EXAMPLE 1 – MIDS W231 FINAL PROJECT OUTLINE

COPPA provides regulations on the collection of information on children, that boil down to getting parental consent prior to a child's participation in a website or app. The goal is to avoid collecting personal information on children. But does it actually have any impact on what children disclose online? How actively are parents monitoring their child's online accounts and services?

I have three kids and I am concerned about their privacy online. But I feel like I am not doing a good job of policing their online data.

My kids have Kindles with child profiles that limit their permissions, requiring them to come to me any time they want to add an app. They also use my Android tablets to access games and websites online through separate profiles I set up for them. In both cases, there was technology in place to help me protect my kids' access to the internet and apps. So what's the problem? One big hassle with separate profiles on a single device is I am constantly hitting a space limit. I find myself having to uninstall or clean up data before I can install something new. The other issue with child profiles is I have to approve every app they want to use. This involves logging into my profile, finding the app in the app store, checking the permissions to see if I am okay with installing it, then going to the settings and authorizing their profile to use that app. And when one kid wants a new app, the other two will want to get a new app. It became too time intensive.

First, I stopped studying the permissions requested by the apps as closely. I no longer denied access even if it requested permissions that weren't required for the app to function as advertised. But eventually, even maintaining separate profiles because a hassle, so I started letting them use the main profile on the devices.

On our laptops, I never even bothered setting up separate accounts for them. For online accounts on websites like code.org or tynker.com, I had to enter my email address and confirm my child was allowed to have an account. I can go in and see my children's activity on these sites, but I never do. When my daughter wanted to Skype a friend, I didn't want to bother setting up an account for a child, even if it was possible. I used an alternate email address of mine and created a new account for her to use.

We read that people often act contrary to their privacy concerns online, either depending on the context, or to benefit from some cost savings or customization. How does this extend to our children? Are we more cautious with the privacy of our children?

I would like to create a survey to ask parents about their privacy concerns for their children's online data. Then I want to ask them specific questions about what access their children have to online platforms, and how much oversight they actually engage in. I want to see if they are circumventing COPPA regulations by just setting up accounts in their child's name with their own age and email address, so that the "confidentiality, security and integrity of personal information collected from children" section of COPPA isn't even applied.

And I want to explore the reasons they aren't safeguarding their children's privacy more. I suspect it is more because of the hassle of following good practices more than not being worried about the privacy of their children. If my suspicion is correct, I want to explore or propose technological solutions to make safeguarding children’s date easier for parents, without having to rely on each service provider.

My focus will be on children under 13, those for whom COPPA applies. Teenagers have a whole different set of concerns and issues, including actively trying to hide online behavior from parents. I want to focus on children who still need the help of their parents to access apps and websites. I also want to focus on children in the home, although there are a whole set of issues around data collected by apps children use at school and whether parents are adequately informed of such apps and provide consent. But that is beyond the scope of what I want to cover for this project.

EXAMPLE 2 – MIDS W231 FINAL PROJECT OUTLINE

Overview

India is often referred to as the world's largest democracy with a staggering population of 1.2+ billion people and in recent years India government has made it mandatory for every citizen residing in the country to obtain the Aadhaar Card.

What is Aadhaar?

Aadhaar is a 12-digit unique identification number issued to Indian citizens by the Central government. It is issued and managed by the Unique Identification Authority of India (UIDAI). The Aadhaar card is essentially an identification document issued by the UIDAI after it records and verifies every resident Indian citizen's details including biometric and demographic data.

Why is it important?

The Aadhaar database is one of the largest government databases on the planet. Can it become an all-pervasive tool? The opportunity created by having a single, secure identification for all citizens has led to rapid incorporation of the Aadhaar number into many aspects of daily lives. People can use their number to access government benefits, apply for a passport on an expedited basis, or collect their pensions. However, the use of Aadhaar is increasingly being made mandatory in a number of other, more mundane situations, such as the renewal of insurance policies, taking an exam in school, or even buying rail tickets.

Privacy Concerns

We will inspect the various privacy aspects, for example: Once the framework is in place, can it be changed or extended (e.g. recent addition of facial recognition)? What concerns have people raised about the universal collection and storage of centrally accessible biometric information? Does this normalize the use of biometrics? Will the existence of Aadhaar and the potential it creates to uniquely associate individuals to transactions erode privacy rights, lead to greater security, or both? (Cellphone operators are now required to link every SIM card to a verified Aadhaar number, so that all users of their services are uniquely identifiable, ostensibly to combat fraud and terrorism.) Vendors who operate terminals used for Aadhaar verification are required to collect metadata - it clear what is being collected, and how it will be used?

We will analyze the mandatory nature of such identification, and examine how the privacy concerns of citizens have been addressed. What protections are in place, and do they appear adequate?

Security Concerns

We will examine concerns about the use of a lifelong ID number, that is being requested by in an increasing number of everyday transactions. Who has access to the database, and how secure is it? Is there an opportunity for leaks, hacks etc? Could someone intercept or copy the number / thumbprint scan during collection or transmission? Is there a provision to update the information submitted on a later date?

Fairness and Transparency

Are there problems of excluding certain populations? There have apparently been issues with manual laborers, whose fingerprints have degraded. People who develop cataracts and are unable to afford treatment have trouble submitting to an iris scan. How do people establish their identity in the first place? Does it disadvantage people without documentation, or those in rural areas who have to travel? How will it impact immigrants, refugees etc? Are there examples where lack of an Aadhaar number has led to discrimination or the deprivation of a person's rights? Even if provision of a number is not legally mandatory, does widespread use eventually make it impractical for people to try to withhold it in some circumstances?

Legal Aspects

We will inspect the legal validity of this scheme, including recent challenges through the courts. The original intention of Aadhaar was to underpin the disbursement of welfare to the underprivileged, but certain language was included that allowed private companies to request the number in order to establish identity (Section 57) - this has led to increasingly widespread use and given rise to some interesting legal debates that we could explore.

EXAMPLE 3 – MIDS w231 FINAL PROJECT OUTLINE

The W231 Privacy Policy Assignment enabled students to explore the privacy policy of one service that they use frequently, understand its scope, conduct user testing, determine whether they align with standards, and consider any ethical or legal issues. However, it was difficult to gain perspective and understand the document in relation to others because only one document was the focus. After selecting a service's privacy policy and looking into previous versions from that service as well as privacy policies from related services/platforms, I became curious why particular revisions were made and I was more interested in understanding in how policies for related services also evolved. This proposed project is an extension of the previous assignment that aims to identify similarities, differences, and general trends for privacy policies over time as well as across multiple sites in a few domains.

Ideas / Action Plan

- Select top sites in a few domains (e.g. news, social media, online retail) and explore common trends for the latest privacy policy versions

o Examples include font (via online detection services), color scheme for text and background of main area where privacy content exists (grayscale/B&W, uni-, bi-, tri-, multi-color categorization), layout, navigation, readability, and comprehension

o How does this differ from older versions of the privacy policies? How many previous versions are easily accessible (e.g. CNN.com requires googling previous versions, whereas Reddit has links on the main privacy page)?

- Compare & contrast across domains with specific questions, including:

o Does one domain (e.g. social media) dedicate a larger or more comprehensive section to how information is being used than another domain, such as online shopping platforms?

o What is the average number of textual examples per domain? How about images, tables, or charts?

o Which domains provide better privacy policies according to existing standards (e.g. CALOPPA) as a whole? Which domains score the highest for specific parts (e.g. readability)? User testing may be required.

Outline

- Introduction

o Addressing the purpose of a privacy policy document, what it typically contains, and what constitutes a "good" privacy policy document by current standards.

o Rationale for project topic (primarily extension of previous assignment for added perspective, standard/theory vs. practice) o Results teaser

- Methods

o Reasons for choosing most popular sites (as opposed to random sites)

! List + links of selected sites + previous policy versions in Appendix

o How were trends identified and adequately compared when there are differences in publication dates? If comparing year-to-year, should the middle date for each available year be taken, the last date, or the closest possible to others in the domain?

o How was user testing conducted? What questions were asked?

- Results

o What were trends in privacy policies across domains & over time with respect to font, color scheme, layout, navigation, readability, and comprehension

o Domain specific questions (see Action Plan section)

- Discussion

o Limitation: regardless of the findings, generalizing to the domain-level only applies when considering “top sites.”

! Preliminary belief: due to the high number of visitors and/or usage, it may be that top sites (especially older ones) may have more resources and/or more at stake to ensure they have an exemplary privacy policy. Greater generalizations can be made after examining random sites, but these may not be as mature or be able to spend as many resources to focus on developing, testing, and maintaining stellar policy pages that adhere well to existing standards.

- Conclusions