

Big brother is watching where you are

Een onderzoek naar het bewustzijn van privacy bij Foursquare-gebruikers

Student: Rik van Ooijen

Studentnummer: 3513998

Cursus: Eindwerkstuk

Cursuscode: 200401010

Thema: Sociale en technologische netwerken

Docent: M. van den Boomen

Datum: 22 juni 2012

Inhoudsopgave

Sociale netwerksites	2
Persoonlijke gegevens op sociale netwerksites	2
Privacyvoorwaarden	3
Privacy	4
Informationele privacy	4
Privacy in netwerken	5
Privacy en locaties	6
Foursquare	7
Privacy bij Foursquare	7
Methode	9
Procedure	9
Ontwerp enquête	9
Respondenten	10
Resultaten onderzoek	11
Omgang met persoonlijke gegevens	11
Omgang met privacy-instellingen	12
Soorten check-in locaties	13
Zorgen over openbaring locatiegegevens	14
Effect enquête op bewustzijn privacy	16
Conclusie	18
Discussie	20
Bibliografie	21
Bijlage A: Enquête Foursquare-gebruik	23

Sociale netwerksites

Sociale netwerksites als Facebook en Hyves stellen gebruikers al jaren in staat om interesses en activiteiten te delen met anderen. Gebruikers op dit soort online platformen creëren in feite een representatie van hun identiteit. Sinds kort is het online delen van fysieke locaties omarmd door gebruikers. Zo is het aantal leden van de sociale netwerksite Foursquare, waar het delen van locaties centraal staat, binnen enkele jaren gegroeid naar meer dan tien miljoen gebruikers wereldwijd (Foursquare 2011). Op Foursquare kunnen gebruikers met vrienden delen waar en wanneer ze bijvoorbeeld hebben gegeten, gewerkt of op vakantie zijn.

Persoonlijke gegevens op sociale netwerksites

Tegenwoordig is er op internet sprake van een enorme hoeveelheid persoonlijke gegevens die in databases wereldwijd worden opgeslagen. Wanneer we inchecken met een OV-chipkaart, een camera kopen op een webshop of aanmelden op een forum; al deze gegevens worden op verschillende plekken en in verschillende media opgeslagen. Deze technologische ontwikkelingen hebben ook gevolgen voor wetgevingen. EU-parlementariërs maken zich tegenwoordig sterk voor duidelijke regels op het gebied van datavergaring, zodat gebruikers weten hoe gegevens worden verzameld, geraadpleegd en gebruikt. Er wordt gepleit voor het herzien van de op dit moment gehanteerde EU-gegevensbeschermingsregels, die in 1995 zijn opgesteld (Europa Nu 2012). In dat jaar was minder dan één procent van de Europeanen actief op het internet en was de hoeveelheid opgeslagen persoonlijke data beperkt. Nu een overgroot deel van de bevolking online informatie deelt, blijkt dat deze oude regels niet goed toepasbaar zijn en explicieter gemaakt moeten worden.

Gebruikers maken zich tegenwoordig zorgen over de openbaarheid van de persoonlijke gegevens die ze op sociale netwerksites plaatsen. Een site als Facebook stimuleert het gebruik van echte namen en het uploaden van persoonlijke informatie op de profielpagina, de representatie van de gebruiker. Het gaat hierbij om informatie als de verjaardag, het telefoonnummer en het huisadres, maar ook meer intieme informatie zoals interesses, hobby's en seksuele voorkeur.

Sinds de enorme toename in het gebruik van deze sociale netwerksites zijn de zorgen over privacy een controversieel en vaak bediscussieerd onderwerp. Alleen al op Nederlands meestbezochte nieuwswebsite NU.nl zijn het afgelopen jaar meer dan 80 nieuwsberichten geplaatst die gerelateerd zijn aan privacy op Facebook. Ook Bits Of Freedom, een Nederlandse stichting die het grondrecht op privacy verdedigt, wijst gebruikers op het belang van privacy op deze sociale netwerksites (Bits of Freedom 2012). Dit is niet zo

verwonderlijk aangezien het vergaren van persoonlijke gegevens van gebruikers op een platform als Facebook een cruciaal onderdeel is van het bedrijfsmodel. Facebook gebruikt deze gegevens namelijk om advertenties op een specifieke doelgroep te kunnen richten.

Er is in recent onderzoek aangetoond dat 47 procent van de respondenten zich minder comfortabel voelt over hoe software-ontwikkelaar Google data verzamelt, nadat ze het Google-privacybeleid hebben gelezen (Siegel and Gale 2012). Uit dit onderzoek blijkt tevens dat de begrijpelijkheid van de privacyvoorwaarden van Facebook en Google bijna twee keer lager ligt dan overheidsberichten en creditcard-overeenkomsten.

Privacyvoorwaarden

Hoewel sociale netwerksites in hun beleid vaak stellen zorgzaam te zijn met persoonlijke informatie, is het voor veel gebruikers vaak een omstreden kwestie. Zodra een persoon gebruik wil maken van een sociale netwerksite, dient hij of zij de privacyvoorwaarden van deze site te lezen en te accepteren. Onderzoek toont aan dat privacyvoorwaarden van websites vaak zonder te lezen worden geaccepteerd door gebruikers (McDonald & Cranor 2008). De belangrijkste reden dat gebruikers niet de moeite nemen dit te lezen is de lengte van de documenten. Het lezen van de voorwaarden duurt bij de 75 meest populaire websites gemiddeld 10 minuten (ibid.). Gebruikers van sociale netwerksites accepteren dan wel de privacyvoorwaarden om gebruik te kunnen maken van deze websites, maar het is de vraag of ze zich ervan bewust zijn van hoe er daadwerkelijk met hun data wordt omgegaan.

Privacy

Wanneer we het hebben over ethische kwesties wat betreft persoonlijke informatie spreken we al snel in termen van *privacy*. Er zijn vele definities van privacy en er kan op verschillende manieren naar gekeken worden. Vanuit een juridische invalshoek spreken we over het recht op privacy van de mens. Het recht op privacy is in verschillende landelijke en internationale verdragen vastgelegd. Privacy wordt vaak omschreven als het recht van burgers om de persoonlijke levenssfeer te beschermen. Daarnaast beschrijft De Van Dale privacy als 'de mogelijkheid om in eigen omgeving helemaal zichzelf te zijn'. Een van de eerste werken rondom privacy noemt het 'het recht om alleen gelaten te worden' (Warren & Brandeis 1890). Filosoof Van den Hoven benadrukte al dat er op verschillende manieren kan worden gedacht over wat privacy inhoudt:

'Privacy is construed as a need, a right, a condition, or an aspect of human dignity. Sometimes it is construed as intrinsically valuable; sometimes it is construed as deriving its value from other sources, for example, from the fact that it is conducive to autonomy or freedom' (Van den Hoven 2008, 302)

Dit citaat illustreert dat privacy een begrip is waar mensen op een verschillende manier invulling aan kunnen geven. Het is dus van de interpretatie afhankelijk of privacy iets is waar we allemaal recht op hebben en gebruik van maken, of dat privacy een diepgewortelde behoefte is waar we naar willen of moeten streven. Het is nu van belang om een inzetbare conceptualisatie van privacy in dit onderzoek te hanteren waarin het informationele aspect van privacy naar voren komt.

Informationele privacy

Waar mensen privacy kunnen zien als 'recht om alleen gelaten te worden' kan het ook worden gezien als 'recht om te bepalen welke informatie je onthult aan wie'. In dit laatste geval spreken we over *informationele privacy*. Hierbij gaat het om onthullen van persoonlijke informatie die gerelateerd is aan een persoon, waarmee hij of zij te identificeren is. Het kan hierbij bijvoorbeeld gaan om informatie als een naam, telefoonnummer, profielfoto of locatie. Waar we als individuen wellicht het liefst de controle over onze eigen informatie willen houden, ligt het opslaan of openbaren van deze gegevens vaak niet in onze handen, maar in die van derden, zoals de overheid.

Er is een aantal entiteiten en processen die een rol spelen bij deze informationele privacy. Daniel Solove maakt onderscheid tussen vier processen: *information collection*, *information processing*, *information dissemination* en *invasion* (Solove 2006). Dit houdt in

dat verschillende entiteiten (personen, bedrijven en overheden) informatie kunnen verzamelen, verwerken en verspreiden of dat zij inbreuk kunnen plegen op iemands privacy. Op deze manieren kunnen we begrijpen hoe er met informatie wordt omgegaan, en welke problemen er kunnen ontstaan met betrekking tot de informationele privacy.

Een probleem dat bij privacy komt kijken noemt Van den Hoven de 'integriteit van informatiesferen' (2008, 314). Wanneer medische informatie van personen wordt gebruikt om ziektes te genezen, zijn daar over het algemeen geen problemen mee. Deze informatie wordt dan alleen gebruikt in de medische sfeer. Wanneer de informatie echter zou worden gebruikt om de hoogte van de zorgverzekering van iemand te bepalen, is er waarschijnlijk hevig verzet. De informatie wordt in dit geval verscheept naar een andere context wat negatieve gevolgen met zich mee kan brengen. Onder privacy wordt dus ook verstaan dat informatie van en over mensen niet voor andere doeleinden en in andere sferen gebruikt wordt dan met de intentie die men had.

Privacy in netwerken

Privacy heeft te maken met het willen delen van persoonlijke informatie met anderen. Het is de vraag wanneer men wel of niet iets wil delen en wanneer ze wel of niet bepaalde zaken als privé beschouwen of niet. Vanuit de sociologie valt hier een verklaring voor te vinden. Socioloog Erving Goffman stelt dat de rol of karakter die een persoon aanneemt afhankelijk is van de situatie waarin hij/zij zich bevindt en welke andere personen hierin aanwezig zijn:

'[...] we project different personas to different people in different situations. For example, a doctor might present a professional persona while working in the hospital, but might be far more casual and open with close friends and family' (Iachello & Hong 2007, 11)

Deze theorie is weliswaar bijna een halve eeuw geleden geïntroduceerd, maar is nog steeds nuttig voor het begrijpen van de manier waarop mensen zichzelf zowel offline als online presenteren. Wanneer iemand bijvoorbeeld een vulgaire grap heeft gelezen, zal hij/zij dit normaal gesproken eerder vertellen aan vrienden dan aan zijn of haar schoonouders. Aangezien deze twee groepen apart te benaderen zijn, kan de grap aan de ene groep worden verteld en aan de andere groep niet. Dit houdt in dat deze persoon bepaalde kenmerken privé wil houden voor een groep en openbaar wil maken voor een andere groep. Personen gedragen zich dus anders bij verschillende personen in verschillende situaties. Dit wordt problematisch wanneer iemand alleen de mogelijkheid heeft om een boodschap over te brengen naar al deze mensen, of naar niemand. De

persoon kan in dit geval informatie delen met een grote groep, maar wanneer hij/zij niet wil dat een deel van deze groep deze informatie te weten kan komen, kan de informatie niet worden gedeeld.

Hierbij valt een onderscheid te maken tussen online en offline sociale netwerken. Offline sociale netwerken bestaan uit zowel oppervlakkige als diepgaande relaties met anderen, waarbij deze relaties kunnen variëren. Bij online sociale netwerken is meer sprake van gecategoriseerde relaties (Gross & Acquisti 2005). Dit houdt in dat het delen van bepaalde informatie gericht aan bepaalde personen problematisch kan zijn in online sociale netwerken.

Een ander verschil tussen online en offline netwerken is dat er bij online netwerken vaak sprake is van een eigenaar. Zo is Facebook niet alleen een sociaal netwerksite maar ook een beursgenoteerd bedrijf met commerciële belangen. Eigenaren van sociale netwerksites hebben er vaak belang bij dat gebruikers persoonlijke informatie plaatsen, simpelweg omdat het veel waard is. De eigenaren van deze platformen zijn belangrijke actoren bij de bescherming van persoonlijke data.

Privacy en locaties

Door een groei in het gebruik van mobiele smartphones en 3G-netwerken zijn steeds meer mensen in staat om altijd en overal online te zijn. Dit houdt in dat sociale media vaker worden gebruikt op een andere plek dan alleen thuis op de PC. Dit heeft geresulteerd in mobiele applicaties die dynamische gebruikers in staat stellen om locaties te delen. De grootste 'locatie-sharing site' is Foursquare. Hierbij checken gebruikers in op plaatsen met behulp van een mobiel apparaat om dit vervolgens te delen met Foursquare-vrienden.

Er is al veel gesproken over welke informatie gebruikers met welke personen delen en welke informatie niet. Er is minder bekend hoe gebruikers privacy ervaren als het gaat om het delen van locatiegebonden gegevens. De vraag rijst of gebruikers van sociale netwerksites zich anders gedragen op deze platformen wanneer ze deze gegevens plaatsen, en in welke gevallen ze deze informatie als intiem en privé ervaren.

Foursquare

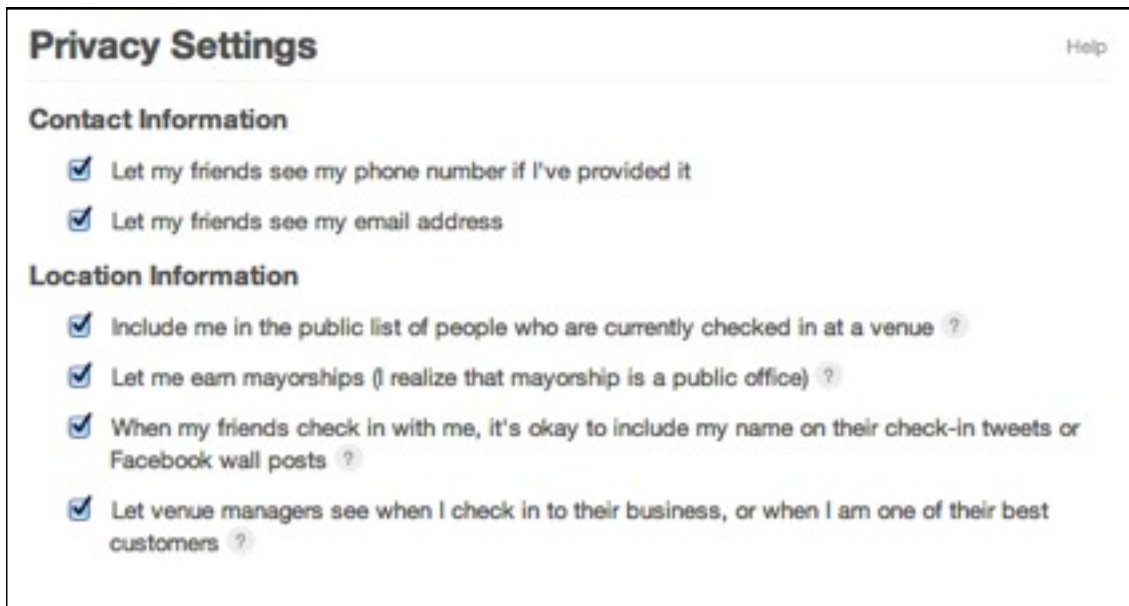
Foursquare kan naast een sociale netwerksite ook als spel worden beschouwd. Wanneer een gebruiker incheckt op een plaats verdient hij/zij hier punten mee. Daarnaast kunnen er *badges* worden verdiend. Wanneer iemand bijvoorbeeld tien verschillende keren heeft ingecheckt is de 'Beginner Badge' verdiend. En wanneer een gebruiker bij 20 verschillende pizzatenten is ingecheckt is hij/zij de eigenaar van een 'Pizzaiolo Badge'. Ook kan een gebruiker een *mayorship* verdienen. Wanneer iemand op een bepaalde locatie de afgelopen 60 dagen de meeste dagen heeft ingecheckt is hij/zij de *mayor* van deze locatie. Sommige bedrijven geven korting aan de Foursquare-mayor van hun bedrijf (Lindqvist et al. 2011). Uit onderzoek blijkt dat het verdienen van deze punten, badges en mayors en de competitie met vrienden een belangrijke drijfveer is voor gebruikers om Foursquare te gebruiken en daarbij hun locatie prijs te geven (ibid.).

Privacy bij Foursquare

Op de website van Foursquare is op verschillende plekken informatie te vinden over privacy op het platform. Er is een informatiepagina over privacy om gebruikers op de hoogte te brengen, een lijst van veelgestelde vragen omtrent privacy en een 'Privacy Grid', waarin wordt aangegeven wat de standaard privacy-instellingen van gebruikers zijn en hoe ze hierin individuele wijzigingen kunnen aanbrengen.

Gebruikers hebben de mogelijkheid om hun persoonlijke gegevens op het platform in te voeren. Er kan onder andere een naam, profielfoto, telefoonnummer, e-mailadres en korte omschrijving worden ingevoerd. Deze informatie is met de standaardinstellingen zichtbaar voor andere Foursquare-gebruikers. Daarnaast is er de mogelijkheid om de 'Privacy Settings' op de site te wijzigen. De gebruiker kan hierbij kiezen om het telefoonnummer of e-mailadres te verbergen voor Foursquare-vrienden. Het betreft hier persoonlijke gegevens van de gebruiker. Ook kan een gebruiker er voor kiezen om de openbaarheid van geplaatste check-ins in te perken. Zo kan er voor worden gekozen om je naam niet weer te geven voor anderen in een publieke lijst van gebruikers die op een bepaald moment op een bepaalde locatie is ingecheckt. Een screenshot van de instellingen is opgenomen in afbeelding 1. Bij het aanmaken van een nieuw account op Foursquare zijn al deze opties automatisch aangevinkt. De gegevens van een gebruiker zijn in dat geval zo openbaar als mogelijk met deze instellingen.

Afbeelding 1: screenshot van aanpasbare privacy-instellingen op Foursquare



Eerder onderzoek heeft uitgewezen dat Foursquare onder andere wordt gebruikt voor plezier, exploratie en coördinatie met vrienden (Lindqvist et al. 2011). Maar er is niet uitgebreid onderzocht hoe Foursquare-gebruikers omgaan met hun privacy.

Het doel van dit explorerende onderzoek is om te bepalen of gebruikers zich bewust zijn van hun privacy op het platform. Op welke manier schermen gebruikers hun informatie af voor anderen? En is voor gebruikers van belang welke individuen of instanties inzicht hebben in hun gegevens? Deze vragen staan centraal in dit onderzoek en zijn gesteld om meer inzicht te krijgen in het bewustzijn van gebruikers wat betreft de privacy van locatiegebonden informatie. De kennis hierover kan worden ingezet om overheden en site-eigenaren te ondersteunen bij het opstellen van wetgeving en regelgeving omtrent de privacyvoorwaarden om burgers te informeren en beschermen. Daarnaast zou dit onderzoek bij kunnen dragen aan een betere informatievoorziening voor gebruikers op sociale netwerksites wat betreft de verzameling, verwerking en verspreiding van hun persoonlijke (locatie)gegevens.

Methode

Om inzicht te krijgen in de manier waarop Foursquare-gebruikers hun privacy op het platform ervaren heb ik een kleinschalig explorerend onderzoek gedaan. Met behulp van een enquête is getracht antwoord te verkrijgen op de volgende vragen:

- Hoe gaan Foursquare-gebruikers om met de privacy-instellingen op het platform?
- Ervaren gebruikers een andere mate van zorgwekkendheid bij het delen van locaties behorende bij de woon- en werkomgeving en bij de vrijetijdsbesteding?
- Ervaren gebruikers een andere mate van zorgwekkendheid bij verschillende personen en instanties die de locaties van de gebruikers weten?

Procedure

Ik heb in mei 2012 via verschillende kanalen potentiële respondenten benaderd. Met een bericht op mijn persoonlijke Facebook-pagina heb ik mensen die Foursquare gebruiken opgeroepen de enquête in te vullen. Hierbij is een hyperlink geplaatst die verwijst naar de online enquête. Daarnaast heb ik contact opgenomen met enkele kennissen waarvan ik weet dat ze Foursquare regelmatig gebruiken. Als laatst heb ik een oproep gedaan door een bericht te plaatsen op het Twitter-account van De Wijkwebsite. Op deze website, mede door mij opgericht, zijn activiteiten en gebeurtenissen in de omgeving van Nijmegen op een kaart zichtbaar voor inwoners. Gebruikers kunnen zelf berichten op de website plaatsen en hieraan een geografische locatie koppelen. Aangezien deze gebruikers van De Wijkwebsite bedreven zijn in het online delen van locaties verwacht ik dat er zich onder deze personen ook gebruikers van Foursquare bevinden. Het Twitter-account heeft op moment van schrijven ongeveer 500 volgers en is daarmee een medium waarop ik een oproep doe aan een groter publiek.

Ontwerp enquête

De enquête bestaat uit 17 vragen waarvan 16 gesloten en één open. Inhoudelijk bestaat de vragenlijst uit vier delen. Het eerste deel bevraagt persoonlijke gegevens door middel van meerkeuzevragen. Het gaat hierbij om geslacht, leeftijd en opleiding, alsook of de respondent op andere sociale netwerksites actief is en hoe vaak hij of zij per maand incheckt op Foursquare.

Het tweede deel focust op de privacy-instellingen van de gebruikers en welke persoonlijke informatie ze vrijgeven of achterhouden. Er is gevraagd of de gebruiker de privacy-instellingen heeft bekeken en gewijzigd en, zo ja, wat hij/zij precies heeft gewijzigd. De respondent kan hierop antwoord geven door middel van een checklist.

Vervolgens geeft de respondent antwoord op de vraag of hij/zij de volledige voornaam en achternaam, telefoonnummer, korte omschrijving en standaardlocatie in het profiel heeft ingevoerd. De respondent kan hier bij meerdere meerkeuzevragen aangeven of hij/zij deze informatie bewust incorrect of onvolledig heeft ingevoerd.

Het derde deel meet de mate waarin gebruikers het zorgwekkend vinden wanneer verschillende personen en instanties de locatie van de gebruiker weten. Deze mate van zorgwekkendheid kan de respondent per type persoon of instantie aangeven op een 5-punts Likertschaal. Er is hierbij een tweedeling gemaakt tussen locaties in woon- en werkomgeving en locaties aangaande vrijetijdsbesteding. Hiermee is achterhaald in welke setting gebruikers meer zorgen hebben over het openbaren van hun locatie. Ook is gevraagd op welke plekken respondenten inchecken om te meten of FS-gebruikers ook daadwerkelijk in verschillende mate locaties delen behorende bij de twee bovengenoemde settings.

Als laatste is respondenten gevraagd of ze zich na het invullen van de voorgaande vragen meer bewust zijn van de mogelijkheden tot het beschermen van de persoonsgegevens en locatiegegevens op Foursquare. Vervolgens is een open vraag gesteld of de respondenten - na het invullen van de enquête - meer aandacht zullen besteden aan het beschermen van hun gegevens. Met deze vragen is gemeten of er een lerend effect bij de respondenten is ontstaan bij het invullen van de enquête.

Respondenten

Er zijn 16 enquêtes ingevuld, waarvan er één is uitgesloten wegens het onvolledig beantwoorden van enkele gesloten vragen. Onder de respondenten waren veertien mannen en één vrouw, respectievelijk 93% en 7% van de gehele groep. Hiervan was 60% tussen de 18 en 35 jaar oud, 33% tussen de 36 en 55 jaar en een enkeling ouder dan 65 jaar. Zie 5.1 voor meer informatie over de onderzoeksgroep.

Resultaten onderzoek

Er hebben vijftien respondenten deelgenomen aan dit onderzoek. Uit de resultaten van de enquête blijkt dat het overgrote merendeel van de respondenten bestaat uit mannen (93,3%). De overige 6,7% bestaat uit één enkele vrouw. Dit verschilt van de 60%-40% man-vrouw verhouding die bij Foursquare blijkt te bestaan (Chappell 2011). De splitsing naar leeftijd, weergegeven in tabel 1, is binnen de groep representatiever voor alle Foursquare-gebruikers. 60% van de onderzoeksgroep is tussen de 18 en 35 jaar, terwijl dit bij Foursquare in zijn geheel zo'n 40% bedraagt (ibid.). Verder is van de respondenten 33,3% tussen de 36 en 55 jaar tegenover circa 51% van alle gebruikers. De respondenten in deze groep zijn dus gemiddeld genomen van iets jongere leeftijd dan alle andere Foursquare-gebruikers.

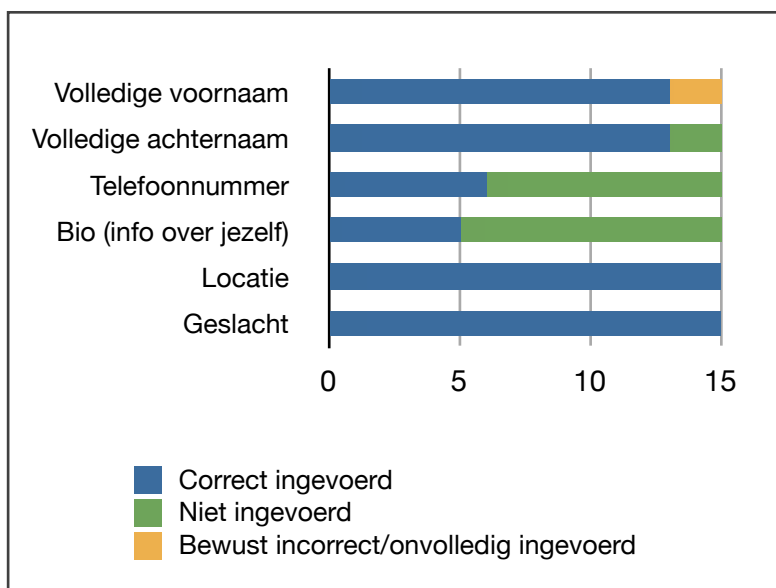
Tabel 1: frequentietabel van leeftijd van respondenten

Leeftijdsgroep	Frequentie	Percentage
Jonger dan 18 jaar	0	0,0
Tussen de 18 en 25 jaar	6	40,0
Tussen de 26 en 35 jaar	3	20,0
Tussen de 36 en 45 jaar	2	13,3
Tussen de 46 en 55 jaar	3	20,0
Tussen de 56 en 65 jaar	0	0,0
Ouder dan 65 jaar	1	6,7
Totaal	15	100,0

Omgang met persoonlijke gegevens

De respondenten is gevraagd welke informatie ze in hun persoonlijke Foursquare-profiel hebben ingevoerd. In het Foursquare-profiel kan de volgende informatie worden ingevoerd: voornaam, achternaam, telefoonnummer, e-mailadres, omschrijving van jezelf, locatie en geslacht. Hiervan moet er bij de voornaam en het e-mailadres verplicht een waarde worden ingevoerd. Aangezien een correct e-mailadres noodzakelijk is voor het activeren van het account, is dit veld niet opgenomen in dit onderzoek. Voor alle overige velden in het Foursquare-profiel hebben gebruikers de mogelijkheid het veld leeg te laten of bewust incorrect of onvolledig in te voeren. Er is gevraagd of gebruikers hiervan gebruik maken.

Figuur 1: verdeling over de invoering van persoonlijke gegevens in het Foursquare-profiel

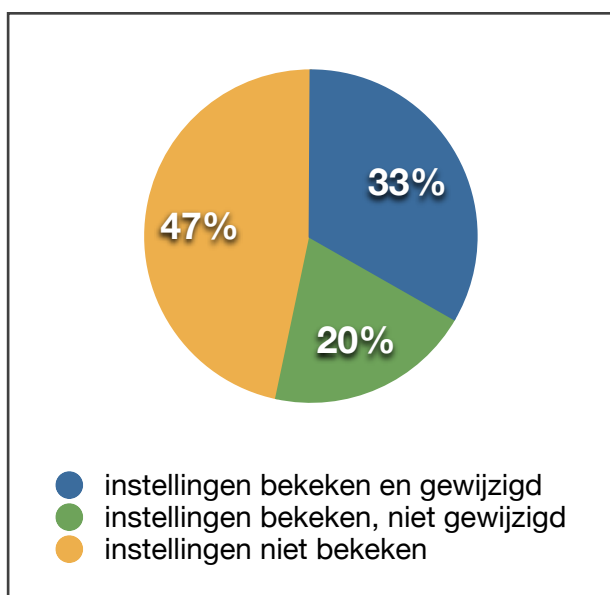


Van alle respondenten hebben er twee (13%) bewust een incorrect of onvolledige voornaam ingevoerd (figuur 1). Gebruikers kunnen bijvoorbeeld alleen een voorletter hebben gebruikt. De overige respondenten (87%) hebben de correcte voornaam ingevoerd. Bij de achternaam hebben dertien respondenten (87%) de correcte achternaam ingevoerd, de overige twee hebben het veld niet ingevoerd (13%). Het telefoonnummer en de omschrijving van jezelf (Bio) is vaker leeg gelaten, respectievelijk 60% en 67%. De locatie en het geslacht is door alle respondenten correct ingevoerd. De respondenten hebben dus in overgrote meerderheid hun voornaam, achternaam, locatie en geslacht naar waarheid ingevoerd. Het telefoonnummer en de omschrijving van jezelf is door de meerderheid niet ingevoerd.

Omgang met privacy-instellingen

Om een beeld te schetsen van de omgang van Foursquare-gebruikers met de privacy-instellingen is allereerst gevraagd of de gebruikers de instellingen weleens hebben bekeken. De respondenten die dit hebben gedaan is hierna gevraagd of ze de instellingen naar aanleiding daarvan hebben gewijzigd. De respondenten die hier weer bevestigend op hebben geantwoord is vervolgens gevraagd welke instellingen ze precies hebben gewijzigd. Zie figuur 1 voor de procentuele verdeling van de reacties op de eerste twee vragen.

Figuur 1: procentuele verdeling van het wel of niet bekijken en wijzigen van privacy-instellingen door de gebruikers

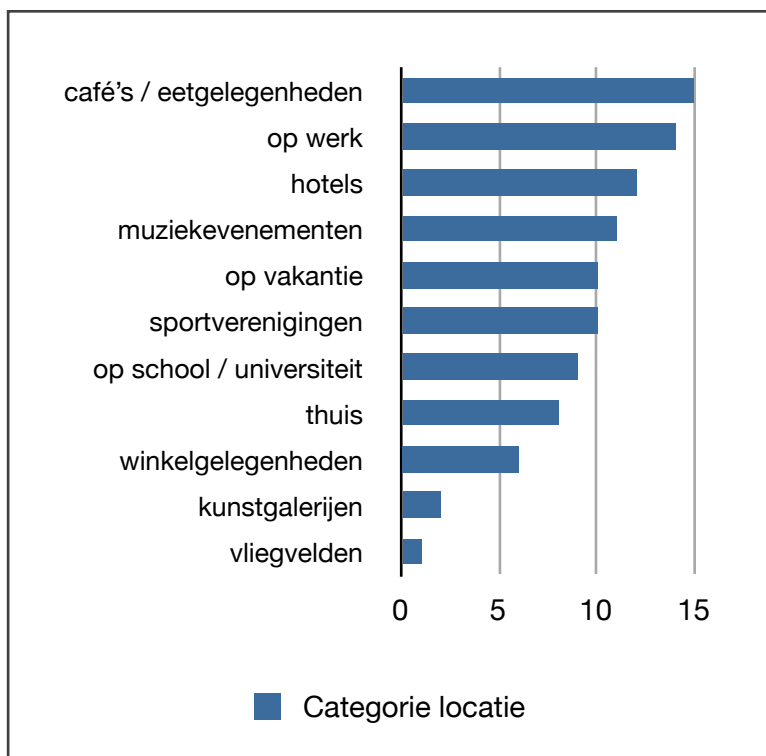


Iets minder dan de helft van de proefpersonen (47%) geeft aan de instellingen nooit te hebben bekeken. 20% heeft de instellingen wel bekeken, maar niet gewijzigd. De overige 33% heeft de instellingen zowel bekeken alsook gewijzigd. Deze laatste groep is gevraagd welke instellingen ze hebben gewijzigd. Van de vijf respondenten hebben allen aangegeven het telefoonnummer te verbergen voor vrienden en drie hebben het e-mailadres verborgen. De overige vier opties is door geen van allen uitgezet. Het gaat hierbij om mogelijkheden om de check-ins af te schermen voor anderen (zie afbeelding 1 op bladzijde 6). Geen enkele respondent heeft er dus voor gekozen om de openbaarheid van de locatiegegevens, de gedeelde check-ins, in te perken.

Soorten check-in locaties

De respondenten is gevraagd op welke verschillende soorten locaties ze inchecken. Hierbij is een lijst van tien soorten locaties voorgelegd met de mogelijkheid om zelf extra antwoorden toe te voegen. De resultaten zijn opgenomen in figuur 2.

Figuur 2: verdeling over de soorten plekken waar respondenten inchecken



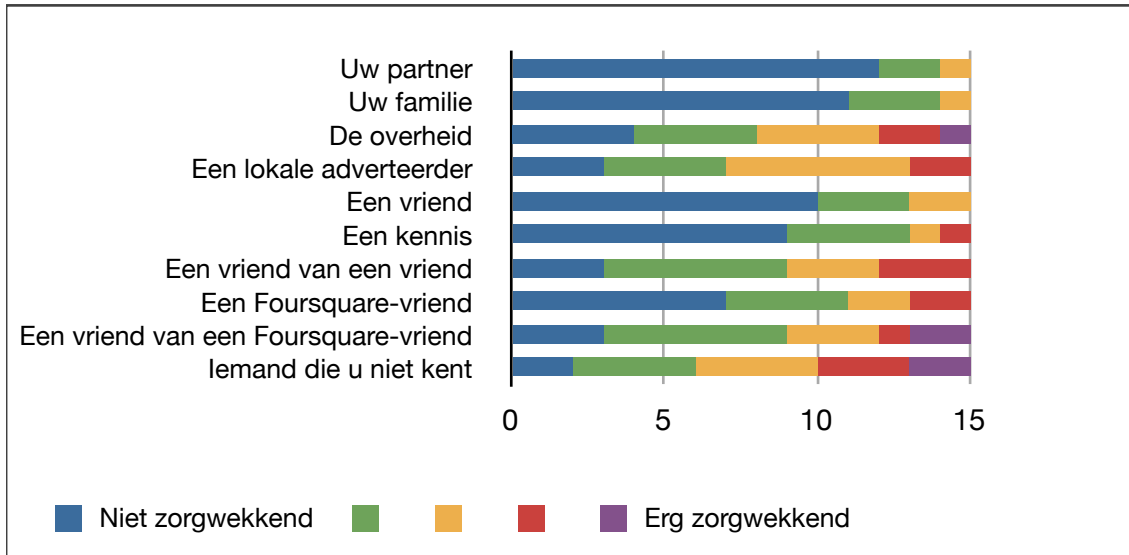
Alle respondenten geven aan weleens in te checken bij cafés of eetgelegenheden. Ook checken bijna alle gebruikers af en toe in op het werk (93,3%). Hierna volgen check-ins in hotels (80%), bij muziekevenementen (73,3%), op vakantie (66,7%), bij sportverenigingen (66,7%), op school / universiteit (60%), thuis (53,3%), bij winkelgelegenheden (40%), bij kunstgalerijen (13,3%) en op vliegvelden (6,7%). Dit geeft weer dat bijna alle respondenten zowel inchecken op plekken in woon- en werkomgeving (op werk, op school / universiteit en thuis) als plekken tijdens vrijetijdsbesteding (overige keuzes).

Zorgen over openbaring locatiegegevens

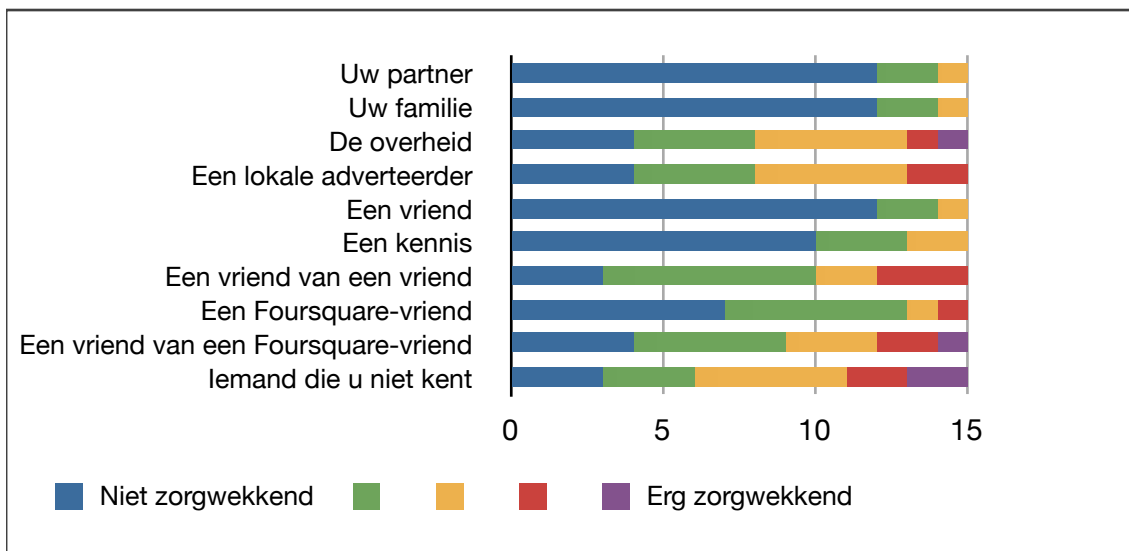
Om te onderzoeken of gebruikers het zorgwekkend vinden wanneer anderen hun locatie weten, is er een tweedelige vraag gesteld. Eerst is de respondent gevraagd in welke mate hij/zij het zorgwekkend vindt wanneer iemand anders weet waar hij/zij woont en werkt/studeert. Er is onderscheid gemaakt in tien verschillende personen of instanties die de locaties te weten zouden kunnen komen: de partner, de familieleden, de overheid, een lokale adverteerder, een vriend, een kennis, een vriend van een vriend, een Foursquare-vriend, een vriend van een Foursquare-vriend en iemand die de respondent niet kent. Vervolgens is gevraagd in welke mate de respondent het zorgwekkend vindt als anderen weten welke cafés en eetgelegenheden hij/zij bezoekt. Ook hier diende de respondent

voor de tien bovengenoemde personen en instanties antwoord te geven. De resultaten zijn opgenomen in figuur 3 en figuur 4.

Figuur 3: verdeling over mate van zorgwekkendheid naar soort personen en instanties, wanneer zij weten waar de respondent woont en werkt/studeert



Figuur 4: verdeling over mate van zorgwekkendheid naar soort personen en instanties, wanneer zij weten welke caf es en eetgelegenheden de respondent bezoekt



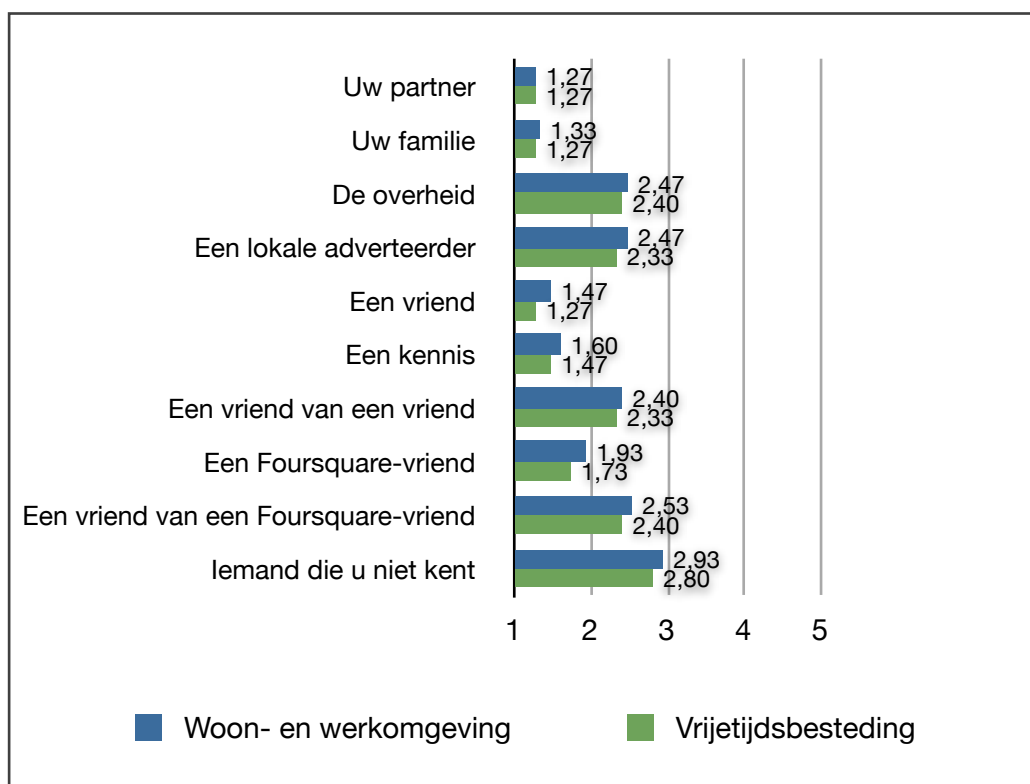
Uit figuur 3 blijkt dat de respondenten het niet erg zorgwekkend vinden als de partner, familie, vriend en kennis weet waar hij/zij woont, werkt of studeert. De gemiddelde waardes zijn respectievelijk 1,27; 1,33; 1,47 en 1,60, waarbij 1 niet zorgwekkend en 5 erg zorgwekkend is. De gebruikers vinden het iets zorgwekkender als een Foursquare-vriend

de locatie weet in woon- en werkomgeving (gemiddelde 1,93). Voor de overheid (2,47), een lokale adverteerder (2,47), een vriend van een Foursquare-vriend (2,53) en een onbekende (2,93) is het voor de respondent het meest zorgwekkend wanneer zij de locaties weten. Uit figuur 4 blijkt dat de zorgwekkendheid bijna gelijk is aan voorgaande wanneer de verschillende personen en instanties weten welke café's en eetgelegenheden de respondent bezoekt.

In figuur 5 zijn dat de resultaten bij de vrijetijdsbesteding en de woon- en werkomgeving samengevoegd.

Figuur 5: weergave van gemiddelde scores van figuur 3 en figuur 4

(1 = niet zorgwekkend, 5 = erg zorgwekkend)



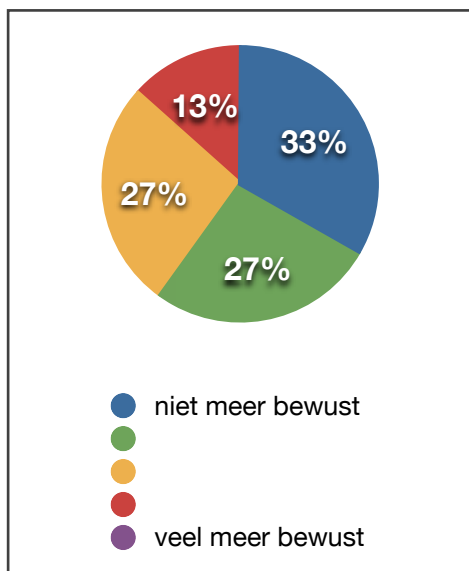
Uit figuur 5 blijkt dat de mate van zorgwekkendheid van de respondenten steeds iets hoger is bij de woon- werkomgeving dan bij de vrijetijdsbesteding. Dit verschil is echter minimaal.

Effect enquête op bewustzijn privacy

Het kan zijn dat de respondenten na het invoeren van de enquête zich meer bewust zijn van de mogelijkheden die Foursquare biedt om de gegevens van de gebruiker te

beschermen. Om dit te meten is gevraagd of de respondent, na het invoeren van de vragenlijst, zich meer bewust is van deze mogelijkheden (figuur 6).

Figuur 6: procentuele verdeling van de mate waarin respondenten, na het invullen van de vragenlijst, zich meer bewust zijn van mogelijkheden voor het beschermen van gegevens op Foursquare



Uit figuur 6 blijkt dat vijf respondenten zich net zo bewust zijn van het beschermen van hun gegevens op het platform als ervoor (33%). Vier andere respondenten zijn zich iets meer bewust geworden (27%), vier anderen geven aan meer bewust te zijn geworden (27%). De twee overige respondenten hebben aangegeven zich aanzienlijk meer bewust te zijn geworden van de mogelijkheden tot het beschermen van de gegevens (13%). Niemand heeft voor de laatste optie gekozen.

Tevens is gevraagd of de respondent meer aandacht zal gaan besteden aan het beschermen van zijn of haar persoonsgegevens en locatiegegevens op Foursquare. De respondenten hadden de mogelijkheid met maximaal 200 woorden antwoord te geven. Vijf van de vijftien respondenten hebben geen antwoord ingevoerd. Van de overige tien hebben er negen gesteld er niet meer aandacht aan te besteden. Twee hiervan hebben alleen geantwoord met 'Nee', een ander heeft gereageerd met 'Nee, dat deed ik al' en een ander met 'Nee, ik pas altijd op'. Een ander reageert voorzichtiger met: 'Ik denk het niet. Was me altijd al bewust van het zorgvuldig omgaan met deze gegevens'. De gebruikers lijken er voor te kiezen om gegevens die ze niet openbaar willen hebben ook niet op sociale netwerksites te plaatsen. Zo antwoordt een respondent met: 'Wanneer ik incheck via Foursquare dan heb ik me op voorhand al afgevraagd of ik het erg vind dat wie dan ook dit kan lezen. Ik zal dan ook niet inchecken wanneer ik ergens ben wat ik niet wil delen'.

Conclusie

Uit dit onderzoek is gebleken dat Foursquare-gebruikers vaak de privacy-instellingen niet lezen of veranderen ten opzichte van de ingestelde waarden. Gebruikers schermen hun check-ins niet af van lokale ondernemers en andere (niet bevriende) gebruikers. Hieruit blijkt dat gebruikers er geen problemen mee hebben dat anderen kennis kunnen nemen van de locaties waar ze inchecken, of dat ze simpelweg niet weten dat dit gebeurt. Tevens blijkt dat gebruikers vaak hun echte voornaam en achternaam in de profielpagina opnemen. Gebruikers hebben er geen problemen mee dat deze gegevens inzichtelijk zijn voor anderen. Voor het bedrijf Foursquare is het waarschijnlijk geen probleem dat veel persoonlijke informatie inzichtelijk is. Integendeel, des te meer persoonlijke informatie openbaar is, des te groter de waarde van Foursquare als geheel zal zijn. Foursquare kan deze gegevens namelijk gebruiken om advertenties beter te kunnen toespitsen op hun gebruikers. Voor de overheid is het echter van belang om er op toe te zien dat deze gegevens door Foursquare niet worden misbruikt of voor andere doeleinden worden gebruikt, aangezien gebruikers blijkbaar geen moeite hebben om deze gegevens openbaar te maken.

Foursquare-gebruikers checken zowel in op plekken behorende bij de woon- en werkomgeving als bij de vrijetijdsbesteding. Er is gebleken dat gebruikers het even zorgwekkend vinden als anderen weten waar ze wonen en werken als waar ze hun vrije tijd doorbrengen. Dit onderzoek toont dus aan dat er geen verschil is in de mate van het gevoel van privacy als het gaat om informatie uit de privésfeer en informatie uit de publieke sfeer. Zoals eerder genoemd stelde Goffman dat personen zich anders gedragen bij verschillende personen in verschillende situaties (Iachello & Hong 2007, 11). In dit onderzoek blijkt dat Foursquare-gebruikers het inchecken op locaties in privésfeer en in publieke sfeer echter niet als verschillend ervaren aangezien ze zich hier niet anders gedragen. Wellicht brengt de omgeving van een sociaal netwerksite een ander idee met zich mee over wat mensen publiek maken en wat ze privé houden.

De mate van zorgwekkendheid van de gebruiker is wel afhankelijk van de entiteit die de locatie van de gebruiker weet. Het blijkt vooral zorgwekkend gevonden te worden wanneer de overheid, een lokale adverteerder, een onbekende of een vriend van een vriend kennis heeft van de bezochte locaties. Dit geldt in mindere mate wanneer het de partner, familie of een vriend betreft. Hier blijkt onder andere uit dat de mate van zorgwekkendheid afhankelijk is van de mate waarin iemand bevriend of verbonden is met een ander. Wanneer een kennis weet waar persoon X werkt of studeert blijkt dit iets zorgwekkender te zijn dan wanneer de partner dit weet. Binnen Foursquare kun je alleen locaties delen met al je vrienden en niet een gespecificeerd deel van deze groep. Wanneer

Foursquare de mogelijkheid zou bieden om vrienden onder te verdelen in zelf te beheren groepen zouden gebruikers de mogelijkheid hebben om informatie in een bepaalde kring wel te delen en in een andere kring niet. Zo zou een gebruiker wel zijn huisgenoten kunnen laten weten in een discotheek te zijn geweest, maar dit achterhouden voor de partner en familie. Op deze manier zouden gebruikers meer controle kunnen houden op de plekken waar bepaalde informatie wel of niet terecht komt en wordt het gevoel van privacy meer gewaarborgd.

De respondenten die hebben deelgenomen aan de enquête zijn zich nauwelijks meer bewust geworden van de mogelijkheden tot het inperken van de openbaring van de gegevens op het platform. Uit het onderzoek blijkt dat Foursquare-gebruikers zich bewust zijn van de manier waarop hun gegevens inzichtelijk zijn voor anderen. Ze stellen voorzichtig te zijn met wat ze plaatsen en publiceren alleen de informatie waarvan ze het gevoel hebben dat ze hier geen grote schade bij kunnen ondervinden. Hieruit blijkt dat er enig wantrouwen is in de manier van dataverwerking en dataverspreiding van Foursquare. Dit lijkt een beperking van het platform, want als er meer vertrouwen zou zijn in de bescherming van de data dan zouden gebruikers zich vrijer voelen om ook meer intieme gegevens te plaatsen. Het is belangrijk voor de makers van Foursquare om gebruikers duidelijk te maken hoe ze informatie verwerken en verspreiden.

Discussie

Het onderzoek dat ik heb uitgevoerd is explorierend van aard en kan als aanzet worden gezien voor verder onderzoek naar privacy op sociale netwerksites en privacy omtrent locatiegebonden gegevens. Er hebben vijftien respondenten meegedaan aan het onderzoek waarvan slechts één vrouw. Dit blijkt te verschillen van de 60%-40% man-vrouw verhouding van de Foursquare-gebruikers. Dit verschil is mogelijk te wijten aan het feit dat de meerderheid van de benaderde personen in mijn netwerk mannelijk is. Naar mijn idee hoeft dit geen consequenties te hebben voor de resultaten van het onderzoek, aangezien ik geen reden heb om aan te nemen dat mannen en vrouwen andere ideeën hebben over privacy op Foursquare. Een gelijkwaardig onderzoek onder een grotere groep Foursquare-gebruikers, met een evenwichtige verdeling over mannen en vrouwen, zou statistisch betrouwbaardere resultaten op kunnen leveren en een eventueel verschil tussen mannen en vrouwen kunnen aantonen.

In dit onderzoek is respondenten gevraagd naar hun mate van zorgwekkendheid wanneer anderen kennis hebben van hun locatie. Er zijn echter geen vragen gesteld of de respondent het 'aangenaam' of 'belangrijk' vindt als een entiteit weet heeft van zijn/haar locatie. De indeling van de enquête leent zich er sterk voor om naast een mate van zorgwekkend ook andere waarden bij de gebruikers te meten. Op deze manier kan er nog meer inzicht worden verkregen over de beweegredenen van gebruikers om een locatie wel of niet te delen op het platform.

Ik heb gevraagd of Foursquare-gebruikers hun privacy-instellingen op het platform bekijken en/of wijzigen. Een andere manier om deze gegevens te achterhalen, is om het direct uit de database van het Foursquare-platform af te lezen. Hiermee heb je een betrouwbaarder resultaat, aangezien je de beschikking hebt over de gegevens van alle gebruikers en geen risico loopt dat gebruikers de vragen onjuist invullen op een enquête. Aangezien alleen Foursquare toegang heeft tot deze gegevens zullen deze resultaten door Foursquare zelf naar buiten moeten worden gebracht. Het is de vraag of dit niet als schending van de privacy van de gebruikers kan worden gezien.

Bibliografie

- Bits of Freedom. 2012. Webwijs. *Bits of Freedom*. Januari 21. <https://www.bof.nl/ons-werk/webwijs/>
- Chappell, Brian. 2011. 2011 Social Network Analysis Report – Geographic – Demographic and Traffic Data Revealed. *Ignite Social Media Blog*. April 6. <http://www.ignitesocialmedia.com/social-media-stats/2011-social-network-analysis-report/>
- Europa Nu. 2012. Europese Commissie wil grondige hervorming bescherming persoonsgegevens. *Europa Nu*. Januari 25. http://www.europa-nu.nl/id/viwfi9piewzi/nieuws/europese_commissie_wil_grondige?ctx=vhsih95vppua
- Foursquare. 2011. Wow! The foursquare community has over 10,000,000 members! *Foursquare*. Juni 26. <http://blog.foursquare.com/2011/06/20/holysmokes10millionpeople/>
- Gross, Ralph & Acquisti, Alessandro. 2005. Information Revelation and Privacy in Online Social Networks (The Facebook case). In *The Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, 71-80.
- Hoven, Jeroen van den. 2008. Information Technology, Privacy, and the Protection of Personal Data. In *Information Technology and Moral Philosophy*, ed. Jeroen van den Hoven & John Weckert, 301-321. New York: Cambridge University Press.
- Iachello, Giovanni & Hong, Jason. 2007. End-User Privacy in Human-Computer Interaction. *Foundations and Trends in Human-Computer Interaction* 1(1): 1-137.
- Lindqvist, Janne, ed. 2011. I'm the Mayor of My House: Examining Why People Use Foursquare. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI-11)* 54(6): 2409-2418. Online beschikbaar. <http://www.cs.cmu.edu/~jasonh/publications/chi2011-foursquare-final.pdf>

McDonald, Aleecia M. & Cranor, Lorrie Faith. 2008. The Cost of Reading Privacy Policies. In *A Journal of Law and Policy for the Information Society* 4(3): 543-897. Online beschikbaar.

<http://www.cs.cmu.edu/~jasonh/publications/chi2011-foursquare-final.pdf>

Siegel and Gale. 2012. A SimplicityLab Consumer Research Survey. *Siegel and Gale*. Maart 12.

http://www.siegelgale.com/white_paper/a-simplicitylab-consumer-research-study/

Solove, Daniel. 2006. A Taxonomy of Privacy. *University of Pennsylvania Law Review* 154(3): 477-560.

Warren, Samuel & Brandeis, Louis. 1890. The Right to Privacy. *Harvard Law Review* 4(5): 193-220.

Bijlage A: Enquête Foursquare-gebruik

Beste Foursquare-gebruiker,

In het kader van mijn studie Communicatie- en Informatiewetenschappen (Universiteit Utrecht) doe ik een onderzoek naar het gebruik van Foursquare. Ik ben geïnteresseerd in de manier waarop gebruikers omgaan met de informatie die ze op Foursquare plaatsen. Ik wil u vragen deze enquête in te vullen, dit kost slechts enkele minuten.

Let op: u kunt deze enquête alleen invullen wanneer u met enige regelmaat gebruik maakt van Foursquare.

Alvast bedankt!

Met vriendelijke groet,
Rik van Ooijen

1. Wat is uw geslacht?

- Man
- Vrouw

2. Tot welke leeftijdscategorie behoort u?

- Jonger dan 18 jaar
- Tussen de 18 en 25 jaar
- Tussen de 26 en 35 jaar
- Tussen de 36 en 45 jaar
- Tussen de 46 en 55 jaar
- Tussen de 56 en 65 jaar
- Ouder dan 65 jaar

3. Wat is uw hoogst genoten opleiding?

- Middelbare school
- Middelbaar beroepsonderwijs
- Hoger beroepsonderwijs
- Wetenschappelijk onderwijs

4. Bent u ook actief op Facebook?

- ja
- nee

5. Bent u ook actief op Twitter?

- ja
- nee

6. Sinds wanneer bent u actief op Foursquare? (U kunt uw eerste check-in vinden op www.foursquare.com onder 'History')

[maand] [jaar]

7. Hoe vaak checkt u ongeveer per maand in? (U kunt dit vinden op www.foursquare.com onder 'History')

- Minder dan 5 keer
- 5 tot 10 keer

- 10 tot 20 keer
- 20 tot 30 keer
- 30 tot 40 keer
- 40 tot 50 keer
- Meer dan 50 keer

8. Hebt u de Privacy Settings van uw Foursquare-account weleens bekeken?

- ja
- nee

Bij 'ja' naar vraag 9, bij 'nee' naar vraag 11.

9. Hebt u deze Privacy Settings naar aanleiding hiervan gewijzigd?

- ja
- nee

Bij 'ja' naar vraag 10, bij 'nee' naar vraag 11.

10. Wat heeft u precies gewijzigd?

- Telefoonnummer verbergen
- E-mailadres verbergen
- Jezelf verbergen in lijst van personen die op een bepaalde plek hebben ingecheckt (Who's here)
- Jezelf geen (publieke) mayorships laten verdienen
- Jezelf verbergen wanneer een vriend jou noemt in een checkin post op Twitter of Facebook
- Jezelf verbergen voor eigenaren van plaatsen (café's, etc) waar je incheckt.

11. Heeft u in uw profiel de volgende informatie ingevoerd: (zie

www.foursquare.com => Settings)

	niet ingevoerd	correct ingevoerd	bewust incorrect/onvolledig ingevoerd
a. Volledige voornaam	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
b. Volledige achternaam	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
c. Telefoonnummer	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
d. Bio (info over jezelf)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- | | | | |
|-------------|-----------------------|-----------------------|-----------------------|
| e. Locatie | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| f. Geslacht | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

12. Op welke plekken checkt u weleens in? (meerdere antwoorden mogelijk)

- thuis
- op werk
- op school / universiteit
- café's / eetgelegenheden
- sportverenigingen
- winkelgelegenheden
- hotels
- muziekevenementen
- kunstgalerijen
- op vakantie
- anders, namelijk

13. Geef voor de volgende vragen aan in welke mate het voor u van toepassing is.

- a. Ik gebruik Foursquare om bij te houden waar mijn vrienden zich bevinden
niet waar waar
- b. Ik gebruik Foursquare om nieuwe vrienden te vinden
niet waar waar
- c. Ik gebruik Foursquare om Mayorships en Badges te verdienen
niet waar waar

14. Wat vindt u er van als:

- | | | | | | | |
|---|------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| | niet zorgwekkend | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | erg zorgwekkend |
| a. Uw partner weet waar u woont en werkt/studeert | | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

b. Uw familieleden weten waar u woont en werkt/studeert	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
c. De overheid weet waar u woont en werkt/studeert	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
d. Een lokale adverteerder weet waar u woont en werkt/studeert	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
e. Een vriend van u weet waar u woont en werkt/studeert	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
f. Een kennis van u weet waar u woont en werkt/studeert	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
g. Een vriend van een vriend, die u niet kent, weet waar u woont en werkt/studeert	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
h. Een Foursquare-vriend weet waar u woont en werkt/studeert	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
i. Een vriend van een Foursquare-vriend, die u niet kent, weet waar u woont en werkt/studeert	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
j. Iemand die u niet kent weet waar u woont en werkt/studeert	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

15. Wat vindt u er van als:

	niet zorgwekkend		erg zorgwekkend		
a. Uw partner weet welke café's en eetgelegenheden u bezoekt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
b. Uw familieleden weten welke café's en eetgelegenheden u bezoekt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
c. De overheid weet welke café's en eetgelegenheden u bezoekt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
d. Een lokale adverteerder weet welke café's en eetgelegenheden u bezoekt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
e. Een vriend van u weet welke café's en eetgelegenheden u bezoekt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
f. Een kennis van u weet welke café's en eetgelegenheden u bezoekt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
g. Een vriend van een vriend, die u niet kent, weet welke café's en eetgelegenheden u bezoekt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
h. Een Foursquare-vriend weet welke café's en eetgelegenheden u bezoekt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
i. Een vriend van een Foursquare-vriend, die u niet kent, weet welke café's en eetgelegenheden u bezoekt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
j. Iemand die u niet kent weet welke café's en eetgelegenheden u bezoekt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

16. Bent u zich, na het invullen van deze enquête, meer bewust van de mogelijkheden voor het beschermen van uw persoonsgegevens?

niet meer bewust veel meer bewust

17. Denkt u dat u, na het invullen van deze enquête, meer aandacht zult besteden aan het beschermen van uw persoonsgegevens en locatiegegevens op Foursquare?

Bedankt voor het invullen van deze enquête!