Mobile Privacy Workshop, University of Maryland, June 25-26, 2018
Scoping Paper

This event will be an intimate gathering of stakeholders in academia, industry, and policy from the U.S., Canada, and Europe to help discuss emerging issues in privacy within mobile ecosystems, further build the trans-Atlantic network of privacy researchers, explore innovative methodological approaches in privacy research, and generate feedback on our next steps for the project. The preliminary findings of the *Mapping Privacy and Surveillance Dynamics in Emerging Mobile Ecosystems: Practices and Contexts Project* will be presented. The workshop primary goal is to crowdsource innovative solutions for privacy research in the context of mobilities and devices, as well as to build an international network of researchers, designers, and policymakers in this space. Participants will engage in discussions and small group-sessions focused on vignettes for triangulating research, data collection, conceptual reconsiderations, and multi-focus and cross-national research.

About the Project

This project is a collaboration between Jessica Vitak at UMD, Michael Zimmer at UW-Milwaukee, and Jason Pridmore and Daniel Trottier at Erasmus University. There are four PhD researchers involved: Priya Kumar, Yuting Liao, Katie Chamberlain Kritikos, and Anouk Mols. The project received funding from the NSF (US) and NWO (Netherlands). For more information and (draft) papers, check: https://mobileprivacy.umd.edu/.

Broadly speaking, this project evaluates mobile users' mental models of privacy alongside the perceived social costs (e.g., interpersonal and institutional surveillance), affordances (e.g., ubiquitous communication, facilitated social coordination), and (un)anticipated byproducts (e.g., routine upkeep of profiles and configuring settings) associated with the pervasive use of mobile technologies. The relationship between these factors is evaluated through a collaborative, multidisciplinary investigation of three cross-cutting mobile ecosystems by an international research team. The chosen ecosystems—health and fitness tracking, mobile messaging, and intelligent personal assistants—highlight both emergent and longstanding privacy challenges associated with data surveillance. The research team is evaluating how cultural differences and contextual practices influence individual users' attitudes toward privacy and surveillance generally, as well as their attitudes toward specific facets of mobile technologies and specific actors involved in data transactions. The goal of these evaluations is to inform both conceptual models and practical implementations that pertain to the digital self, with an emphasis on tensions between privacy, disclosure, mobility and surveillance in the US and Europe.

Research within the three foci of the project play into current events such as the recent introduction of interactive home devices and new privacy guidelines like the General Data Protection Regulation (GDPR).

Below, we highlight some of our (preliminary) findings during the first 18 months of the project.

Mapping Privacy and Surveillance Dynamics in Emerging Mobile Ecosystems: Practices and Contexts

1 Fitness Trackers

U.S. Research (2017): 361 survey responses and 33 interviews from staff at UMD and UW-Milwaukee who currently owned and used a Fitbit or Jawbone fitness tracker. See the iConference paper[1] for analysis of survey data and the ICA paper for analysis of interview data. Two additional papers using the interview data are currently under review.

- ➔ **Fitness tracker users had very limited knowledge of the policies of fitness tracking companies.**
  73% of respondents did not know whether Fitbit/Jawbone sold their data, and 66% were not sure who owned their data. Regarding data retention, 85% of respondents did not know how long companies stored the data, and 89% were unsure where their data was stored besides the device.

- ➔ **Users with higher general privacy concerns and higher mobile data privacy concerns were more likely to perceive personal fitness information (PFI) as "sensitive" data.**
  Using structural equation modelling, these two variables explained 22% of the variance in responses to the question, *"How concerned would you be if your [Fitbit/Jawbone] data were compromised, such a through a security breach at the company?"*

- ➔ **Perceived benefits greatly outweighed concerns about how PFI might be (mis)used.**
  "I don't think there's that much information out there that really would hurt me if anybody knew about it. I don't think there's anybody that's going to take my pattern of heart rate and go with and do anything to me. Where are you going to get that? Maybe that's just I'm a trusting person or maybe that's I'm naïve, but unless I have a reason for thinking or knowing that something's going to hurt me, I don't care."

- ➔ **Data generated by fitness trackers is largely seen as innocuous and participants saw few opportunities for negative outcomes.**
  "It has crossed my mind what if this information were shared with an insurance company or it impacted my health care in some way, or my ability to obtain health care in some way? It's crossed my mind, and then I dismiss it."

  "If this information was public, I wouldn't be upset by it. If anybody wants to know how much water I drink, wow, they need to get a life."

- ➔ **Trust in the company collecting data (e.g., Fitbit) reduced privacy concerns.**
  "I don't have any reason to not trust [Fitbit]. I haven't heard anything bad about them. There hasn't been any information out there about any breach of the data that they collect. I'm sure that when I did the set-up it had a whole privacy statement and all that kind of stuff on it. If I had had any concerns about it, I probably wouldn't have set it up."

- ➔ **Participants engaged in limited behaviors related to protecting their PFI; most said they had not looked at the privacy settings since first downloading the app.**

[1] Vitak et al. (2018). Privacy Attitudes and Data Valuation Among Fitness Tracker Users. iConfernce. Available: http://mobileprivacy.umd.edu/wp-content/uploads/2018/01/Fitbit-privacy-2018-final-iconf-edits-Dec10.pdf

"I can't remember [having any privacy concerns when setting up my Fitbit] and I wouldn't have checked what they were collecting. Again, if it's not very front-facing about it, I'm bad about going in and looking at it. I know I should, but I just get lazy about it, so I don't think so. And if there was, I may have gone in and changed the settings to say, 'No, I don't want you actually doing this,' or I may have tried and got annoyed and then forgot."

2 Messaging Apps

NL Research (2017): 28 interviews and 2 focus groups (43 respondents) in work environment and neighbourhood watch contexts.

"When there are cars in the neighbourhood **we're not familiar with**, or we are not sure about **people we have never seen before**, we'll **make a picture and send it**: 'Do we know anything about this?'" (Pauline, moderator WhatsApp neighbourhood crime prevention group)

➔ **Messaging apps increase and <u>mobilise</u> lateral surveillance.**

"I'm so boring**, I have so little to hide**, I don't really have a problem [with online monitoring] (...) **I don't care**, you know, if the NSA wants to know where I am, that's fine, and if Google wants to read my email, yes, I'd rather get targeted advertising than advertising about women's products. **Fine by me**." (Kai, moderator WhatsApp neighbourhood crime prevention group)

➔ **Many respondents seem to accept online monitoring, yet ...**

"Well, **nobody needs to know** what I'll do all day. (…) And you can have **private reasons** for not reacting to messages" (Joyce, works in a restaurant)

"On WhatsApp, **it is easy to forward messages**, and people **show messages to others**. Or your phone is lying around and someone reads your WhatsApp. Nobody will easily read your emails, but some **think it is funny** to read someone else's messaging conversations." (Roy, HR manager at a multinational)

➔ **They voice concerns about privacy breaches in an interpersonal context.**

"**Privacy means a lot for me**, really a lot, and it is worth a lot as well. So that's why I make a deliberate choice about which things I **do or don't share** via WhatsApp or, more generally, digital communication. (…) On the other hand, I'm an open book in everyday life. So, I like sharing feelings or things like that. But there is always that thought process going on: 'Hey, I want to share this, what am I going to say now'. So, **privacy is really important**, but **flexible** as well" (Paul, works at a software company)

➔ **Privacy negotiations are visible on multiple levels.**

> "For me **that's a privacy thing, those blue checks** [on WhatsApp]. It **pushes me to react directly** because I've read it. And therefore, sometimes I **deliberately** do not open my messages. Because if I do, I know that they know that I've read their message and did not react." (Robin, works at a communication firm)

➔ **Respondents devise individual strategies to protect privacy.**

Privacy is more tangible in an interpersonal context. Respondents struggle with privacy concerns, blurring boundaries, collapsing contexts, and information overload, so they devise their own strategies to cope with this.

3 Intelligent Personal Assistants (IPAs)

Cross-cultural Research (2018): While the prior studies were conducted independently, our study our IPAs (including Siri, Google Assistant, Alexa, and Google Home) was conducted simultaneously in the U.S. and the Netherlands using the same survey instrument and focus group protocols in Spring 2018.

For the survey, we gathered random samples of university staff from UMD, UW-Milwaukee, and Erasmus University. The only criteria for participating were being 18+ and a smartphone user, as we wanted to gain attitudes from adopters and non-adopters (and because these tools are still limited in the Netherlands). We collected 265 completed responses from the Netherlands and 1178 responses from the U.S. data collection.

3.1 Survey Preliminary Results

We first asked respondents whether they currently or previously used a personal assistant on their smartphone, either through a built-in feature like Siri or a downloadable app like Google Assistant. Responses in both countries are presented in Figure 1.

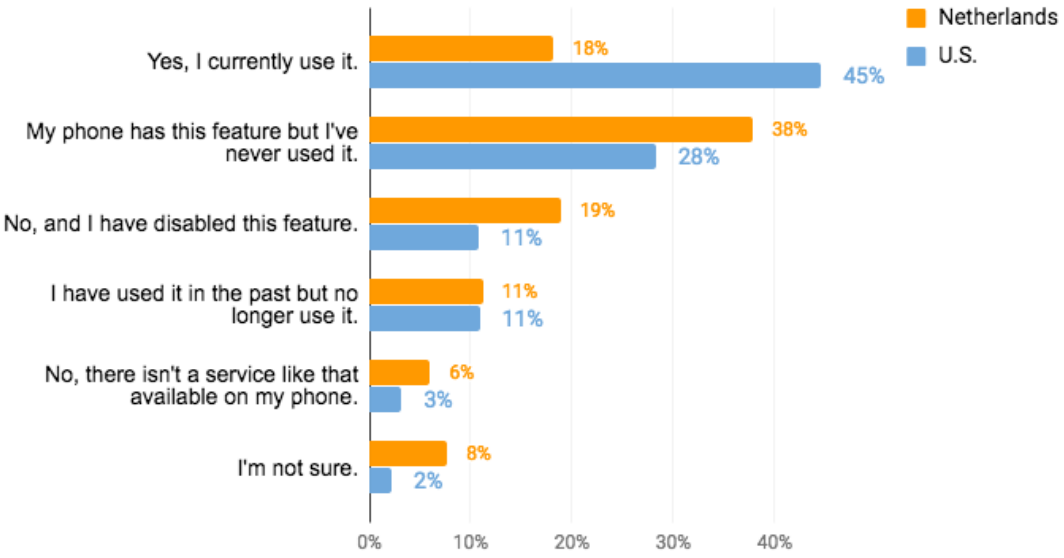

Figure 1. Survey Question: Do you have Siri, Google Assistant, or another intelligent personal assistant (IPA) activated on your smartphone?

Based on how respondents reported their use of IPA on the smartphone, we asked branch questions in the survey to gauge different angles of experiences and attitudes among current users and non-users.

Smartphone IPA current users

IPA is more popular and used more frequently among smartphone users in the U.S. compared to that in the Netherlands. In our sample, 44.6% of smartphone users (n=524) in the U.S. reported that they currently use Siri, Google Assistant, or other IPA on their smartphones, while only 18.2% of respondents (n=52) in the Netherlands have activated an IPA on their smartphone (see Figure 1).

For those who currently use IPAs on their smartphone, people in the U.S. reported a higher frequency of use [Range 1(less often)—5 (multiple times a day); *M*(*SD*)=3.62(1.36)], compared to people in the Netherlands [*M*(*SD*)=2.87(1.46)].

People use smartphone IPAs for a variety of purposes (see Figure 2). In the U.S., people reported that they used the following features the most: "Ask factual questions (e.g., weather conditions, film times)," "Get directions/location of a place," and "Ask silly/funny questions just for laughs." In the Netherlands, the top three most reported purposes were: "Ask factual questions (e.g., weather conditions, film times)," "Ask silly/funny questions just for laughs," and "Set a timer."

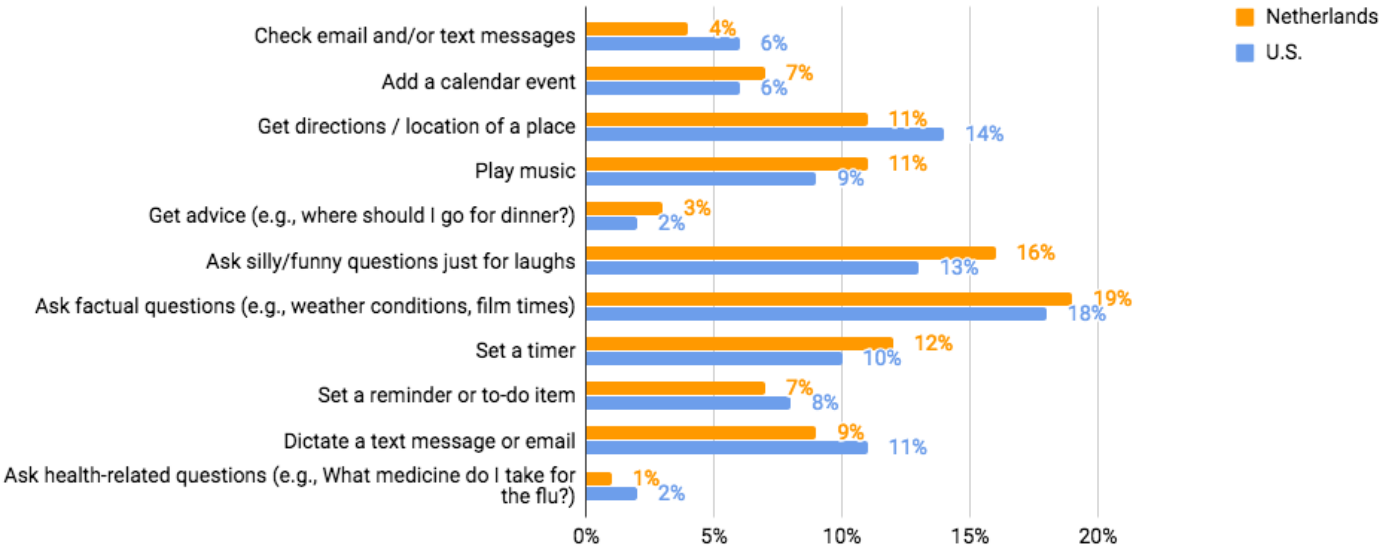

Figure 2. Have you ever used Siri / Google Assistant for any of the following purposes? Select all that apply.

Smartphone IPA non-users

Twenty-eight percent of smartphone users (n=332) in the U.S. reported that, "My phone has this feature but I've never used it," compared to 38 percent (n=108) in the Netherlands. We further asked respondents to rate the importance of a list of factors in their decisions to not use an IPA on their phone. For respondents in the U.S., the top three most important factors were: (1) "I don't see any benefits from this feature," (2) "I don't like talking aloud to my phone," and (3) "The user-interface is frustrating/doesn't work like I want it to." In the Netherlands, the top three most important factors were: (1) "I don't see any benefits from this feature," (2) "I don't like talking aloud to my phone," and (3) "It's awkward to use."

In both countries, having privacy concerns was not a very important factor in their decisions not use IPA on the smartphone (*M*=2.94 in Netherlands, *M*=2.88 in U.S.).

Home IPA use

We asked respondents whether they had heard of IPA-enabled smart home devices and we specifically asked about three types: Google Home, Amazon Echo, and Apple Homepod. The vast majority of respondents in the U.S. said they have heard of at least one of the devices, while fewer people in the Netherlands heard of these home devices (see Figure 3).

Next, we asked whether respondents own an IPA home device (see Figure 4). Ten percent respondents (n=108) in the U.S. reported that they own a Google Home/Home Mini, 24 percent (n=272) respondents reported owning an Amazon Echo/Echo Dot. However, very few people in the Netherlands own the devices, with only 2 percent (n=6) owning Google Home/Home Mini and 2 percent (n=5) owning Amazon Echo/Echo Dot.

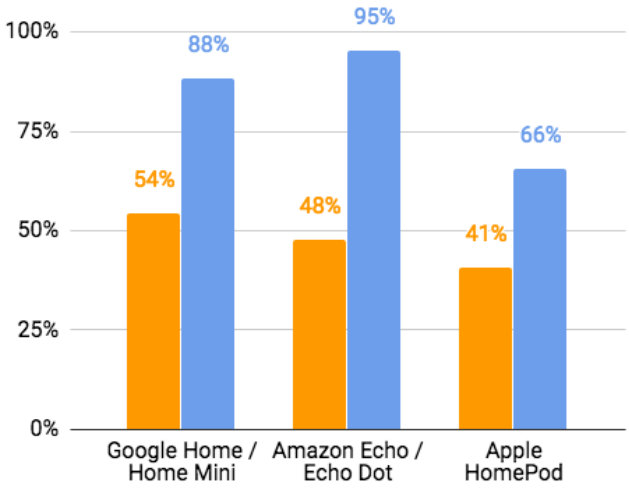

Figure 3. People (%) who heard of IPA home devices

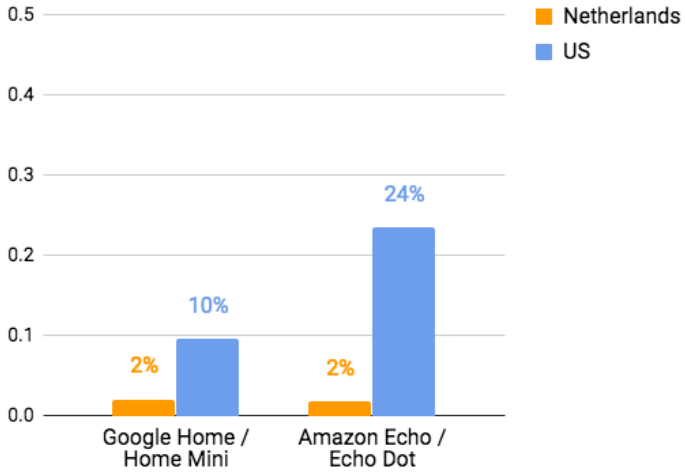

Figure 4. People (%) who own IPA home devices

In the U.S., owners of IPA smart home devices reported their main reasons for buy it, with the most common reason being they had received it as a gift, followed by "Controlling smart home devices," "Just curious/for fun," "Streaming music," and hands-free access to online information.

Privacy Concerns

Concerns regarding digital technology and mobile apps

Respondents in both countries were generally fairly concerned about their privacy when using communication technologies (e.g., social media, email, apps), with slightly higher general privacy concerns among U.S. respondents (*M*=3.27, *SD*=.98) than Netherlands respondents (*M*=3.18, *SD*=.89).[2] When it comes to the use of mobile phone apps, people in both countries reported a higher level of privacy concerns, with both countries reporting the same average score (*M*=3.94, *SD*=.77).

IPA data concerns and confidence

We asked respondents to indicate their level of concern for a list of statements specifically related to

[2] Both privacy measures and the IPA Data Concerns measure used five-point Likert-type scales for response options, with 1=Not at All Concerned and 5=Extremely Concerned.

IPA data collection. Sample items included, "My questions directed at the device are stored and sold to third parties (e.g., advertisers)," "The device is always listening," and "Other people might activate/access the device and trigger unauthorized purchases." Respondents in the Netherlands indicated slightly higher concerns compared to those in the U.S. (*M*=3.26, *SD*=.97 vs. *M*=3.11, *SD*=1.14).

Respondents in both countries reported very low confidence in their knowledge of IPAs and the data practices of IPA service providers (mean scores at or below 2 on a 5-point scale where 1=Not at all confident and 5=Very confident) when responding to four items, including, "I am confident these devices are secure and cannot be hacked or accessed without authorization" and "I am confident any personal information communicated to/from the device is protected by a privacy policy."

3.2 IPA Focus Group Research Details

Research: For the focus groups, we recruited both users and non-users of phone and home IPAs and varied focus group composition (some had all users, some had all non-users, and some had a mix). In the Netherlands, we held six focus groups with 35 participants. In the U.S., we held 12 focus groups (six at each institution) with 65 participants. Audio has been transcribed and in the Netherlands, analysis has become (U.S. analysis will begin this summer).

Based on focus group sessions from the Netherlands, the attitudes/themes that came up can be clustered into four archetypical users or type of concerns:

1. Unconcerned users – Trusting attitudes

> "I expect that Google is an organisation that **will not be hacked easily**. So what they store about me. I **expect that this device will be protected**, and not easy to hack." (Andreas)

2. Fatalistic users – Giving in to technologies

> " That's what I'm concerned about. It is not that you are in contact with Google, but what is that **third party** going to do with your data? And **how anonymous are your data**?" (Robert)

3. Critical users – Concerned attitudes

> " Yes, **I gave up** in the meantime. Because it is almost impossible to not share your location. So it is often switched on on my phone. You're being followed automatically, that's with eh, a tracker. So everyone knows where you are." (Dennis)

4. Sceptical non-users – Rejecting attitudes

> "If you choose consciously, you are **kind of in control**. However, I do question that for these things [smart speakers], what you said, okay, predictive behaviour and things like: You have to leave because there will be a traffic jam. That makes me think, won't we **serve technology that way in the end**?" (Jessie)

4 Next Steps: Evaluating Cross-Cultural Attitudes Toward Privacy and Surveillance

Differences between European and U.S. regulatory approaches to privacy have been well documented and analyzed. Broadly speaking, EU regulators embrace a more paternalistic approach to data protection policy including within the Netherlands, aiming to preserve a fundamental human right of its citizens through pre-emptive governmental action. In contrast, the governance of privacy in the U.S. follows a more reactive approach, often emerging only after some informational harm has occurred and taking the form of industry self-regulation or very targeted legislation.

These regulatory differences might lead to different approaches toward mobile privacy: the Netherlands focus on direct and pre-emptive regulation of the collection and use of personal data, prohibiting "excess" data collection and restricting use to the original and stated purposes of the collection, might cause Dutch persons to be more suspect of sharing data. The U.S. framework—where most data collection and use is considered both acceptable and beneficial, that restrictions should be primarily voluntary and non-invasive, and that regulation should only address documented instances of abuse—might lead Americans to be more willing to share data with technology companies and developers.

The qualitative results from the first phase of the research project on users' everyday experiences of mobile privacy will be systematically evaluated and integrated into the second phase, focusing on the development of a comparative cross-cultural survey of persons in the U.S. and the Netherlands to determine the broader social and cultural impacts of privacy with regards to mobile technologies.

To evaluate broader cross-cultural differences and similarities in attitudes towards privacy and surveillance within the three emerging mobile ecosystems under study the full research team will develop a series "privacy vignettes" for the survey. A factorial vignette survey methodology allows researchers to identify and compare individuals' privacy norms across contexts and cultures. Vignettes are used to address the ambiguity and the context dependence of the central concerns for this research. Within standard surveys, respondents may understand questions in different ways, particularly due to the abstractness of some of the concepts, their complexity, and potential cultural differences. Vignettes translate multidimensional concepts into tangible situations that allow respondents to better reflect on and describe their perceptions and values. Validation exercises during the first workshop will ensure that vignettes reflect the invited stakeholders' societal and policy priorities.