Can Social Media Users Continue to Trust Facebook?

MARK ZUCKERBERG'S PRIVACY MANIFESTO: MORE DECEPTION AND ANOTHER FAILED ATTEMPT TO APOLOGIZE

BY REX M. LEE

Can Social Media Users Continue to Trust Facebook?
Mark Zuckerberg's Privacy Manifesto: More Deception & another Failed Attempt to Apologize
By Rex M. Lee

I heard about Mark Zuckerberg's privacy manifesto, "A Privacy-Focused Vision for Social Networking", and I was actually glad that Facebook was finally going to address privacy in a serious manner or so I thought.

However, I was skeptical of Mr. Zuckerberg's new commitment to privacy given Facebook's long track record of abuse, negligent, and harmful use of their subscriber's personal and professional information.

Let's remember that Mr. Zuckerberg admitted that people should not trust him with their personal information as he once called the Facebook subscriber a "Dumb F*ck" for trusting him with their personal information during an interview.

Let's examine Mr. Zuckerberg's thoughts about the Facebook subscriber who made him a multi-billions of dollars while making him one of the richest people on the planet:

- **Mark Zuckerberg, CEO & Chairman, Facebook**: Zuckerberg: "Yea so if you ever need info about anyone at Harvard, just ask. 'i have over 4000 emails, pictures, addresses, sns" Friend: "what!? how'd you manage that one?" Zuckerberg: "people just submitted it. i don't know why. **they trust me. dumb f*#Ks**"- Daily Mail, March 19th, 2018

Not only does Mr. Zuckerberg think the Facebook subscriber is a "Dumb Fu*K", he also does not mind experimenting on his subscribers by developing a platform that is addictive, intrusive, exploitive, and harmful.

The Facebook platform, like many smartphone apps and other platforms, is designed to be addictive so that Facebook can exploit the platform user for financial gain even at the expense of the user's privacy and safety whether that user is an adult, teen, or child.

Let's examine what Sean Parker, Co-founder of Facebook, had to say about the development of Facebook's platforms and all associated apps in an Axios Interview in 2017:

- **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.

Remember that Facebook also owns Instagram and WhatsApp which according to Mr. Parker are also designed to be addictive in order to exploit the user for financial gain at the expense of the user's privacy and safety.

I've written about these quotes numerous times but these quotes have never been more relevant until now.

I light of Mr. Zuckerberg's new commitment to privacy, I was willing to give Mr. Zuckerberg the benefit of doubt until I read Mr. Zuckerberg's vision of privacy for social media regarding his manifesto titled "A Privacy-Focused Vision for Social Networking" published on Wednesday March 6th, 2019.

Let's review Mr. Zuckerberg's privacy manifesto paragraph by paragraph so nothing I write about is taken out of context.

A Privacy-Focused Vision for Social Networking by Mark Zuckerberg, CEO & Chairman, Facebook


A Privacy-Focused Vision for Social Networking

MARK ZUCKERBERG · WEDNESDAY, MARCH 6, 2019

Paragraphs 1- 8: Executive Summary

In the first paragraph Mr. Zuckerberg willing to work with experts is very promising as he has this to say:

- *"There's a lot to do here, and we're committed to working openly and consulting with experts across society as we develop this"- Mark Zuckerberg*

As a privacy and data security consultant with application development experience, I will be willing to volunteer my time free to consult Facebook in regards to the changes that need to be done to ensure the user's has 100% control over their personal and professional information known as the user's "digital DNA".

As a matter of fact, if any executives at Facebook are reading this article, I've outlined the framework for legislation designed to protect citizens, teens, and children from companies that employ predatory surveillance and data mining business practices such as Facebook.

The two part article is titled "The Need for an Electronic Bill of Rights Part 1 & Part 2" which was published in February of 2019 by The Epoch Times.

The article is based on a request from Senator Ted Cruz's office who asked me to submit a policy change proposal for legislation back in 2017 so the framework is legit.

All Mr. Zuckerberg has to do is simply read my article and give me a call so I can submit the policy change proposal, which contains more detail, to Facebook myself.

I won't even charge a consulting fee as I will be happy to submit if for free but it won't cost you your privacy to read it plus it is safe since the words are not addictive or written in a harmful manner.

So far so good, let's review the second paragraph.

Paragraph 2 is where the train went off the tracks for me. I was astonished regarding Mr. Zuckerberg's lack of knowledge regarding privacy in the home as he had this to say:

- *"Over the last 15 years, Facebook and Instagram have helped people connect with friends, communities, and interests in the digital equivalent of a town square. But people increasingly also want to connect privately in the digital equivalent of the living room"- Mark Zuckerberg*

What world is Mr. Zuckerberg living in regarding the year 2019 or is it 1984?

First of all when you connect with friends and community in the town square, your friends and community do not invade your privacy after the meeting in the town square is over by conducting unauthorized surveillance of your personal and professional activities 24 x 7 365 days per year.

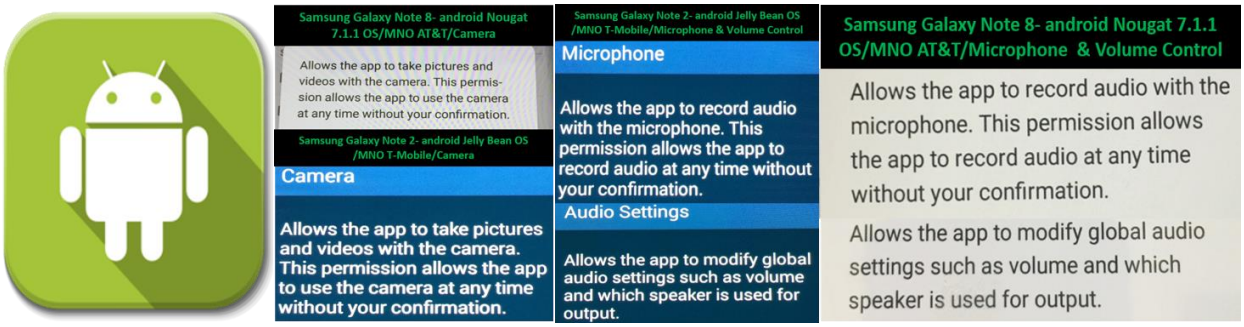
Additionally, there is nothing private about our living rooms anymore thanks to Google, Apple, Microsoft, Amazon, and Facebook who have all made sure their intrusive and exploitive products support most connected products such as smartTVs these days.

For example, Sony 4K TVs data mine the user thanks to the android OS so watching TV is no longer private either as many 4K TVs are supported by cameras plus the 4K TV remotes are supported by microphones.

Our homes have been invaded by addictive, intrusive, and exploitive technology such as voice automated assistants which include Amazon's Alexa and the new Facebook Portal which both are supported by a camera and microphone which can be turned on without our consent or knowledge according to the app permissions that support such products.

According the android Facebook camera and microphone app permissions, Facebook is enabled to conduct audio and video surveillance of the Facebook app user at any time without the user's knowledge or consent even when the user is not on Facebook's platforms or using all associated Facebook apps.

Let's examine the Facebook android microphone app permission carefully: *"Allows the app to record audio with the microphone. This permission allows the app (Facebook App) to record audio at any time without your confirmation".*



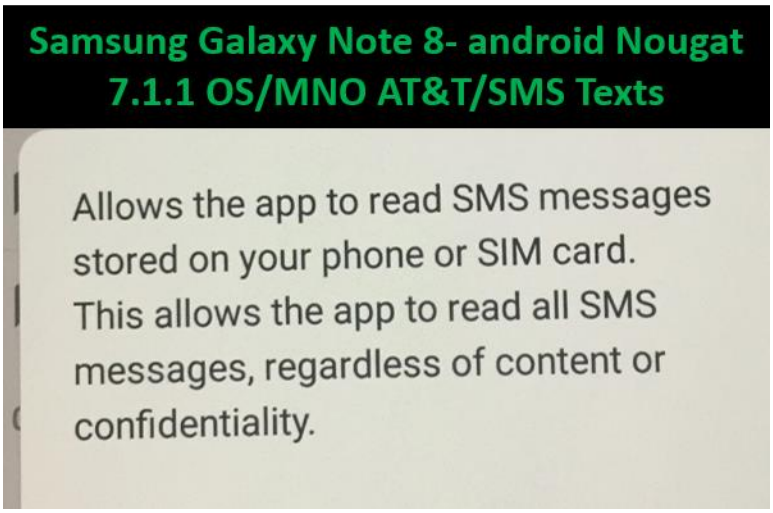
Aside from voice automated assistants, Google has invaded the home with intrusive products such as Nest which contains a hidden microphone of which Google forgot to mention to their customers who purchased Nest products as reported by The Atlantic in Feb of 2019.

Although our calendar year is 2019, Mr. Zuckerberg forgot that Silicon Valley tech giants such as Google and his company Facebook have rolled the year back to 1984 with their Orwellian surveillance and data mining business practices.

In paragraph 3 Mr. Zuckerberg had this to say about private messaging:

- *"Today we already see that private messaging, ephemeral stories, and small groups are by far the fastest growing areas of online communication. There are a number of reasons for this. Many people prefer the intimacy of communicating one-on-one or with just a few friends"- Mark Zuckerberg*

This statement was really laughable if you read the text messaging app permission that supports the android Facebook apps which states this: *"Allows the app (Facebook App & WhatsApp) to read SMS messages stored on your phone of SIM card. This allows the app to read all SMS messages, regardless of content or confidentiality":*



At this point, is Facebook willing to retract these types of application permission statements and capabilities from Facebook apps that include WhatsApp?

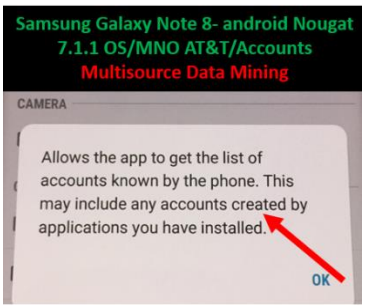
As of today, Facebook does not mind collecting your intimate SMS texts messages between you and your friends, family and significant others to use for financial gain so what the heck is he talking about?

Mr. Zuckerberg went on to say this:

- *"People are more cautious of having a permanent record of what they've shared. And we all expect to be able to do things like payments privately and securely."- Mark Zuckerberg*

Has Mark Zuckerberg ever read the app permissions that support Facebook apps including WhatsApp? Facebook is not only keeping a permanent record of all messaging associated with the Facebook platform and all associated apps such as WhatsApp but I imagine they are also keeping a permanent record of your smartphone and tablet PC SMS text messages as well.

He also mentions keeping your payments private, however the Facebook app enables Facebook to collect information on any account you set up on your smartphone including medical, credit card, and banking accounts according the Facebook android app permission: *"Allows the app to get a list of accounts known by the phone. This may include any accounts by applications you have installed."*



Per the account android app permission, Facebook is also keeping track of all of your banking and purchases by way of any banking or credit card apps you set up on devices such as your smartphone.

Like most people, it sounds like Mr. Zuckerberg has never read the terms of use that support the apps developed by Facebook.

I have and there is nothing remotely private, secure, or safe about the terms of use that support Facebook products including the platform and all associated Facebook apps that support smartphones, tablet PCs, connected products and PCs.

Paragraphs 4 - 8 are encouraging in regards to the fact Mr. Zuckerberg seems to be saying that a private social media network needs to be developed.

I agree, but given Facebook's track record of abuse, negligent, and harmful use of their user's personal and professional information coupled with the fact that Facebook's platform is designed to be addictive and exploitive, I would not trust Facebook to develop a private platform.

Would you trust a bank robber with writing laws that govern bank robbery?

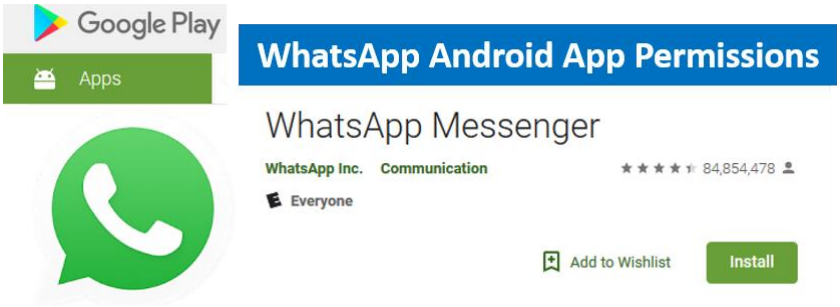
Mr. Zuckerberg had this to say about WhatsApp in regards to the app being private:

- *"We plan to build this the way we've developed WhatsApp: focus on the most fundamental and private use case – messaging…."- Mark Zuckerberg*

I have to laugh hard at this statement as again Mr. Zuckerberg sounds like he has never read the intrusive and exploitive terms of use that support Facebook or the application permissions that support the android version of WhatsApp.

Mr. Zuckerberg, I'm here to help you understand the terms of use and app permissions that support your products such as the Facebook app and WhatsApp.

Please pay close attention to the following because Google and your company are responsible for the terms of use that are enclosed below regarding WhatsApp.



Below is a list of personal and professional information (digital DNA) that Google enables Facebook to collect via the WhatsApp while enabling Facebook to conduct audio and video surveillance of the app user 24x7 365 days per year even when the WhatsApp user is not on the platform or using the app:

Google Play, WhatsApp Messenger android Application Permissions:

1. **Device and App History**- WhatsApp enables Facebook to collect information about the use of the device and the use of all apps on the device.

2. **Identity-** WhatsApp enables Facebook to collect information about all accounts that the device supports including medical, banking, social media and any account.

3. **Contacts**- WhatsApp enables Facebook to collect all of the user contacts, personal and professional, associated with the device's electronic address book.

4. **Location**- WhatsApp enables Facebook to conduct physical surveillance on the app user 24x7 365 days a year even if the user is not using WhatsApp or on any of the platforms owned by Facebook.

5. **SMS (Text Messages)-** WhatsApp enables Facebook to collect all SMS text messages associated with the device which would include a smartphone, tablet PC, or even a PC. These SMS text messages are not the same text messages the user sends by way of the WhatsApp messenger but are your personal and professional text messages in general.

6. **Phone**- WhatsApp enables Facebook to collect all phone and messaging logs which enables Facebook to identify all of the people who you are in contact with by way of phone and messaging. Facebook will also own a record of all of the calls made from your smartphone just like the NSA regarding Edward Snowden's revelations about the NSA Prism scandal.

7. **Photos/Media/Files**- WhatsApp enables Facebook to collect all photos, media (music, books, etc.), and files from any device that supports the app such as a PC, smartphone, or tablet PC.

8. **Storage (Multisource Data Mining)**- WhatsApp enables Facebook to reach beyond the host device to data mine information from any connected source including external thumb drives, computers, connected TVs, internet accounts and so on.

9. **Camera & Microphone (Audio & Video Surveillance)**- WhatsApp enables Facebook to conduct audio and video of the user's personal and professional activities 24x7 365 days a year without the user's consent or knowledge.

Keep in mind that the personal and professional information listed above is associated with the WhatsApp user's smartphone and is totally separate from the personal and professional information that is collected by Facebook by way of the use of the WhatsApp Messenger's Facebook platform.

As The Epoch Times article, "Smartphone App Users Are Data Mined Even When Not Using The Apps", I authored, apps such as the Facebook app and WhatsApp enable companies such as Facebook to surveil and data mine the app user even when the app user is not on the Facebook or WhatsApp platform or using the all associated apps.

Additionally, apps such as the Facebook app and WhatsApp enable Facebook to collect personal and professional information associated with devices such as smartphones that has nothing to do with the use of the apps and platforms such as the app user's smartphone SMS text messages or audio and video of the user's personal and professional activities associated with the smartphone.

Paragraphs 9 – 12: Private Interactions as a Foundation

In paragraph 9- Mr. Zuckerberg had this to say:

- *"But one great property of messaging services is that even as your contacts list grows, your individual threads and groups remain private. As your friends evolve over time, messaging services evolve gracefully and remain intimate"- Mark Zuckerberg*

In regards to the WhatsApp SMS text messaging app permission, Facebook has a total disregard for the privacy of the smartphone user so this statement is another half-truth, lie, or misleading statement according to the Facebook App and WhatsApp android SMS app permission.

Furthermore, android app permissions that support apps such as the Facebook app and WhatsApp enable the app developer to identify the app user: *"Allows apps (Facebook/WhatsApp) to read personal profile information stored on your device, such as your name and contact information. This means apps can identify you and may send your profile information to others."*

I stress that Mr. Zuckerberg either is lying or he has no idea how his platform and apps collect the app user's personal and professional digital DNA so that Facebook can exploit it for financial gain increasing Mr. Zuckerberg's personal wealth.

In paragraph 11 Mr. Zuckerberg had this to say:

- *"In WhatsApp, for example, our team is obsessed with creating an intimate environment in every aspect of the product."- Mark Zuckerberg*

If the WhatsApp team is so obsessed with a private and intimate enviroment, how come the team developed WhatsApp to enable Facebook with the ability to surveil the user while the app data mines the user's personal and professional digital DNA from the host device such as a smartphone?

What Mr. Zuckerberg is not addressing here is the fact that the WhatsApp user experience may seem private in regards to the use of the app and platform, but what he is not addressing the fact that WhatsApp is intentionally designed to be addictive in order so that Facebook is enabled to surveil and data mine the app user by way of the host device that supports the app.

Facebook app and WhatsApp users must understand that there is two types of surveillance and data mining associated with apps such as the Facebook app and WhatsApp which include:

1. Personal and Professional information that is collected from the use of the apps and associated Facebook platforms.

2. Personal and professional surveillance data (location data) and sensitive user data (digital DNA) WhatsApp enables Facebook to collect from the host device such as a Smartphone.

Combined, Facebook is collecting personal and professional information associated with both the use of the device such as a smartphone and the use of all associated Facebook products such as WhatsApp or the Facebook social media platform.

Social media users such as Facebook subscribers have no idea that they are being surveilled and data mined by way of the Facebook apps and associated platforms plus by way of the devices that support the Facebook apps including WhatsApp.

People must also understand that free apps such as WhatsApp are not free, the user pays for the app with their personal and professional information and/or digital DNA which is exploited for financial gain by Facebook even at the expense of the user's privacy and safety as admitted by Sean Parker, Co-founder of Facebook.

Again, it sounds like Mark Zuckerberg does not even understand Facebook's surveillance and data mining business practices which are predatory to say the least.

Paragraphs 13 – 19: Encryption and Safety

In paragraph 13 Mr. Zuckerberg had this to say:

"People expect their private communications to be secure and to only be seen by the people they've sent them to -- not hackers, criminals, over-reaching governments, or even the people operating the services they're using."- Mark Zuckerberg

This statement is incredible to me considering Facebook was one of many tech giants to have exposed their user's personal and professional information to the U.S. government by way of the NSA's Prism program as exposed in 2013.

Facebook has already cooperated with an over reaching government regarding the Obama administration.

Did Mr. Zuckerberg forget that he was in front of the Senate Judiciary Committee about a year ago regarding the Facebook Cambridge Analytica scandal in which Facebook irresponsibly sold access to the Facebook user to a data broker named "Aleksandr Kogan"?

I guess that he forgot that Mr. Kogan used the Facebook user's personal information in a harmful manner by selling it to Cambridge Analytica.

Cambridge Analytica in turn applied artificial intelligence ("AI"), predictive analytics, and suggestive technology to the user's personal information in order to develop micro-targeted ads based on the user's personal preferences in order to manipulate the Facebook user to vote for a presidential candidate named Donald J. Trump.

Mr. Zuckerberg also must not have seen the Axios interview with Sean Parker who said that the Facebook platform was intentionally designed to be addictive so that Facebook could exploit the product user for financial gain even at the expense of the user's privacy and safety whether the user is an adult, teen, or child.

Mr. Parker even addresses himself as a hacker within the interview by stating "It's a social-validation feedback loop ... exactly the kind of thing that a *hacker like myself would come up with*…" while referring to the addictive, intrusive, and harmful nature of the Facebook platform.

Furthermore, Mr. Parker said Mr. Zuckerberg was aware that the Facebook platform was intentionally designed to be addictive, intrusive, exploitive and harmful but he and Mr. Zuckerberg developed the platform anyway regardless of the harm to the platform user.

Mr. Zuckerberg needs to understand that Sean Parker has already incriminated Mr. Zuckerberg as being a hacker who develops addictive, intrusive, and harmful products in order to exploit the Facebook and WhatsApp user for financial gain.

In this segment Mr. Zuckerberg tries to ensure the privacy of the new Facebook platform through encryption yet he is not addressing the fact that the apps which will support the platform will still enable Facebook to surveil and data mine the product user for financial gain.

Mr. Zuckerberg is not addressing the fact that the only way to truly make the new Facebook platform private and secure is to simply not enable Facebook to monetize the Facebook platform and app user.

Furthermore, he is not addressing the fact that another way to make the new Facebook platform private and secure is to enable the user to delete all of their personal and professional information on demand.

He also needs to address the fact that the new Facebook platform and all associated apps cannot be intentionally designed to be addictive, intrusive, exploitive, and harmful if he is serious about the user's privacy and safety.

Encryption alone does not protect the Facebook platform and app user from predatory surveillance and data mining business practices that can bring harm to the product user.

Paragraphs 20 – 24: Reducing Permanence

The name of this segment, "Reducing Permanence" is in regards to reducing the time that a company such as Facebook can store a Facebook user's personal and professional information.

The name of this segment by Mr. Zuckerberg already sounds like a statement from a shady politician who is trying to use flexible words such as "reducing" to distance himself from a phony promise made today and then broken tomorrow.

The name of this segment should be titled "Eliminating Permanence" rather than using a watered down word such as "reducing".

However, Mr. Zuckerberg is correct in regards to how a social media platform should be designed as he had this to say in paragraph 23:

- *"For example, messages could be deleted after a month or a year by default. This would reduce the risk of your messages resurfacing and embarrassing you later. Of course you'd have the ability to change the timeframe or turn off auto-deletion for your threads if you wanted."- Mark Zuckerberg*

The problem with this statement and this segment is the fact that Mr. Zuckerberg is only addressing the personal and professional information associated with the use of the new Facebook platform rather than addressing the personal and professional information the Facebook app and WhatsApp enables Facebook to collect from the host device such as a smartphone.

The scam is the fact that Facebook, Google, Apple, Amazon, and other tech giants use their platforms as a means to support their intrusive apps of which do the dirty work in terms of enabling these tech giants to collect personal and professional information from the host device separate of the use of all platforms and apps concerned.

Mr. Zuckerberg's statements in this section ring hollow until he addresses the collection of personal and professional surveillance data (location data) and sensitive user data that the Facebook app and WhatsApp enables Facebook to collect from the user's host device such as a smartphone.

Mr. Zuckerberg's contention that WhatsApp is private, secure, and safe needs to be challenged due to the numerous application permission statements associated with WhatsApp which enables Facebook to collect personal information from the user's host device in addition to the personal information collected by the use of the WhatsApp Messenger.

Paragraphs 25 – 31: Interoperability

Interoperability in this segment refers to a unified messaging platform that can manage all forms of messaging such as text messaging coupled with the use of a messenger app such as WhatsApp.

Interoperability would be a good thing in regards to a unified messaging platform as long as the messages are not monetized and exposed to third-parties such as advertisers and data brokers.

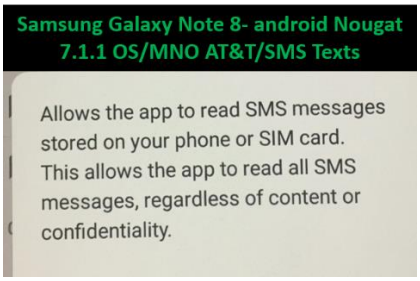
Aside from encryption, the user should be able to control the deletion of their messages on demand meaning that if the user hits delete, the messages are permanently deleted immediately without delay.

Regarding Facebook's track record, would you trust Facebook to have access to all of your messages including your android text messages as he is suggesting regarding paragraphs 26 & 27?

- "We plan to start by making it possible for you to send messages to your contacts using any of our services, and then to extend that interoperability to SMS too…. For example, many people use Messenger on Android to send and receive SMS texts…"- Mark Zuckerberg

Oh, I forgot, the Facebook app and WhatsApp today already give Facebook access to your android SMS text messages by way of the android SMS application permission statement that supports the android version of the Facebook app and WhatsApp as I noted earlier in this article.

Don't believe me, read the android Facebook SMS app permission again: "Allows the app (Facebook & WhatsApp) to read SMS messages stored on your phone (android phone) or SIM card. This allows the app to read all SMS messages, regardless of content or confidentiality."



Again, Mr. Zuckerberg is either lying or simply is oblivious to Facebook's surveillance and data mining business practices associated with all Facebook products concerned.

He seems to have a vision one day of gaining access to android SMS text messages when Facebook is already collecting android SMS text messages by way of the Facebook app user's smartphone without the Facebook app user's consent or knowledge.

Paragraphs 32 – 36: Secure Data Storage

Mr. Zuckerberg's contests that the Facebook philosophy is not to store their user's personal and professional information in countries with a poor human rights record which is a good philosophy when he had this to say in paragraph 33:

- *"we've chosen not to build data centers in countries that have a track record of violating human rights like privacy or freedom of expression."- Mark Zuckerberg*

However, nation-state companies from adversarial countries such as China and Russia pose a huge threat to platforms as I wrote about regarding the article Google, Apple, and Microsoft Distribute Chinese Surveillance Technology which exposes Google, Apple, and Microsoft apps developed by Tencent and Baidu.

This is a big problem for platforms such as Facebook since Facebook's business model is to sell access to the Facebook user to data brokers who develop intrusive apps such as the case with Aleksandr Kogan as noted earlier in this article.

These types of app developers use their apps to surveil and data mine the Facebook user such as was the case regarding Aleksandr Kogan and the Facebook Cambridge Analytica Scandal as noted earlier in this article.

The Facebook Cambridge Analytica scandal proved that the Facebook user's personal information can be collected and used in a harmful manner by other Facebook app developer who develop apps to be deployed within the Facebook app ecosystem such as Angry Birds and other entertainment apps that are designed to collect personal information from the app user.

Mr. Zuckerberg needs to stop selling access to the Facebook user to third-parties such as data brokers who develop innocent looking entertainment apps that are really a legal form of malware designed to enable the app developer to surveil and data mine the app user.

Paragraphs 37 – 41: Next Steps

Mr. Zuckerberg closes by stating this in regards to next steps:

- *"I believe we should be working towards a world where people can speak privately and live freely knowing that their information will only be seen by who they want to see it and won't all stick around forever. If we can help move the world in this direction, I will be proud of the difference we've made."- Mark Zuckerberg*

In my opinion, so far the only difference companies such as Google, Apple, Microsoft, Amazon, and Facebook have made is the elimination of *civil liberties, privacy, cyber security and safety associated with smartphones, tablet PCs, connected products, PCs, and the internet in general*.

This is a statement coming from a man who runs a company that censors political adversaries while exploiting his patrons for financial gain at the expense of the patron's privacy and safety which is hilarious to say the least.

Mr. Zuckerberg sounds sincere in regards to addressing privacy and safety issues associate with all Facebook platforms concerned but after numerous apologies and promises, can we trust Mr. Zuckerberg?

I say No due to his track record of meaningless resolve and phony apologies. He sounds like a broken algorithm stuck in a constant loop of damage control by way of phony apologies and meaningless resolve.

It is time the FTC and state AGs hold Facebook accountable for the abuse, negligent, and harmful use of personal and professional information by way of deceptive trade practices.

Case and point, he sets the expectation that Facebook will address privacy now but sets the expectation that the process will take some time:

- *"Over the next year and beyond, there are a lot more details and tradeoffs to work through related to each of these principles. A lot of this work is in the early stages, and we are committed to*

consulting with experts, advocates, industry partners, and governments -- including law enforcement and regulators -- around the world to get these decisions right."- Mark Zuckerberg

Like a true politician making another phony promise that will never be kept, he sets expectations that change is in the near but far away future at the same time.

So it will be business as usual at Facebook in the interim which is to make money at the expense of the user's privacy and safety.

Until there is real changes and companies such as Facebook are held accountable for their negligent actions, the next steps the Facebook product user needs to take to ensure their privacy and safety is to simply disable all apps associated with all Facebook products and simply delete all user accounts associated with all Facebook platforms concerned.

Rex M. Lee is a tech journalist, cybersecurity & privacy advisor, and Blackops Partners senior analyst & researcher. For more information go to www.MySmartPrivacy.com Plus follow Rex on LinkedIn at: www.linkedin.com/in/rex-lee-5b5a5410

Facebook App Analysis- android OS

Enclosed below is a graphic that shows how much personal and professional information OS developers such as Google, Apple, and Microsoft enable Facebook to collect from smartphone, tablet PC, and PC users who access Facebook by way of the Facebook App (actual screen shots of android Facebook app permissions):