"Step Big Brother"- Corporate Surveillance

TECH GIANTS SURVEIL & DATA MINE CHILDREN FOR PROFITS: GOOGLE & APPLE MAY BE VIOLATING FTC CHILD PRIVACY LAWS!

BY REX M. LEE

This document includes data that shall not be disclosed by the requesting party, and shall not be duplicated, used, or otherwise disclosed—in whole or in part—for any purpose other than to evaluate this article & analysis unless otherwise approved by Rex M. Lee. The contents of this document shall be protected as Rex M. Lee Proprietary unless otherwise approved for release by Rex M. lee. The information, data, and graphics subject to this restriction are contained in all pages of this document.

Tech Giants Surveil & Data Mine Children for Profits:
Google and Apple May be Violating FTC Child Privacy Laws!
By Rex M. Lee

My daughter brought to my attention that the high school she attends forces the students to use intrusive Google apps plus Gmail (Google) which could be considered "forced participation" regarding predatory surveillance and data mining business practices employed by Google.

My daughter expressed concern that schools are enabling Google to data mine students via Gmail plus Google student-centric apps such as Google Classroom, Google Docs and Google Family Link for Parents.

All of these Google student related apps are distributed through Google Play plus the Apple App Store (Google Classroom).

I decided to do a deep dive on the app permissions that support Google Classroom, Google Docs, Google Family Link for Parents and the Gmail app that supports Gmail.

As I've been reporting for The Epoch Times, apps that support smartphones, tablet PCs and connected products are nothing more than legal malware that enables the app developer to monitor, track, and data mine the product user for financial gain even at the expense of the user's privacy and safety.

Regarding the predatory surveillance and data mining business practices employed by Google, it is no surprise that the Google student-centric apps are in fact malware that enables Google to surveil and data mine the product user for financial gain which includes teachers, teens, and children.

This is no surprise since Google's business model is based on Surveillance Capitalism which many parents and educators need to understand.

What is surprising is the fact that school districts nation-wide are adopting intrusive technology such as Google apps enabling companies such as Google to surveil and data mine students that could include children under the age of 13 which could be a violation of child privacy laws.

Surveilling and data mining children for financial gain under the age of 18 is bad enough much less children under the age of 13 which could be a violation of the FTC Children's Online Privacy Protection Rule ("COPPA"- https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions).

Understanding Surveillance Capitalism 101

Before we examine COPAA compliance to see if tech giants such as Apple and Google may be violating FTC COPAA compliance, let's review the app permissions that support Google Classroom, Google Docs, and Gmail which students at my daughter's high school are being forced to use without parental consent.

Google Classroom, Google Docs, & Gmail App Permissions- Distributed by Google Play and the Apple App Store (Google Classroom)

RML Business Consulting, LLC All Rights Reserved- 2019

The Google Classroom App is marketed to students and teaches as a way to connect the student and the teacher to support activities such assignments and homework. Below is the actual description of how the app works from Google Play:

- "Classroom is a free service for schools, non-profits, and anyone with a personal Google account. Classroom makes it easy for learners and instructors to connect—inside and outside of schools. Classroom saves time and paper, and makes it easy to create classes, distribute assignments, communicate, and stay organized."

Like Google Docs and Gmail, Google Class Room is another free application that provides convenience but is the app really free?

Is Google a non-profit company that spends millions on R&D to develop "Free Stuff" that they give away to the public?

Of course Google is not a non-profit. Google loves profits especially when it comes to surveilling and data mining their product users for financial gain after all Google's intrusive business plan is based on Surveillance Capitalism which means that companies such as Google monetize their product users such as you.

Like Apple, Microsoft, Amazon and Facebook, Google views their product users as *"uncompensated information producers"* whom are to be exploited for profits at the expense of the user's privacy whether the user is an adult, teen, or child or in this case a teacher or student.

By way of the Google student-centric apps, Google is enabled to collect a lot of valuable sensitive user data known as a person's digital DNA which is the most valuable commodity on earth.

Why do you think that Google and Apple are some of the most valuable corporations on earth? Is it because they give away "Free Stuff"?

No of course not, these companies have become some of the most valuable companies on earth by profiting off of the use of their operating system ("OS") product user's personal and professional digital DNA which includes surveillance data (e.g. location data) and sensitive user data.

Understanding Intrusive and Exploitive Apps 101

Now that you understand Surveillance Capitalism let's understand how intrusive and exploitive apps work.

Exactly how much personal and professional digital DNA does the student-centric Apps enable Google to collect, use, share, sell, and aggregate for financial gain?

The Answer: "A lot according to my analysis of the app permissions associated with each student-centric app."

The collective student-centric android apps are granted many intrusive application permissions per app enabling Google to collect highly confidential personal and professional digital DNA from the student and teacher who uses these apps.

RML Business Consulting, LLC All Rights Reserved- 2019

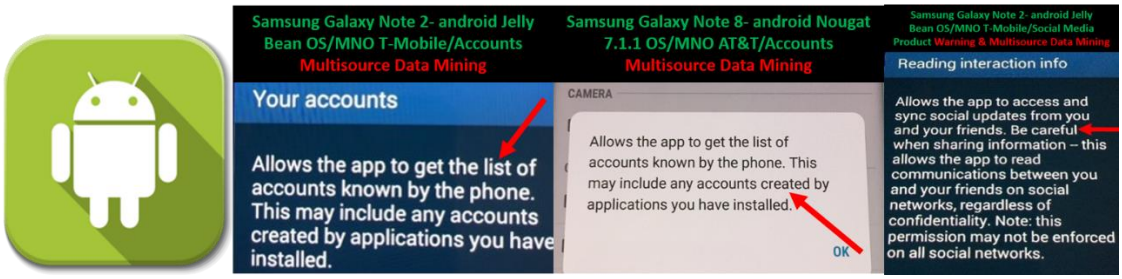
I will highlight only a few of the app permissions associated with Google Classroom, Google Docs, and Gmail plus other android app permissions that are relevant to the use of android apps in general:

- **Identity**- This gives Google access to Accounts set up on the device which would include smartphones, tablet PCs and other connected products that support the app including PCs.

  Access to accounts means that Google can collect information on any account set up on the device such as banking, medical, social media, personal accounts and other highly confidential account information.

  Don't take my word for this claim, read a few of the android application permissions associated with access to accounts, social media accounts, contacts and user identity of which these types of permissions are associated with apps such as Google Class Room App, Google Docs, and Gmail (App):

  Android Account Application Permission Statement. *"Allows the app to get the list of accounts known by the phone. This may include any accounts created by application you have installed. This means non-Google applications as well."*



- **Android Social Media Account Application Permission Statement & Product Warning.** *"Allows the app to access and sync social updates from you and your friends. Be careful when sharing information- this allows the app to read communications between you and your friends on social networks, regardless of confidentiality…."*

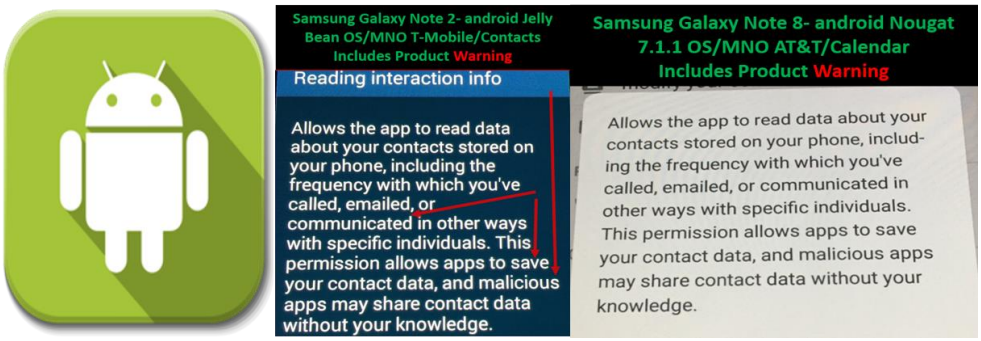
  Regarding the collection of messages from social media apps, note that the android social media app permission is an example of how much information Google can collect from a social media account even social media accounts that are not associated with Google products such as Facebook, Twitter, Instagram, LinkedIn and other accounts.

  The amount of personal and professional information Google can collect from an account set up on the device is astonishing and concerning to say the least.

  Potential Violation of Medical Information Laws (HIPAA). Parents need to consider that teens and children may have apps associated with their healthcare providers on their smartphone of which are considered accounts. This means that Google and other app developers can access medical accounts by way of preinstalled and third-party apps such as Google Classroom.

RML Business Consulting, LLC All Rights Reserved- 2019

- **<u>Android Contacts (Electronic Address Book) App Permission Statement & Product Warning.</u>** *"Allows the app to read data about your contacts stored on your phone, including the frequency with which you've called, emailed, or communicated in other ways with specific individuals. This permission allows apps to save your contact data, and malicious apps may share contact data without your knowledge."*



The contacts application permission not only allows Google to collect the user's electronic contact address book but also enables Google to surveil the app user by tracking how the student communicates with their family, friends, teachers and others by phone, email and other ways such as text messaging or instant messaging.

<u>Violation of Consumer Laws Governed by the FTC and State AGs- Hidden Product Warnings.</u> Like the android social media account application permission statement, the contacts app permission statement also contains a product warning that is hidden from the app user which I believe is illegal according to existing consumer laws governed by the FTC and state AGs which should be concerning to parents and educators.

"Should adults, teens, children, students and teachers be using intrusive and exploitive apps that are supported by hidden application product warnings?"

<u>Deceptive Trade Practices- Illegal Terms of Use</u>. Educators and parents should be highly concerned in regards to intrusive and exploitive apps that are supported by hidden application product warnings that are not published online within T&Cs, privacy policies or end user licensing agreements ("EULAs").

Hiding application legalese and app product warnings I believe is illegal according to existing consumer laws.

It is clear that Google, Apple, and Microsoft are taking advantage of the fact that parents, students, and educators do not understand the terms of use that support intrusive and exploitive apps such as Google Classroom.

- **<u>Android Personal App Permission Statement- App Developers can Identify App Users!</u>** *"Allows apps to read personal profile information stored on your device, such as your name and contact information. <u>This means apps can identify you and may send your profile information to others</u>."*

RML Business Consulting, LLC All Rights Reserved- 2019

Deceptive Trade Practices- Personal Identity. Like other people who are under the impression their identifiable personal information associated with products such as smartphones and table PCs is protected by companies such as Google, you have been deceived as the android personal information app permission confirms.

Regarding the Facebook and Google congressional hearings in 2018, Mark Zuckerberg, Chairman/CEO of Facebook and Sundar Pichia say that Facebook and Google do not sell or share identifiable personal information to third-parties such as data brokers like Cambridge Analytica.

However the hidden android application permission statement above confirms that app developers such as Google and Apple can identify the app user plus forward the user's identity and contact information to "Others".

"Others" sounds like third-parties to me. Educators, Parents, and Students should be highly concerned that apps enable app developers to identify the app user which includes children under the age of 18 and 13 which would be a violation of FTC COPAA compliance (see enclosed info for details).

Harmful Use of a Child or Student's Personal Information ("digital DNA")

Telecom providers such as AT&T, Verizon, T-Mobile, and Sprint were in the news recently regarding the sale of their paying customer's location data to data brokers such as Zumiga and Locationsmart* who used the information in a harmful manner.

** Source Business Insider- June 2018: https://www.businessinsider.com/verizon-att-t-mobile-sprint-will-stop-selling-smartphones-location-data-2018-6/#verizon-1*

Over the past two years there have been numerous reports of abuse, negligent, and harmful use of personal and professional information by tech giants that include Google, Apple, Facebook and other tech giants.

For example**, some of the reports include the Facebook Cambridge Analytica scandal, Apps share personal info with Facebook and Google forgetting to tell Nest customers that secret microphones are embedded in their products, and the list goes on.

RML Business Consulting, LLC All Rights Reserved- 2019

***Source Wall street Journal- Feb 22nd, 2019: https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636 Source C-Net- Feb 20th, 2019: https://www.cnet.com/news/google-calls-nests-hidden-microphone-an-error/*

- For more details regarding harmful use of personal and professional information by telecom and tech giants, read my article, "*Smartphone Surveillance & Data Mining: Who is Protecting Us*", published by The Epoch Times.

After numerous examples of abuse, negligent, and harmful use of personal and professional information, where is the FTC and state AGs when it comes to enforcing existing consumer laws?

The question that the FTC, state AGs, law makers, parents, and educators need to ask at this point is:

"Is Google using student and child personal information acquired from apps such as Google Classroom in a manner that can bring harm to the child or teacher?"

People tell me all of the time, *"I'm not a terrorist or breaking the law so I don't care if Google is surveilling and tracking every aspect of my personal and professional life."*

This is the worst statement regarding a person's privacy of all time.

Per the telecom Zumiga/Locationsmart and Facebook Cambridge Analytica scandals, companies such as Google sell access to their product users to data brokers such as Aleksandra Kogan.

Mr. Kogan an innocent looking Facebook survey app that enabled him to surveil and data mine millions of Facebook users for financial gain and then sold the Facebook user's personal and professional digital DNA to Cambridge Analytica who exploited the user data for financial gain at the expense of the user's privacy and safety.

This means that personal and professional digital DNA acquired by apps such as Google Classroom could end up in the hands of data brokers, employers, state actors, institutions of higher learning, law enforcement, insurance and bank underwriters, and other entities that could bring harm to the user such as student or teacher.

Google Exposes Children to Child Predators.*** Another example of online harm by way of an app is the recent story regarding the fact that YouTube continually poses harm to their users including children such as the case involving child predators who engage children who are viewing content from companies such as Disney.

**** Source The Verge February 19th, 2019: https://www.theverge.com/2019/2/19/18229938/youtube-child-exploitation-recommendation-algorithm-predators*

Addictive, Intrusive, Exploitive and Harmful Apps Disguised as Social Media and Gaming Apps

As I've reported several times, Sean Parker, Cofounder of Facebook and Tristan Harris, former product designer for Google have publically admitted that Facebook and Google intentionally develop addictive platforms, apps and technology in order to exploit their product users for financial gain even at the expense of the user's privacy and safety whether the user is an adult, teen, or child.

Don't take my word of this claim, Mr. Parker explains it better than I can per an Axios interview from 2017:

RML Business Consulting, LLC All Rights Reserved- 2019

- **Sean Parker (Co-Founder Facebook & Spotify)**: a) "It's a social-validation feedback loop ... exactly the kind of thing that a hacker like myself would come up with, *because you're exploiting a vulnerability in human psychology*…….***God only knows what it's doing to our children's brains***……The inventors, creators — it's **me**, it's **Mark [Zuckerberg],** it's **Kevin Systrom** on Instagram, it's **all of these people** — ***understood this consciously. And we did it anyway***…."- Sean Parker, Axios- November 9th, 2017.

At this point we need to ask the question: *"How come the FTC, state AGs and law makers are not protecting the public from addictive, intrusive, exploitive and harmful technology?"*

The answer: major media news organizations plus the FTC, state AGs, and law makers have turned a blind eye to these types of public admissions made by senior executives and product designers for Facebook and Google. Why?

How Laws are Written in Washington D.C. 101. Erich Schmidt, former chairman Alphabet Inc. (Google), explains how telecom and tech giants have invested millions into lobbying efforts that have resulted in the reason why the FTC, FCC, state AGs and law makers may have turned a blind eye to incriminating admissions made by Mr. Parker and Mr. Harris:

- *"The average American doesn't realize how much of the laws are written by lobbyists" to protect incumbent interests….. It's shocking how the system actually works….. Washington is an incumbent protection machine."*****

I did not learn this in my high school civics classes.

***** Source The Atlantic, October 2010: https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/

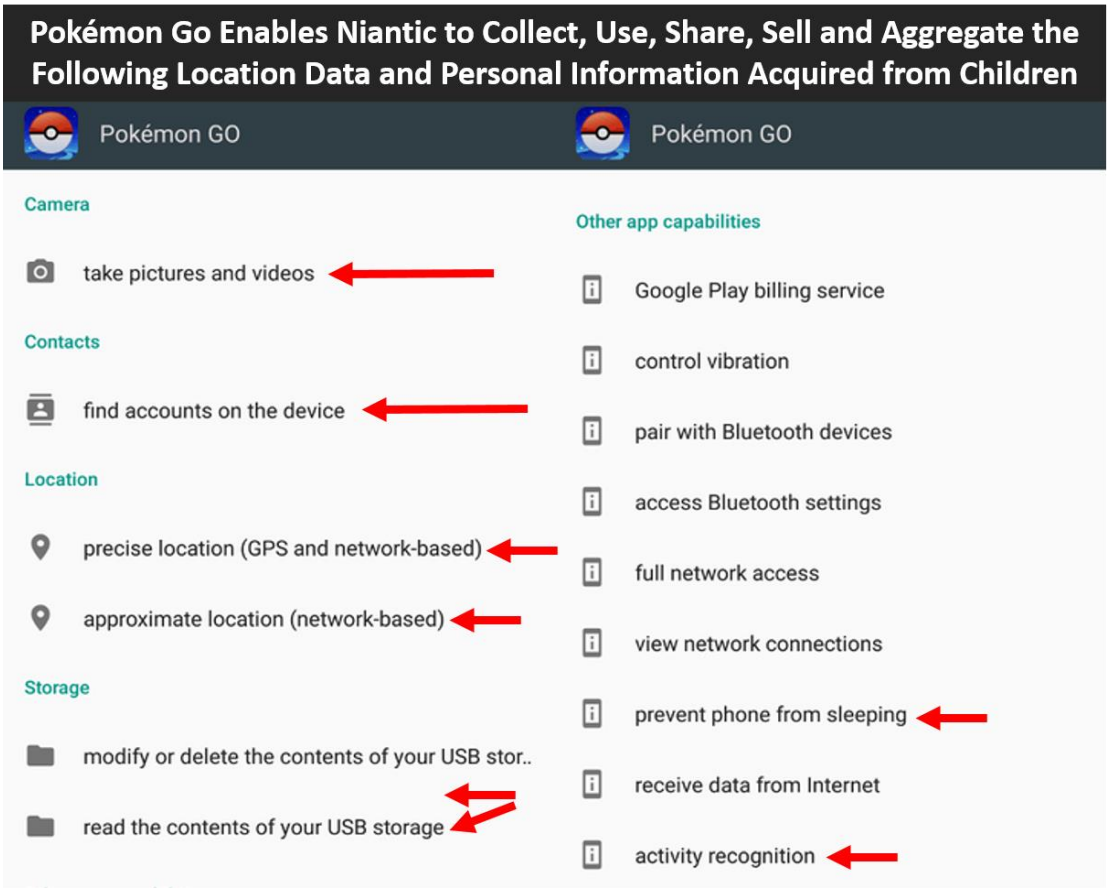
Now that we understand that companies such as Facebook and Google write consumer laws associated with privacy plus addictive, intrusive, exploitive, and harmful technology, we can now understand why agencies such as the FTC, FCC plus state AGs and law makers are not protecting us.

- Read my article *"Facebook and Google Congressional Hearings: Meaningless Resolve and Phony Apologies"* to understand why Government is failing to protect citizens, teens, and children from companies that employ predatory and harmful surveillance & data mining business practices.

Aside from Google and Facebook addictive and harmful apps, parents and educators need to be concerned with third-party apps such as Pokémon Go which I also believe are not complaint with FTC COPAA.

To understand why, all you have to do is view the android and Apple app permissions associated with the Pokémon Go app to realize how intrusive, exploitive, and potentially harmful this app is.

RML Business Consulting, LLC All Rights Reserved- 2019



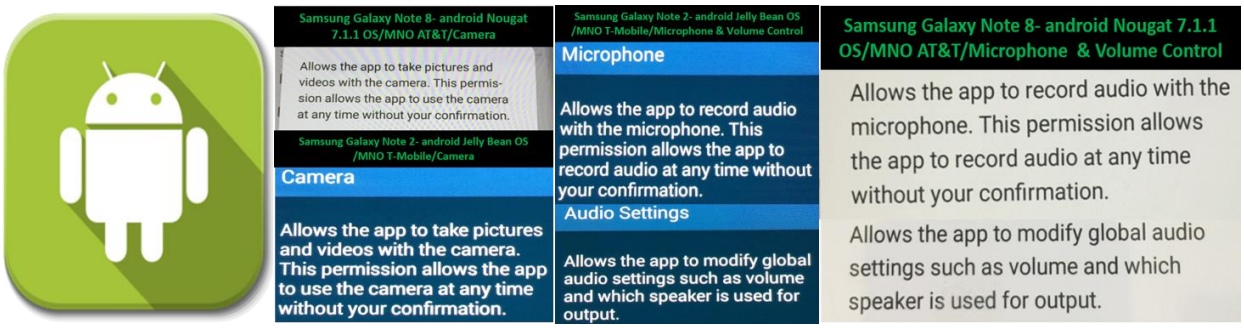
The Pokémon Go app permissions explain how much surveillance data and personal information the app developer, Niantic (former Google Company), is enabled to collect from teens and children who use the app and platform.

Below are some of the intrusive and exploitive app permissions granted to Niantic by Google:

- **Access to Hardware such as the Camera**. This enables Niantic to conduct audio and visual surveillance on the teen and child's activities 24x7 365 days a year even when the teen or child is not using the app.

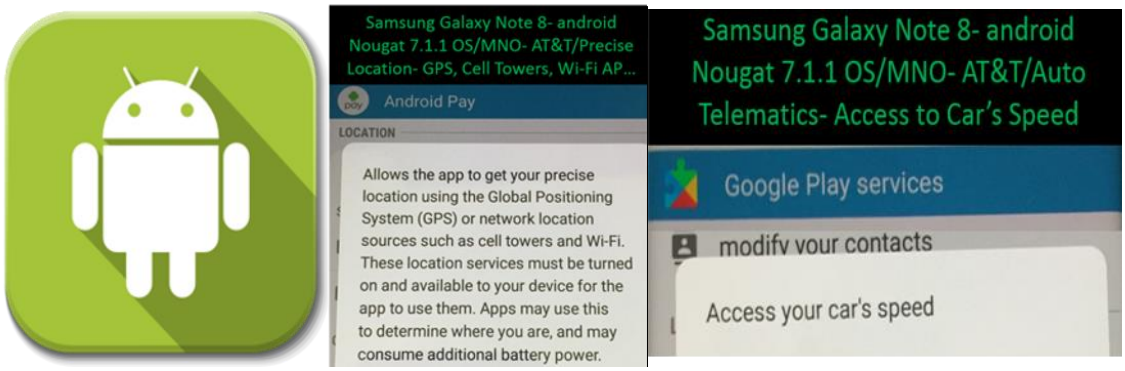
    - **Android Camera App Permission**: *"Allows the App to Take Pictures and Video with the Camera. This permission allows the app to use the camera at any time without your confirmation."* This means without parental consent which could be a violation of FTC COPAA compliance (see enclosed information).

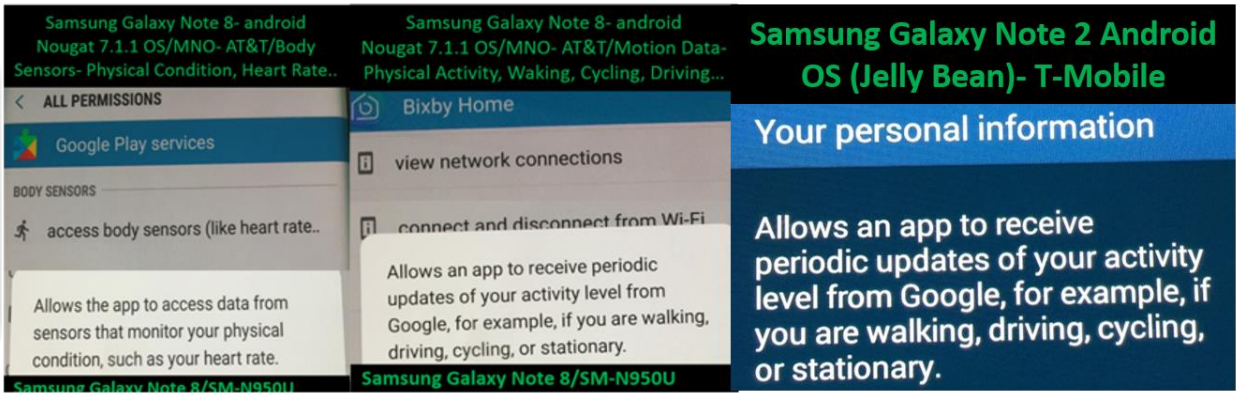
RML Business Consulting, LLC All Rights Reserved- 2019



- **<u>Access to Location Data and Physical Activity.</u>** Google is enabling Niantic to conduct surveillance on the teen and child's activities 24x7 365 days a year plus monitor when the teen or child is sitting, walking, running, cycling or even when riding in a car.

  <u>Android Location Data, Physical Activity App Permissions & Auto Telematics:</u> *"Allows the app to get your precise location using the Global Positioning System (GPS) or network location sources such as cell towers and Wi-Fi…Apps may use this to determine where you are….Allows the app to receive periodic up-dates of your activity level from Google, for example, if you are walking, driving, cycling or stationary….Access your car's speed."*





Another question to ask?: *"What parent would knowingly allow complete strangers to conduct audio, video and physical surveillance on their children 24x7 365 days a year?"*

RML Business Consulting, LLC All Rights Reserved- 2019

Google is enabling Niantic to *indiscriminately* monitor, track and data mine the app user which includes teens and children 24x7 365 days a year whether the teen or child is using the Pokémon Go app or on the platform.

Like Facebook, Amazon, Google and Apple, the Pokémon Go app user does not have to be actively using the apps or be on the platforms associated with the apps in order Niantic to monitor, track, and data mine the app user for financial gain.

In addition, Google is enabling Niantic to collect personal information from the teen and child that has nothing to do with the use of the Pokémon Go app or platform.

For example, Niantic is enabled by Google to collect the user's contacts, audio and video of the user's activities, physical activity data and location data associated with the user's activities even when the teen or child is not using the app or on the platform.

Violation of COPAA Compliance- Child Surveillance and Data Mining for Profits

To collect personal information from a child 13 and under, a company such as Google must receive parental consent according to FTC COPPA******:

- **When do I have to get verifiable parental consent?** The Rule provides generally that an operator must obtain verifiable parental consent before collecting any personal information from a child, unless the collection fits into one of the Rule's exceptions described in various FAQs herein. *See* 16 C.F.R. § 312.5(c).
  ****** Source- FTC COPAA: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Verifiable Parental***

One would have to ask at this point: *"Are companies such as Google, Apple, Microsoft, Facebook, Amazon, Niantic and other tech giants getting lawful consent from parents regarding predatory surveillance and data mining business practices?"*

I think not. The exceptions to this rule are too deep to list in this article but I can tell you that I believe companies such as Google, Apple, Microsoft, Facebook, Amazon and other tech giants are not in compliance regarding FTC COPAA regarding a number of issues I've documented in this article.

To find out more, I suggest parents and educators visit the FTC COPAA website: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

The FTC and state AGs need to start enforcing existing consumer laws that protect adults, teens, and children from companies that employ predatory and harmful surveillance & data mining business practices.

Tips on Protecting Your Child's Personal Digital DNA

It is a fact of life that children will need to use smartphones, tablet PCs, and connected products supported by the android OS, Apple iOS, and Microsoft Windows OS.

RML Business Consulting, LLC All Rights Reserved- 2019

Last question: *"What can parents do to protect their child's privacy and personal information (digital DNA)?"*

Enclosed below are a few tips for protecting your child's digital DNA:

1. **Keep your "digital DNA" clean**. I tell my kids to not do anything online or on smartphone, table PC or connected product via an app that they will regret or could cause embarrassment.

2. **Audit your child's use**. Don't be afraid to conduct a usage and app audit with your children present. Let them know you are not invading their privacy but helping to protect them from harm.

3. **Communicate and collaborate with other parents, educators, & children**. It is important as a society we discuss privacy topics that include predatory surveillance and data mining business practices employed by Google, Apple, Microsoft, Amazon, Facebook and other tech giants.

4. **Ask questions**. Contact your telecom service provider and ask them why they are selling smartphones, tablet PCs and connected products that are supported by addictive, intrusive, exploitive and harmful technology such as apps.
    a. Discuss child privacy and safety concerns with your telecom providers.
    b. Again, why is AT&T, T-Mobile, Verizon, and Sprint exposing their paying customers to companies that employ predatory surveillance and data mining business practices?

5. **Read the Terms of Use**. Don't click on "I Agree" without reading the terms of use. Convenience is not worth the value of your privacy plus personal and professional Digital DNA.

6. **Take Action**. File complaints with your service providers as well as government agencies such as the FTC & FCC:

    - FCC: https://www.fcc.gov/consumer-help-center-data
    - FTC: https://www.ftccomplaintassistant.gov/#&panel1-
    - Various State AG Offices: https://www.thespruce.com/find-a-state-attorney-general-office-3542885

7. **Find Resources that Provide Information Regarding Intrusive and Harmful Tech**. Check out Tristian Harris's site, Time Well Spent: http://www.timewellspent.io/ Take his and my advice to unplug from time to time.

    a. Here is a novel idea, play an unconnected game of monopoly with your children in the *privacy* of your home.

       Just make sure all smartphones, tablet PCs and other connected devices are put into safe and are buried in the backyard before you play the game.

Hopefully the FTC, FCC, state AGs and law makers will finally stop turning a blind eye and start protecting citizens, teens, and children from companies that employ predatory and harmful surveillance & data mining business practices rooted in Surveillance Capitalism.

RML Business Consulting, LLC All Rights Reserved- 2019

Rex M. Lee is a privacy and data security consultant and Blackops Partners senior analyst and researcher. For more information go to www.MySmartPrivacy.com Plus follow Rex on Twitter @RexMLee1

RML Business Consulting, LLC All Rights Reserved- 2019