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

Characirizing everyday misuse of smarthome devices

-unauthorized use and missuse - unauthorized use means use without explicit permission. (alexa van een vriend vragen iets toe te voegen aan amazon cart <-> sensitive informatie opvragen als eigenaar niet thuis is)

er zijn 10 categorien van unautorized use: - entertainment; muziek, films e.d kijken via persoons account - Monitor activities: videocamera's bekijken zonder weten van gefilmde - Broken device: slopen van apparaat van eigenaar - Dataleakage: iemand krijgt toegang tot je data (payment information etc.) - Modify enviromet: ongevraagd aanpassen van dingen (temperatuur, tv settings, e.d.) - Modify data: liedjes toevoegen aan je playlist, volgorde van foto's aanpassen in digi-lijstje - Delete data: instellingen, presets, foto's e.d. verwijderen - Change settings: wat zou dat betekenen he.. - Trigger unwanted behavior: alarm af laten gaan, alexa triggeren e.d. - Make purchase: heeft een aankoop gedaan zonder vragen via jouw account

Dit is opgedeeld in 2 delen: Meegemaakt en gedaan Als we alleen kijken naar het "smart cameras" gedeelte, want de rest is niet heel relevant voor dit onderzoek. Dan komt de volgende data naar boven:

Zijn (expliciet)	zijn (impliciet)	zijn (geen toestemming)
11+0+0 = 11	11+0+4 = 15	5+2+5 = 12
hebben (expliciet)	hebben (implicient)	hebben (geen toestemming)
10+1+0 = 11	2+1+4 = 7	1+0+2 = 3

Table 1: Aantal mensen die zijn gemonitord of hebben gemonitord

hier kijk ik alleen naar de volgende categorien: Monitor activities, data leakage trigger unwanted behavior

Hier beschouw je de literatuur: niet alleen "wat zegt studie X", maar ook: hoe hangen deze bevindingen samen, waar spreken ze elkaar tegen, en wat valt jou op.

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)

5 Voorbeeldcitatie

Lamport beschreef het gebruik van als documentopmaaksysteem al in de jaren negentig (Tabassum & Lipford, 2023). Ook Knuths werk over blijft invloedrijk. (Chaudhari et al., 2020) blablalbalbalba (Kelly, 2023)

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.

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

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