



DECEMBER 31, 2019

CRITICAL CHALLENGE PROJECT
CHILDREN'S PRIVACY

GULSEN SAFFEL
BROWN UNIVERSITY
EXECUTIVE MASTER IN CYBERSECURITY '2020

TABLE OF CONTENTS

Introduction.....	2
Challenge Statement.....	3
Approach.....	7
Next Steps.....	9
Bibliography.....	12
Appendix.....	13

INTRODUCTION

We are challenged by the continuously and exponentially diminishing privacy of children.

In this paper, the diminishing privacy of children is deliberately called a “challenge”, but not a problem. A problem implies a clearly negative circumstance to be resolved. However, a challenge represents a new state, perhaps as a result of change in the norms in this case. A challenge presents opportunity for positive outcome, but also complexity and dilemma to be unraveled first.

“We” refers to the group of people who must acknowledge this challenge and act. “We” starts with anyone in a parent role. Parents set the tone and execute most of the early privacy practices for the children. Parents are also carefully observed by children, for how they treat their own privacy. “We” then captures every adult who is a family member, teacher, neighbor, or friend’s parent. Finally, “we” includes any decision-maker on the business or regulatory conduct of children’s information and privacy.

Discussing children’s privacy challenge is very important. If we do not act with urgency, information, conscience, and firm intention the challenge is rapidly headed to become a problem for arguably the most vulnerable, and loved at the same time, people in our lives - the children.

This project aims to discuss children’s privacy, trigger thought, a little bit of guilt, but ultimately make a difference through action. This project aims to deliver a simple empowering source of information for parents and others to raise children who are informed and intentional about managing their own privacy.

THE CHALLENGE STATEMENT

Technology-fueled innovations and trends have inevitably changed our lifestyles, habits, and norms at a pace faster than any previous generation has experienced. We have become the society of “now” and “going viral”, to name a couple. We want information, at our disposal and at all times, and we generate it for others too.

The ways we communicate has changed. In just a couple of decades, children’s communication expanded from using a shared home phone to a dozen social media platforms. We know how quickly cellphone-ownership went from being a luxury to a necessity – due to change in what we consider “necessary”. What about the continuously dropping age to own a cellphone? Elementary school children are wearing trackable watches and sporting cellphones nowadays, and these devices are more capable than ever.

We have also witnessed that the original intention can become irrelevant and the innovation could be used for anything, including “harm” – harm being an undesired consequence for at least one of the parties. For example, Jeremy Hsu from Wired published that Fitbit device data could be used to create a heatmap of critical US military personnel (Hsu, 2018).

Most recently, NBC News reported about a mother installed a Ring camera with the intention to better monitor her daughter. But a hacker accessed the camera and caused a very scarring experience for the family, and importantly the child. (Burke, 2019) Any parent with some understanding of crimes against children can imagine that this incident could have gone worse, if the hacker was sexually or financially motivated.

The picture for the challenge would not be complete without highlighting the exponentially increasing value of any given bit of data. In 2017, an Economist article covered mathematician Clive Humby's quote from 2006, that "*data is the new oil*" (Parkins, 2017) – his vision took years to resonate with the world. It is hard to argue otherwise today; data runs the modern day, empowers those who have it, and rewards those who know what to do with it. For that reasons, companies are eager to collect as much data as possible about their current and prospective customers, fueling the engines of marketing, business development, technology, and operations functions. The maturing field of artificial intelligence now enables once-implausible capabilities. Gigen Mammoser's Healthline article reports that artificial intelligence capabilities can diagnose skin cancer more accurately than doctors. (Mammoser, 2018) Such development is only possible with abundance of data – "the oil" companies are after and the current society is generously sharing. It is only natural to wonder in this case, "what else is possible?" Could someone's childhood pictures be used to identify hereditary or intellectual traits about them, so that important future decisions are already made for the children such as their education or health benefits?

The connectedness offered by innovative solutions is very hard to resist. In fact, the more we resist to adapt, the more isolated and inconvenienced we might find ourselves. Because for every report of an unintended-consequence story for Fitbit or Ring, there is at least one with a happy-ending. We realize the change is inevitable, as Viktor Frankl says: "*when we are no longer able to change a situation - we are challenged to change ourselves*". So, we adapt and find out the conveniences we get are not without a cost.

The dynamic explained above is already quiet challenging to navigate for adults. Many adults have the advantage of matured judgement, mostly private past, and some skepticism that was part of

their initial resistance to change. They know what it was like “without it” but now they also see how convenient things can be “with it” and many times they can weigh the costs vs. benefits.

Children, on the other hand, are born into a lifestyle that is densely populated with solutions that are monitoring, alerting, tracking, and recording them. Their lives are very well-documented from the very beginning. Because a robust digital trail has been initiated by the adults, well before the children can agree to or even understand the permanency and the potentially negative consequences.

We have to consider the impact of our choices, changes, and actions on their privacy because, most of the time, the impact is permanent. As a result of our even well-intended actions children may have their information all across the internet that they may never be able to recover. Something as simple as sharing the joy of new parenthood with the world results in potentially valuable childhood records splattered across the internet, permanently. The pride, love, and excitement cause the parents commit serial “*sharenting*” (Wikipedia, 2019) - the act of sharing too much information about children and often. Moreover, the tone parents set, and the diligence they apply to protect their children’s information is likely mirrored by the extended family, friends, and other adults in the children’s life.

General lack of understanding of technology is a challenge. The gap between what the “average Joe” thinks technology can offer to diminish his privacy and what is really possible is growing at an incredible pace. Without understanding the extent and consequences of sharenting, it is hard to develop an urge for action. Also, the overall diminishing sense of privacy in the society is also contributing to the challenge. What is considered unacceptably-exposing to one person today, can be “in” overnight with a single viral act of a celebrity or a YouTuber. Therefore, we might find

ourselves justifying actions simply by the actions of others, even if it is not the best decision when we think of it in isolation.

Children's sense of privacy and habits are first developed by their observations of those around them and it is very important that they learn how to guard *their own privacy*. The consequences we see are already saddening. Children develop anxiety and other mental issues and feel isolated, because loss of privacy can easily make them the target of bullying, blackmailing, or stalking. The Netflix show "13 Reasons Why" covered real-life inspired stories of children committing suicide, experiencing sexually assault, and attempting mass school shooting. They could be kidnapped, or targeted by pedophiles much easier if their information is so readily available. Criminals store and trade very private information children locked in the darkness and the depths of the internet. Extremist groups are hunting for recruits on the internet, and children are not off limits. Sometimes it is years before children realize their identity has been stolen and they start their financial life with the burden of a damaged credit. The information revealed about them could be used to discriminate against them in school admissions, healthcare benefits, housing or financing decisions. The list can grow longer and even more grim. What we know about the evil today is bad, but what we don't know yet could be even worse.

Bottomline, "we" have a responsibility to acknowledge the challenge regarding children's privacy and act. Because, by now almost all of us have experienced at least once, the sense of fear, loss, and even anger, when we found out our privacy was violated in some form.

APPROACH

This project focuses more on raising awareness about the unintended and harmful consequences of information sharing. It does not aim to encourage an entirely off-the-grid life for children. In today's conditions, we must accept it is unrealistic, isolating, and exhausting to manage for both the adults and the children. The project aims to trigger thought and then action.

First, this project aims to recalibrate the thinking about ownership of privacy and information sharing. We, as parents and other adults, do not own the privacy of children. If the information sharing has permanent impacts on the children's privacy, our role is more like a transitional agent or a guardian. Therefore, this project will boldly and maybe controversially highlight for responsible adults "*Children's Privacy is Not Yours to Share*". We must acknowledge and prepare ourselves and the children to the transition of the reigns to their own privacy – and it happens at single digit ages.

Next, this project aims to trigger self-awareness. We should not consider our own privacy decisions to be independent from that of the children. First, such habits are observed and mirrored by the children. If kids see us constantly snapping pictures and sharing on the social media, they will consider that behavior as "the normal". Second, our information could lead to data about the children too. Taking a commercial DNA test such as "23 and Me", leads to very private information about the children. Eric Rosenbaum's article covered the risks of DNA tests such as the challenges of security, lack of regulatory protections, and the permanency of potential damage from losing something so personal that cannot be changed, the DNA data. (Rosenbaum, 2018) The project will encourage taking a good hard look at our own privacy and information sharing habits

thinking about the known and to-be-discovered consequences of information sharing. Key is to determine the right balance and tone to model for the children and behave consistently.

Learning about the subject of children's privacy and determining a consistent approach is key to making informed decisions for ourselves and for children. However, for anyone who is not working in an information security related field, the amount of information and technical jargon can be overwhelming.

This project aims to curate content from various sources and deliver actionable messages in simple language. Goal is to spark privacy consciousness for children, offer small steps, and eventually drive intentional sharing of information of any sort and for anyone. Success looks like ripples of small improvements across friends and families in sharing habits. Because children will learn mostly through observation and take charge of their own privacy much sooner than we think or anticipate.

NEXT STEPS

This project will leverage two communication channels – a blog and a presentation that can be taken to schools to share with educators and parents. Also, social media accounts should be used to spread the word on the activities.

The articles in the blog have to be easy to consume – both in length, language, and content. Every article should be short and sweet, written in a simple yet punchy language, and close with a suggestion for a healthy habit. Momentum, consistency, and persistence are key to success of the blog. Articles should cover real-life cases followed by relevant information and suggestions so the readers can understand “the why” and find actions applicable to their own circumstances.

The blog is going to clarify that the subject matter expertise is not centralized and there is no one right answer to children’s privacy. Children’s privacy is a balance to strike for every parent, and every child. It is a journey to be taken one step at a time, adapting to changes around us.

Blog aims to deliver research and collaboration to offer synthesized information to educate parents, so they can decide what fits them. Goal is to inflict intentional sharing of information and developing healthy habits.

Blog articles will also highlight the importance of being proactive, and focusing on preventative and protective measures than to rely on law and other clean-up or recovery efforts. Any regulatory protections may or may not offer a direct remediation to the impacted children. Besides, the consequences are mostly permanent, may never be possible to correct the damage at all.

The blog will be a platform to bring in opinions from others who also care about the subject, and have relevant knowledge, expertise, and experience. Contributions could be from hackers, security experts, lawyers, journalists, and EMCS cohorts.

The blog URL is www.Privacy4Children.org.

Gaining and Keeping Momentum

Goal is to publish 1-2 articles a week. A few of the posts are attached in the appendix.

Once enough content is posted, I would like to start spreading the word through social media.

After the blog gains some momentum, focus will shift to preparing a 30-minute presentation to be shared with schools and other similar platforms. The agenda of such session would be very simple and include:

- Outline of the Challenge
- Current and relevant examples (i.e. Ring Camera, Facial Recognition, Identity Theft)
- Small Improvement Ideas
- Open Discussion / Q&A

Presentation will aim to deliver similar messages in a different, more conversation-based format. Ultimately, the goal is to invoke sparks of thought that different people have different appetites for information sharing, and no adult should make assumptions on the information of other children such as taking the picture of someone else's child and posting on the social media without consulting his/her parents. Another possibility is to bring a hacker friend to set up a "Pineapple" in order to add shock factor through demonstration.

There are endless options to expand upon, but approach will be to start with the blog, accumulate some reader base, and then refine content and start the talks with local schools. Eventually

generating YouTube videos or interviews would also be an addition for those who are more “watchers” than “readers”. This topic can be discussed in relevant privacy and security conferences as well.

BIBLIOGRAPHY

- Burke, M. (2019, December 12). *NBC News*. Retrieved January 2020, from [www.nbcnews.com:
https://www.nbcnews.com/news/us-news/man-hacks-ring-camera-8-year-old-girl-s-
bedroom-n1100586](https://www.nbcnews.com/news/us-news/man-hacks-ring-camera-8-year-old-girl-s-bedroom-n1100586)
- Flender, S. (2019, February 10). *Towards Data Science*. Retrieved January 2020, from [www.towardsdatascience.com: https://towardsdatascience.com/data-is-not-the-new-oil-
bdb31f61bc2d](https://towardsdatascience.com/data-is-not-the-new-oil-bdb31f61bc2d)
- Hsu, J. (2018, January 29). *WIRED*. Retrieved January 2020, from [www.wired.com:
https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/](https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/)
- Mammoser, G. (2018, June 11). *Healthline*. Retrieved January 2020, from [www.healthline.com:
https://www.healthline.com/health-news/ai-may-be-better-at-detecting-skin-cancer-than-
your-derm#1](https://www.healthline.com/health-news/ai-may-be-better-at-detecting-skin-cancer-than-your-derm#1)
- Wikipedia. (2019, September 29). *Wikipedia*. Retrieved January 2020, from [Wikipedia:
https://en.wikipedia.org/wiki/Sharenting](https://en.wikipedia.org/wiki/Sharenting)

APPENDIX

Blog Post 1: Internet of Toys

Think about the toys most children play with nowadays, how many of them are connected to the internet? How many of the games they play are from a connected device? How many of these games allow children to play with others they meet on the gaming platform?

You are probably scanning through all the toys and games in your household, wondering which ones are connected right now. Think about how many of them have required you to create an account associated with your child, potentially sharing the name, birthday, gender, and even more information? How many of them have requested a profile picture, camera access, microphone access? How many times did you click through long texts “accepting” terms?

I want to give you a straightforward example, and you know there are more grim stories on the internet if you look for it. I just want you to see that it is so easy to risk our children’s privacy, even with the best of intentions. [In 2017, Lee Mathews covered the story of CloudPets leak](#) – please read it.

Do you know what data is collected during the setup? What is being continuously collected during use, and what happens to it? What are their data-sharing practices, for operations or for-profit? Can you control any of the sharing?

It is not possible to avoid connected toys or devices altogether, for children's entertainment or education. What is possible is, using them with caution. I want to give you some simple tips to keep in mind when purchasing, setting up, and using a connected toy or device.

- Read the privacy policy, look for answers to some of the questions I laid out above. Find out how the information is collected, used, shared, and what can you do about any of it? Are there settings you can limit the sharing of the data for profit or further marketing communications?
- Ask, does the device/toy need to be connected at all? Just because it can, doesn't mean it has to be. After setup, does it have to stay connected?
- Consider powering off the devices every once in a while, or disconnect when not needed. If there is a software update offered, do not delay, update right away.
- If you have to create an account, avoid usernames and passwords that give away information like name, last names, birthdays, pet names, etc. Think about the times it would be okay to be less transparent with your child's personally identifiable information? I am going to post separately about password and browser security tips, please look for it.
- Understand the extend of communication possible with others on the platform. Can they create and share information- in form of text, picture, video, or voice recording?
- Google. We google for all of our questions, then use Google to read about the product. Not to horrify yourself, but to inform yourself of the uses and the risks of such technology. Think about how someone could get around some of the factors you think you can control? Because kids will, intentionally or unintentionally.
- Talk about it with other parents. At school, at birthday parties, in group texts. You are always in touch with other parents about anything. Talk about this too, share thoughts, research, experience, and best practices. Spreading awareness is the best

- **DO NOT PANIC.** It is normal to be shocked with what you learn when you take the time to learn these things. Please do not overreact to your children, as a knee jerk reaction, while they are having fun with it. They are unaware of what you know and what you imagine. Remain calm and share what you learned, why it matters, and why you have to make some changes based on that information. It is very important that children understand where some of our decisions come from, so they can hopefully multiply the thinking in similar situations. It could be productive to explain how you will change some of your habits based on this situation too, so the children don't feel that they are the only ones impacted.

To sum up, parents, please do not blindly buy, setup, click on a series of accepts, and not monitor what happens with the connected toys or games. Take your time to read about the products, and risks, privacy policies, and understand what data is generated, stored, shared, and do not give in if anything seems to be an excessive amount of sharing or permissions.

Blog Post 2: Basics for Parents: Password Security

In this blog, I will focus on topics that directly concern children's privacy; however, every once in a while, we have to talk about security and privacy basics for parents too. Because you cannot protect your children's information if you cannot protect your own.

How many online accounts do you think you have accumulated over the years? Potentially hundreds. It is unrealistic to think we will remember every username and password combination (that we remember to own). So, we do a few things hackers love, such as setting short passwords,

reusing them, or never changing them. We are all guilty of one or a few of the things here. It's okay, that's why we are here.

Here are a few things to consider while managing your online accounts:

Avoid creating usernames and email addresses that include your information: name, last name, birth date, and other details that are useful for breaching your account.

Avoid short and simple passwords. They are easy to remember and quick to type. If your password has something like password1, abc123, 123456, qwerty, you have just picked yourself one of the most popular passwords THAT HAVE BEEN BREACHED over and over again. (You can read this article from CNN: [How hackable is your password?](#))

Never write down your passwords, anywhere... I saw this in too many "great gifts" lists, so I have to call out: A password notebook/organizer is a TERRIBLE gift.

Avoid reusing usernames and passwords. At times the username will be your email address, unavoidably, but exercise this especially for your passwords. Shared password means, if one account is breached, a hacker would have immediate access to your other accounts too.

Consider using a password manager, like 1Password or LastPass, to create long, complex, and unique passwords. Most devices include one, like the Apple KeyChain. I encourage you to Google "best password managers," read about them and pick one that is best for you.

Avoid sharing accounts and passwords with people you love and trust. Please don't gasp at this – it is for your protection and theirs.

Avoid password remembering functionality if you are on a device that doesn't exclusively belong to you. I would go as far as suggesting the same on your own devices too, but I am aware that it is too much convenience to let go.

Please do not type your password anywhere other than where it belongs: the website account login page. I am aware of websites that may ask for to link accounts. If you are not particularly security-savvy, look for an alternative way or call customer service to validate accounts. This way, you never have to decide when it is an authentic request, and when it is not.

Do not share your password via email or over the phone, even if you are convinced that it is a legitimate request. Ask for an alternative way, and do not give in. No company that cares about your security will ask for this information through anywhere other than its login page.

Change your passwords – change them when you get a default password assigned to you, no matter how long or complex it looks. Change your existing passwords, especially important ones, as often as you can.

It is okay to permanently delete accounts you don't use. You may think it is no harm to keep, but it is your information in the company's systems that has to be protected. Does it matter which company loses your credit card number, bank, or your favorite merchant? It is okay to cut down the number of accounts that "know you" and request the deletion of your data if it is offered.

Parents, I am fully aware this can take a lot of your time to improve. But I can assure you, it is still less time (and money) than recovering an important account, your identity, or credit line if breached. Your breached accounts could lead to loss of your children's critical information, such as SSN, and it is much harder to catch. Please do invest time to make improvements on this topic, so your children are not impacted, directly or indirectly.

Blog Post 3: Facial Recognition

I am going to cover our social media habits and impacts on children in a separate post, probably in many posts. Before that, I want to share a recent breach that can help you understand WHY I am going to make a big deal out of children in social media.

Have you heard of a company called Clearview AI? This company collected billions of pictures from the internet and created a facial recognition capability by using Artificial Intelligence.

Professor Freedman discussed this on her blog just last month, and here we are hit with the news that the company has been breached. CNET covers the story here, please read this. Please do not take it lightly where the journalist is pointing out that this company “has a database of 3 billion photos that it collected from the internet, including websites like YouTube, Facebook, Venmo, and LinkedIn.”

This is a big deal, and I want to leave you with a few things to chew on concerning this breach:

This is not the only company you have not heard of that scrapes the internet collecting pieces of information about you and monetizes it.

This is by no means harmless. Your information is now in hands you didn’t intend it to be.

“I have nothing to hide” is a dangerous thought. A single photo or post may be benign, but you see companies can scrape the entire internet. Do you see the potential that one day, someone else will know about you more than you do?

Artificial intelligence is in its infancy, and it can already do more than most of us understand.

Parents, I know you have heard “whatever you put on the Internet, assume it is permanent.” It is not only true, and now may be incomplete. I suggest, “whatever you put on the Internet, assume it is permanent, and you don’t know how it could be used for or against you.”

I look forward to hearing your thoughts on this.