



THE LONDON SCHOOL
OF ECONOMICS AND
POLITICAL SCIENCE ■

They know everything: understandings of data privacy among teens in East Asia

LSE Research Online URL for this paper: <http://eprints.lse.ac.uk/104694/>

Version: Published Version

Online resource:

Bulger, Monica and Burton, Patrick (2020) They know everything: understandings of data privacy among teens in East Asia. Parenting for a Digital Future (29 Apr 2020). Blog Entry.

Reuse

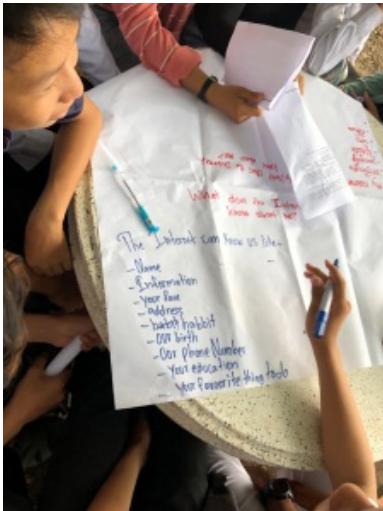
Items deposited in LSE Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the LSE Research Online record for the item.

'They know everything': understandings of data privacy among teens in East Asia



In this blog, we report on interviews with teens in East Asia, many of whom are urban poor. We asked what social media apps might know about them, exposing a broad spectrum of understandings of data privacy. This is the third in a [series of field dispatch reports](#) conducted by [Monica Bulger](#) and [Patrick Burton](#) in East Asia for UNICEF's East Asia and Pacific Regional Office in spring of 2019 [\[1\]](#).

At a school in Phnom Penh, ten kids squeeze around a single table. We're in the large schoolyard and about 200 younger children play around us, calling to each other, running around, climbing on tables, and tossing a ball that seems roughly half their size. Midday is sweltering and we sit under one of the few clusters of trees. When we speak about apps they use, the conversation is lively, with many children speaking at once. But when we ask [what social media apps might know about them](#), conversation stalls. "What do you mean?" one girl asks, leaning forward, pressed between two classmates. We clarify, asking what information they might have given the apps when they signed up. "Name," one answers, "telephone number," another volunteers.



We spread two large white sheets of paper and ask them to write down [other things apps might collect about them](#). "Location," "friends," "likes/hobbies" makes the list and then they stop. When we repeat this exercise with other groups from the same school, it is apparent that [most had not thought about what apps might collect about them](#). When asked why apps might collect information, a boy volunteers, "to check our age," and "to remind us of old posts."

A school for Somali refugees in Kuala Lumpur frequently changes location. Whether this is due to prejudice the children and their families endure, or whether because of limited finances is unclear. We visit during a sudden rainstorm, the tile street slick outside the second-floor school. In a narrow room with ten girls dressed in black hijabs, we talk about what information social media apps might collect about them.

First responses mirror those of all of our groups: name, age, gender, password. Then the girls start looking at their phones and debating what else is collected. Location is discussed, maybe some places but not everywhere? Do the apps know their home address if they haven't provided it? A 14-year-old Eritrean refugee writes "anything you post on social media, every single person's number, it keeps your history, videos, conversations, images, shopping online."

Asked why social media apps might collect information about them, a 17-year-old confidently answers, "For national security." Another responds, "For our protection." My facial expression must give it away, because the first girl says, "It's not?" The girls start talking, and there is confusion. They assumed the [apps were acting in their best interest](#) and any information they gave was for an altruistic purpose.

"Why would they want to know these things about me?" the 17-year-old asks. I suggest for commercial purposes and the conversation stops. We shift to talking about what social media apps do not know about them. The same girl says "That I am Muslim," she says she's never posted anything about her religion online. I look at her hijab, smiling wryly, and ask if she's posted photos of herself. She puts her hand to her head, returning the smile, and nods.



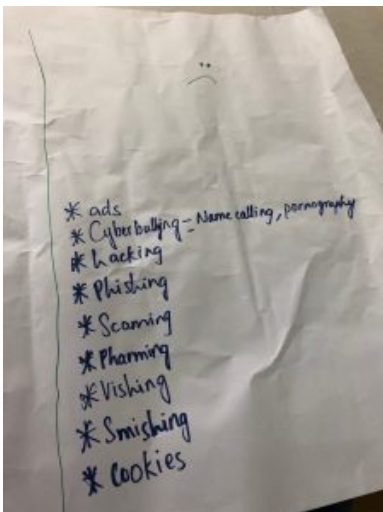
As a group, we take this new knowledge and turn it over. Is it [dangerous](#) for the apps to know so much? Probably not. They reflect on the reasons they enjoy social media, with staying in touch with friends and family in their home country the primary positive, followed by meeting new friends. The girls enjoy learning new things through watching videos about cooking, painting, crafts, gardening, and fitness. A few of the girls describe thinking the apps cared about them to provide all of these wonderful opportunities for free.

At a larger refugee school elsewhere in Kuala Lumpur, the teens have a much more sophisticated understanding of data privacy. [“Everything,”](#) one girl says, “Google knows everything about us.” A boy beside her leans forward and adds, “On your phone, they save all your data.

You’re in the hospital? Google knows already.” Another boy asks, “You know Facebook owns WhatsApp and Instagram?” as his classmates nod, he repeats the refrain “everything, they know everything.” Another boy says he changes the date and month of his birthday, but shrugs about whether this makes a difference, “Doesn’t know exact age, but almost same.” Another boy responds, “You can do that, but they already know the truth. They just let you fake it.”

Speaking over each other, the group calls out all that is known about them by their apps: “relationships, it can discover if you’re single,” “location, what school you go to... your high school,” “where you work, your occupation”. As a further description a 16-year-old boy clarifies, “most people lie about their occupation on Facebook, I told them I work at Facebook.” His classmates stop their writing to laugh together.

Their list of what data is collected about them rivals any expert’s list. Their list of potential negative experiences encountered online might even surpass most adults’ understanding.



This level of understanding is [not the norm](#). There is a spectrum of [awareness](#) around what information is collected and for what purposes. In our focus group discussions, understanding does not seem related to socio-economic status or even level of use. In most cases, older children were more knowledgeable, but not always.

The teens have advice for promoting privacy, but are not optimistic. A 17-year-old avid gamer and Pakistani refugee explains, “For Google and other websites, if you don’t log in with your email, they can’t save much about you. Most of the information that is collected is usually linked to your email, so that’s how they know who you are. Usually, you have to use your email for most things.” Before he finishes, his classmates respond:

“My Instagram email and my Facebook email are different.” “Do you know how many emails I have? Not just two!” “I think I have 5!” “I have two phone numbers, one I use for everything, one nobody knows!”

When asked what advice they would give to a younger sibling about protecting their privacy, a 16-year-old Liberian refugee says, “Honestly? I think if you expose them earlier and show them how they’re using it...if you teach them how to use it, there’s a lower chance of them experiencing problems.” A 16-year-old Rohingya refugee adds, “Sometimes they learn stuff. From YouTube, you can learn a lot of things.”

A 17-year-old Afghani refugee adds, “It has to be monitored by parents, so they can go and check what the kids are doing.” A 15-year-old girl sitting across the table nods, saying, “You can use it, but the parents just need to be involved.”

Caught amid global platforms with limited to no protections for vulnerable young users, and in national contexts where the rule of law is weak, there is an expectation of individual responsibility for data privacy without any actual transparency or ability to control social media platforms' data privacy practices. Most of the children participating in our focus groups, like their counterparts in the [US](#) and [UK](#) had internalised messaging from tech companies and [governments](#) that limit the liability of companies and expect the individual to protect their privacy, even though the platforms make information [public by default](#) and are [opaque about their data use practices](#).

Notes

*[1] Qualitative focus group interviews were conducted April-May 2019 in Kuala Lumpur, Jakarta, Phnom Penh, and Bangkok. 301 social media users aged 11-19 participated. We aimed to include marginalised populations often excluded from this type of research: 121 of our participants were urban poor and included children with disabilities, street children, refugees, juvenile offenders, children exploited in prostitution, and survivors of sex trafficking. We conducted focus group discussions in shelters and other places of care, and in middle and secondary schools, both public and private. Recognising the importance of community and institutions in a child's life, we interviewed 74 frontline practitioners in the region, including child psychologists and psychiatrists, social workers, counsellors, teachers, principals, and youth activists working with children. We additionally interviewed parents, grandparents, policymakers, and technology providers. Please see [our report](#) *Our Lives Online: Use of Social Media by Children and Adolescents in East Asia – Opportunities, Risks and Harms* for a full description of methods and findings.*

This post gives the views of the authors and does not represent the position of the LSE Parenting for a Digital Future blog, nor of the London School of Economics and Political Science.

Featured image: Teen Somali refugees write about what the internet knows about them during focus group discussion in Kuala Lumpur. Photos by Monica Bulger