijk antwoord op je onderzoeksvraag. Trek de lijn terug naar contextual integrity: veiligheid en privacy staan niet los van elkaar, maar de balans verschuift zodra technologie te veel buiten de intended context gaat. (max 1 pagina)

References

Chaudhari, U., Gilbile, S., Bhosale, G., Chavan, N., & Wakhare, P. (2020). C. *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