De wereld buiten je voordeur

Contextual integrity bij slimme deurbellen

Matt ter Steege
m.j.ter.steege@students.uu.nl
Universiteit Utrecht, 9932003
Utrecht, Nederland

Comment for editors:

X Titel en eventuele subtitel, opleiding, naam schrijver, studentnummer schrijver.
- Abstract
- 'Inleiding' met kader, probleemstelling, onderzoeksvraag en aankondiging van de structuur van het verslag. Hierin verwerk je ook een stukje achtergrond met een beschrijving van de belangrijke concepten of 'related work'.
- Een 'Methode' met een beschrijving van de werkwijze die je gaat gebruiken om de onderzoeksvraag te beantwoorden.
- Bespreking van de gevonden wetenschappelijke literatuur in een beschouwend geheel die aansluiten bij de onderzoeksvraag.
- Een overkoepelende conclusie vanuit de verkregen inzichten en beantwoord de onderzoeksvraag met deze inzichten

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

Comment for editors:

CHECK: Contextual integrity uitleggen.
CHECK: Benoem hoe dit verschilt van het klassieke idee van privacy (bijv. "control over information").
CHECK: Breng het naar jouw onderwerp: de context van de stoep voor een huis → normaal geen registratie, maar met een deurbelcamera wel. Hierdoor raakt de normale informatiestroom verstoord.

(Nissenbaum, 2009)[1] 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

[1] Editor's note: Moet je nog lezen :(

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

Hier ga je echt de gevonden artikelen samenbrengen in een doorlopend verhaal. Opdelen in subthema's:

- Bewegingsdetectie, cloudopslag, delen met politie.
- Studies over hoe vaak mensen ongewild gefilmd worden; klachten; gevoelens van surveillance.
- Wat bewoners ervaren: afschrikking, bewijs bij criminaliteit. Literatuur die laat zien of dit effect groot/klein is.
- Hoe de informatiestromen door de deurbel afwijken van de 'normale sociale verwachtingen': een toevallige voorbijganger verwacht niet dat zijn route naar de supermarkt opgenomen en bewaard wordt.
- Burenruzies, wantrouwen, normalisering van surveillance in de publieke ruimte.

3.1

Editor's note: Type bron: Kijk naar het gebruik en misbruik van smart home devices.

(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 op pagina 2 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	impliciet	geen toestemming
11 + 0 + 0 = 11	11 + 0 + 4 = 15	5 + 2 + 5 = 12

Hebben gemonitord:

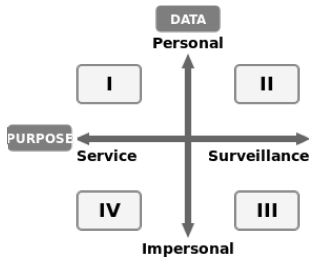
expliciet	impliciet	geen toestemming
10 + 1 + 0 = 11	2 + 1 + 4 = 7	1 + 0 + 2 = 3

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

3.2

Editor's note: Type bron: theoretisch kader dat voorspelt wanneer slimme stadstechnologieën privacyzorgen oproepen.

(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.



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

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.

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, drukte op stations of evenementen, of warmtecamera's die menigten volgen. 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[2].

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.

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

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.

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

[2] Ookwel predictive policing genoemd