2020

Surveillance Capitalism Explained

PRIVACY, CYBERSECURITY, CIVIL LIBERTY, HYBRID WARFARE & SAFETY THREATS

BY REX M. LEE, CYBERSECURITY & PRIVACY ADVISOR/TECH JOURNALIST

Surveillance Capitalism Explained:

Privacy, Cybersecurity, Civil Liberties, Hybrid Warfare & Safety Threats

By Rex M. Lee

Do you ever get the feeling that you are being spied on? I get that feeling every time that I use a smartphone, tablet PC, smartTV, voice automated assistant or any connected product that is supported by the android OS, Apple iOS, Microsoft Windows 10 OS, app or platform such as Facebook.

The reason I get this feeling comes from the fact that the android (Google) OS, Apple iOS, Microsoft Windows 10 OS, apps and platforms, such as Facebook, are supported by predatory surveillance and data mining business practices that are rooted in "Surveillance Capitalism" which can be described as a business model.

The Surveillance Capitalism business model simply means that the end user has been monetized by the OS, app or platform developer.

This means that the developer is able to exploit the end user for financial gain by way of predatory surveillance and data mining business practices associated with intrusive apps and platforms that support connected products such as smartphones.

The Surveillance Capitalism business model has been adopted by global operating system ("OS"), app and platform developers such as Google, Apple, Microsoft, Amazon and Facebook plus companies from China such as ByteDance (TikTok), Baidu (DU Apps) and Tencent (WeChat).

All of these developers are primarily in the information business, aside from developing operating systems, apps and platforms plus manufacturing hardware such as smartphones, tablet PCs, connected products and PCs in general.

Personal & Professional End User Digital DNA - The Rise of the Trillion Dollar Information Industry

Global tech giants use their apps and platforms as a means to acquire Digital DNA which is their end user's personal and employment ("professional") information associated with the use of a smartphone, tablet PC or any connected product supported by the android OS, Apple iOS or Microsoft Windows 8 & 10 OS.

The collection and marketing of end user Digital DNA is a global trillion dollar industry.

For example, Walmart's annual revenues for 2019 were $514 billion dollars* compared to Amazon's annual revenues of $280 billion dollars* yet Amazon's total market cap hit $1 trillion dollars** in January of 2020 compared to Walmart's market cap of $337 billion dollars*.
*Macrotrends **CNBC

Amazon is valued more than Walmart as a company due to the fact that Amazon is viewed by Wall Street as an information based company rather than just a retailer.

To compete against Amazon, Walmart is changing their business model to become more of an information based company rather than just a retailer which is why they are JD.Com's, a Chinese company, biggest investor since JD.Com is the third largest internet company in the world (see enclosed chart for details).

Most tech giants today are valued by Wall Street primarily by the amount of Digital DNA they can harvest from their end users which is why the top ten internet companies in the world have adopted the Surveillance Capitalism business model.

The top ten internet companies* in the world include the following:

1. Amazon $280B- USA

2. Google $120B- USA
3. JD.Com $ 67B- China
4. Alibaba $ 56B- China
5. Facebook $ 55B- USA
6. Tencent $ 44B- China
7. Netflix $ 15B- USA
8. Bookings $ 12B- USA
9. Baidu $ 12B- China
10. E-Bay $ 10B- China

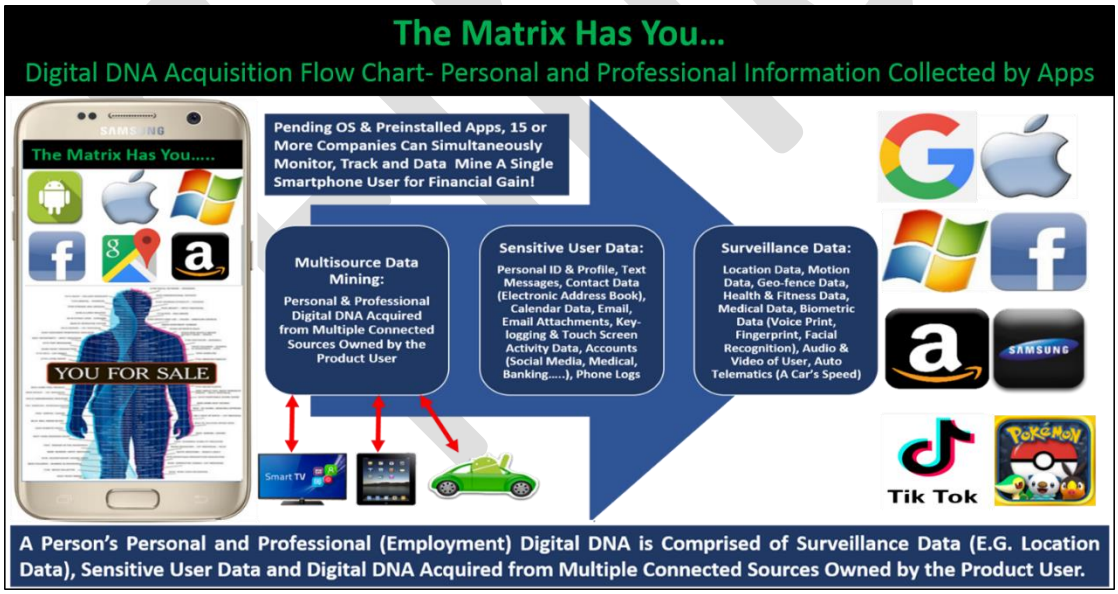
*Source Wikipedia & Macrotrend

Apple and Microsoft are not included on this list due to the fact they are not considered to be internet companies although they develop numerous apps and platforms that are supported by predatory surveillance and data mining business practices.

All of this means that personal and professional information is worth more than gold, diamonds or oil which is one of many reasons why personal privacy should be of highest importance to all OS, app and platform end users which include you and myself.

The Value of Digital DNA- Personal and Professional Information

To fully understand the value of Digital DNA, one must understand what types of personal and professional information that multinational companies, including companies from China and Russia, are collecting.



There are many buckets of personal and professional information that make up an end user's Digital DNA which include the following:

- Surveillance Data
    - Location, Motion (Sleeping, Sitting, Walking, Running), Geo-fence, NFC, Wi-Fi Access Points, Health & Fitness, Medical, and Auto Telematics (i.e. a Car's Speed)

- Biometric Data
    - Facial Recognition, Voice Print, Fingerprint and Retina Data

- Video and Audio Files/Recordings of the Product User
    - Photos, Videos, Recordings, Music, Books, Movies, and so on

- Sensitive User Data
    - Personal/User ID, ID Associated with Contacts, Messaging (Texts, Instant, Social Media), Contact Address Book, Calendar Events, Email, Attachments (PDFs, Word Docs, Photos, Etc.), Accounts (Medical, Banking, Personal, Etc.) and so on

- Key-logging
    - Touchscreen and Key Board Activity Logging

- Activity Logs
    - Phone, Messaging, App Usage and so on

- Multisource Data Acquisition- Intrusive Apps can reach beyond the host device to collect Digital DNA
    - Personal and Professional Information Acquired from Connected Sources to Host Device
    - Connected sources include PCs, USB Storage, Connected Products, Tablet PCs and so on
    - Any Connected Source Supported by the Android OS, Apple iOS or MS Windows OS

In order to collect valuable end user Digital DNA, tech giants use intrusive, addictive, and harmful technology in the form of the OS, apps and platforms that support connected tech and telecom products.

There are two types of apps and platforms which include:

- Uncontrollable preinstalled apps and platforms that support products like smartphones

- Third-party apps that the product owner and/or user downloads from sources such as Google Play, Apple App Store and Microsoft Windows App Store

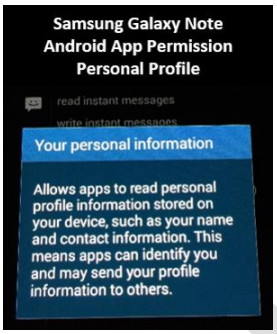
For example, preinstalled apps are the apps that a smartphone owner cannot uninstall, control or disable which means the product owner cannot fully control their device.

The end users needs to realize that data profile is made from their collective Digital DNA. The Data profile includes the end user's identity so that app developers can identify the user while connecting the data profile to the end user's collective Digital DNA.

According to the terms of use, developers are able to sell and share data profiles along with the end user's Digital DNA to third parties so user's in fact identified by app developers.

Don't take my word for this claim, enclosed below is a picture of an actual android (Google) app permission (legalese) that states that Google can in fact identify end users:

- Personal Information android Permission (actual screen shot): "Allows the apps to read *personal profile information* stored on your device such as your name and contact information. This means that apps can *identify you* and *send your profile information to others*"



Tech End User Exploitation- Forced Participation

Due to uncontrollable preinstalled apps, platforms and other content, the end user is forced into participating within a highly intrusive, exploitive and harmful business model known as Surveillance Capitalism.

Unfortunately, companies such as Google, Apple, Microsoft, Facebook and Amazon do not view their loyal end users as paying customers but rather these companies view their end users as *"uncompensated information producers"* whom are to be exploited for profits.

End users need to be aware that their tech providers are exploiting end user personal and professional information for profits at the expense of the end user's *privacy, cybersecurity, civil liberties and safety without compensating the end user for the profits made from end user Digital DNA*.

Legal Malware- Intrusive, Addictive & Harmful Technology

When a person sees an app, they see convenience, entertainment and necessity, not me, when I see an app I see "Legal Malware" designed to enable numerous third-parties with the ability to monitor, track and data mine the end user for financial gain 24x7/365 days per year without compensating the end user.

This means that a Facebook user may be on their Facebook account for one or two hours a day but Facebook is enabled to *"indiscriminately"* surveil and data mine the end user 24 hours a day while collecting the end user's highly

confidential personal and professional information which has nothing to do with the use of the Facebook app or platform. This is true for nearly all apps and platforms.

Indiscriminate surveillance and data mining should be against the law especially if the information collected from an end user has nothing to do with the user's use of an app or platform such as Facebook.

End users need to go to second level thought and ask what does their employment, medical, and non-consumer related personal information have to do with the use of any app or platform such as Facebook, Amazon, Twitter, TikTok, WeChat and so on.

Companies such as Google and Facebook develop their "Legal Malware" in the form of *intrusive, addictive and harmful apps and platforms* in order to make sure that their users spend as much time as possible on their platforms so that they exploit the end user for maximum profits.

Profits are often made at the expense of their end user's privacy, cybersecurity, civil liberties and safety whether their end user is an adult, teen, child or business professional according to Sean Parker who Co-founded Facebook, along with Mark Zuckerberg, and Tristan Harris a former lead product designer for Google:

- *"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, Co-founder Facebook, Axios- November 9th, 2017.

- *"The average person checks their phone 150 times a day. Why do we do this? Are we making 150 conscious choices? One major reason why is the #1 psychological ingredient in slot machines: intermittent variable rewards . . . Addictiveness is maximized when the rate of reward is most variable.....By shaping the menus we pick from, technology hijacks the way we perceive our choices and replaces them with new ones. But the closer we pay attention to the options we're given, the more we'll notice when they don't actually align with our true needs."* – 60 Minutes & TED Talk 2017

The use of intrusive, addictive and harmful technology in order to exploit a person for financial gain is obviously an *illegal business practice* that is not being policed by consumer protection agencies, state Attorney Generals, or government agencies such as the Federal Trade Commission (FTC) within the United States.

Is it legal for companies to use intrusive, addictive and harmful technology in order to exploit their customers for financial gain?

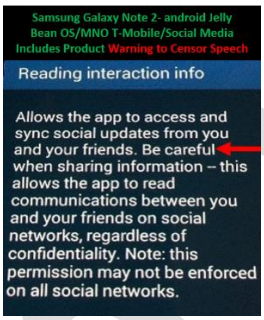
The answer to this question leads to the collective terms of use a person accepts when they click on "I Agree" often without reading the legalese that makes up the collective Terms and Conditions (T&Cs).

The Consequences of Clicking on "I Agree" Without Reading the T&Cs- Predatory Terms of Use

Per my research on the terms of use that support operating systems, apps and platforms, I firmly believe the terms of use are illegal, according to existing consumer protection laws, for many reasons that include:

- Collective terms of use are impossible to read and understand due to the sheer volume of legal text (over 3,000 pages)

- Non-transparent terms of use (hidden in device) that include application product warnings (see enclosed example below)



Aside from the use of addictive and harmful technology, these are two examples associated with the fact that consumer agencies around the globe are not enforcing existing consumer laws.

It is clear that not publishing product warnings within online terms and conditions, may be considered to be illegal according to existing consumer laws.

A contract is also deemed illegal if a consumer cannot read or understand the contract prior to making a product purchase so how is it possible for a consumer to read 3,000 plus pages of legal text prior to making a product purchase?

In my 7 plus years of researching tech and telecom products, I have yet to meet an attorney, CEO, government official, elected official or a person who has ever read the collective terms of use that support all products concerned.

Per my research on a Samsung Galaxy Note supported by the android OS, I've read the collective terms of use that supported the OS plus the preinstalled apps and platforms.

After reading the collective terms of use, I was astonished and horrified at what I had agreed to when I clicked on "I Agree" after activating the Galaxy Note at the T-Mobile corporate store where I had purchased the device.

I realized that I accepted a *"cyber enslavement agreement"* enabling Google, Samsung, T-Mobile plus other developers to *"simultaneously"* surveil and data mine all of my personal and professional information for financial gain 24x7/365 days per year.

As soon as I clicked on "I Agree" accepting the collective terms of use, I went from being a sales prospect to being enslaved as an "*uncompensated employee"* by Google, Samsung, T-Mobile plus 15 other preinstalled app developers, including Baidu a Chinese company.

In plain English, I agreed to the following:

- To use an unsecure smartphone that could not be fully privatized due to preinstalled uncontrollable surveillance and data mining technology
- To use intrusive, addictive and harmful apps and platforms without any protection due to the fact that the agreement does not indemnify (protect) the user from harm or negligence
- The end user cannot file a class action lawsuit due to arbitration
- The loss of privacy, cybersecurity, civil liberties and safety
- To enable numerous multinational companies to *simultaneously and indiscriminately* surveil and data mine all personal and professional information
- To be exploited for financial gain via a product that requires money to participate

- To enable numerous third-parties, including data brokers, governments (including China), law enforcement agencies and "others" to share, sell, aggregate and store end user personal and professional information
- To enable existing or potential business competitors to acquire end user personal and employment related information protected by legal agreements, cybersecurity standards, and confidentiality laws that protect medical information, client attorney privilege and classified information
- To accept a legal agreement published online plus published with in the device hiding product warnings from end users
- And the list goes on…

I firmly believe that if the collected terms of use were written in plain English and published online, such as the example above, nobody would ever purchase or use products such as smartphones supported by operating systems, apps or platforms developed by Google, Apple, Microsoft, Facebook, Amazon, ByteDance, Baidu, or Tencent.

It took me close to four months to analyze the preinstalled apps , over 275, and the collected terms of use, over 3000 pages of legal text, that supported the Samsung Galaxy Note that I had purchased from T-Mobile.

In other words, it took me nearly 4 months to read my cellular phone contract which means that the collective terms of use are illegal to existing consumer laws that are not being enforced by governments around the world.

The Loss of Tech & Telecom Privacy- Intrusive Operating Systems, Apps and Platforms

These egregious and illegal business practices mean that tech and telecom products such as smartphones are not secure nor private due to uncontrollable preinstalled surveillance and data mining technology.

Don't take my word for this claim, Verizon and T-Mobile admit that smartphones, tablet PCs and connected products are not private or secure forms of telecommunications and computing:

- T-Mobile Admission: *"We, too, remember a time before smartphones when it was reasonable to conclude that when you activated service with T-Mobile that only T-Mobile would have access to our personal information. However, with the Samsung Galaxy Note, the iPhone, and many other devices, there are indeed a variety of parties that may collect and use information."* — T-Mobile Privacy Team (FCC Consumer Complaint #423849 Filed by Rex M. Lee/Public Record)

- Verizon Admission *"We have reviewed your request at the highest levels of our organization and have confirmed that the only solutions to make a phone private and secure are available through third parties, not directly from Verizon…. Additionally, Verizon is not equipped to address preinstalled solutions or applications on any device"* – July 02, 2018 (Privacy Product Request by Rex M. Lee)

They concluded that smartphones, tablet PCs or connected products cannot be fully secured or privatized due to *uncontrollable preinstalled surveillance and data mining technology* developed by Google, Apple, Microsoft, Amazon, Facebook, Baidu (China) and other tech giants who are responsible for preinstalled content.

The T-Mobile and Verizon admissions mean that the product owner and/or end user have no control over intrusive preinstalled technology developed by the OS and preinstalled app developers.

The developers are enabled to take remote control of any product in order to conduct audio, video and physical surveillance on the product user via the hardware (i.e. camera & microphone) and sensors that support the device.

An individual may own a smartphone but that product owner cannot fully control their device because the preinstalled apps enable the developers to take remote control over sensors and hardware that include the GPS, accelerometer, camera and microphone in order to conduct physical, audio and video surveillance on the end user.

These intrusive, addictive and harmful apps & platforms are used by citizens around the world which include:

- Adults, Teens and Children (under 13)
- Students (Grade School thru College)
- Board Members (Academic and Business)
- CEOs, C-suite Level Executives, Middle Management & Front Line Employees
- Elected Officials, Govt. Officials & Employees
- Members of the Military & Law Enforcement, Including Family Members
- Local, State and Federal Judges
- Defense Contractors & Employees
- Professionals such as Doctors, Lawyers, Educators, & Journalists
- Business Owners
- And the list goes on….

Users of technology are under some form of corporate surveillance 24x7/365 days per year which is a huge threat to privacy, cybersecurity, safety and civil liberties.

Most app and platform users believe that their personal and professional information is being sold first by companies such as Facebook, Twitter, Amazon or ByteDance (TikTok-China), however, this is not true.

Forced Participation- OS End Users "For Sale" by Google, Apple and Microsoft

The tech and telecom product user is first sold by the OS developer which includes Google, Apple and Microsoft the developers of the android OS, Apple iOS and Microsoft Windows OS.

Google, Apple and Microsoft sell access to their OS end user (you & myself), to companies such as Amazon, Facebook, Twitter, ByteDance (TikTok-China), Tencent (WeChat-China), Baidu (DU Apps-China), and Prima Labs (Apps-Russia).

In essence, the OS end user is auctioned off to the highest bidders by Google, Apple and Microsoft who see their end user as a profit center to be exploited for financial gain rather than a loyal customer OS end user.

The OS monopoly by Google, Apple and Microsoft is another example of forced participation because their operating systems as a whole support nearly 100% of all tech and telecom products worldwide leaving the consumer of technology with no private or secure options to purchase.

Every major manufacturer of tech and telecom products in the world, such as Samsung, Sony, Lenovo, Motorola, HP, Research In Motion (Blackberry) and others, have all adopted the android OS, Apple iOS or Microsoft Windows OS giving Google, Apple and Microsoft a virtual monopoly regarding operating system development.

Due to this monopoly, new competition and innovation are eliminated from the market place regarding a private and secure alternative which is an example of antitrust and unfair business practices that needs to be investigated governments and elected officials worldwide.

As a result of this monopoly, tech and telecom products have been turned into surveillance and data mining tools used by OS and app developers in order to exploit their end users for profits.

This means that every time a person touches their smartphone or any other connected product, that person is producing valuable information and/or Digital DNA for Google, Apple, Microsoft plus other app developers to exploit for financial gain.

This unspoken monopoly means that there are virtually no connected tech or telecom products on the market that can be secured or privatized due to the OS coupled with the intrusive preinstalled apps and platforms that support all products concerned.

The list of unsecure and intrusive tech and telecom products include:

- Smartphones
- Tablet PCs
- IoT/IIoT Devices,
- Voice Automated Assistants,
- Smart TVs and Appliances
- In Home Climate Control and Security Systems
- Connected Vehicles
- Wearable tech
- PCs in general and the list goes on...

Due to the OS monopoly, Google, Apple and Microsoft are largely responsible for the loss of privacy, cybersecurity, civil liberties, and safety associated with tech and telecom products supported by their collective operating systems.

As a result of this monopoly, there are significant privacy, cybersecurity, civil liberty, hybrid warfare and safety threats to the OS end user that need to be addressed by government & elected officials and consumer protection agencies.

Google, Apple and Microsoft are actively developing and distributing intrusive, addictive and harmful technology via Google Play, Apple App Store and Microsoft App Store presenting numerous threats to all tech and telecom product users globally.

End User Threats- Harmful Use of Apps and Platforms

Most OS, app and platform end users tell me that they have never been harmed by their tech and telecom providers but what they don't know is that they are in fact being harmed in many ways they don't understand such as Facebook users regarding the Facebook Cambridge Analytica scandal.

The first form of harm is associated with the fact end users of intrusive apps and platforms are being exploited for financial gain at the expense of privacy and safety by way of addictive and harmful technology.

In recent years it has come to light that app and platform end users are being harmed by companies such as Facebook and Twitter whose platforms have been infiltrated and weaponized by users from adversarial countries such as China and Russia.

Platforms such as Twitter are censoring their users based on nebulous end user terms of use. For example the daughter of a murdered police officer in McAllen, TX left a memorial to her father on her Twitter page and ended the memorial with #BlueLivesMatters. Twitter deleted the post after the twitter subscriber was attacked by other Twitter subscribers*.

*Law Enforcement Today 07.12.2020

Twitter and other social media platforms have no problem censoring U.S. citizens while enabling Chinese government officials and citizens to spread influence, misinformation and propaganda on their platforms with impunity.

As an example of tech based hybrid warfare, users from China and Russia have opened millions of accounts on Facebook, Twitter and other social media platforms in order to intentionally spread misinformation to influence elections, cause discourse between citizens and spread propaganda painting their governments in a positive light.

U.S. social media subscribers, including teens and children, have no idea that they are often being misled by government officials and operatives who are members of the Chinese Communist Party ("CCP") or Russian government.

Aside from users from China and Russia, politicians and political groups around the world are using these social media platforms to spread influence and misinformation around the world leading to people being imprisoned, tortured and even killed.

For example, a Muslim tea shop owner in Mandalay, Myanmar, was falsely accused of rape*. The false accusation was posted on Facebook leading to riots which ended in violence and death yet people injured or killed have no way to sue Facebook due to the fact Facebook users are not indemnified (protected), arbitration and government protection.

*Wired 07.06.2018

Myriad-centric algorithms developed by social media companies, such as Facebook, for advertising purposes enable social media companies to aggregate data by categories.

However, governments can use the algorithms to identified social media subscribers who may be posting anti-government sentiments and/or what could be misidentified as anti-government sentiments leading to subscribers being arrested by their governments.

The misuse of myriad-centric algorithms is not a theory, in 2018 Forbes reported that 65,000 Russian Facebook subscribers could be identified as committing treason placing the Russian citizen in grave danger of being arrested and possibly tortured or killed by way of an algorithm vs. hard evidence or facts*.

*Forbes 7.20.2018

Social media users as well as app and platform users need to realize that state actors, good or bad, are partnering with tech giants to use social media platforms, apps and other platforms as surveillance and data mining tools in order to suppress civil liberties, oppress, arrest, torture and kill end users.

Tech giants such as Amazon are selling end user data to law enforcement agencies* while telecom providers such as AT&T, Verizon, T-Mobile and Sprint have been caught selling their customer's location information to data brokers such as Zumigo and LocationSmart who in turn have sold the location data to law enforcement agencies**.

*The Guardian, 08.30.2020 **USA Today, 02.28.00

Google has also been caught selling end user information to law enforcement agencies regarding a user who was falsely accused of a burglary because his location information put him in the vicinity of a house that was burglarized causing the user to hire a lawyer at his own expense*.

*NBC News, 03.07.2020

A 9 year old boy was shot 4 times, in Atlanta, GA, while filming a TikTok video for his mother*. This is tragic in many ways plus the fact that the boy was not old enough, by law, to even be on the TikTok platform since Child Online Privacy Protection Act (FTC-"COPPA") states that children under 13 cannot be exploited for profits at the expense of privacy. This is an example of the fact that the FTC nor State AGs are enforcing existing consumer laws.

*AJC, Atlanta News, 07.11.2020

These tech giants are fighting laws regulating their use of end user personal and professional information, including the use of biometric data such as facial recognition data*.

*03.08.2020, The Wall Street Journal

End users are not sure if their personal and professional information is being used, shared, sold, aggregated or stored in a manner that can bring harm to the end user.

However, these recent news stories are confirming that end user personal and professional information (Digital DNA) is ending up in the hands of entities that can bring harm to the end user such as law enforcement agencies, political parties, and state actors from countries such as China and Russia.

Until these recent news stories, people had no idea that they were in fact paying for smartphones, tablet PCs or connected products that could bring them harm as a result of the intrusive operating systems, apps and platforms that support all products concerned.

Due to these recent revelations, government agencies need to start enforcing existing consumer protection laws in order to protect consumers from intrusive, exploitive and harmful business practices that are rooted in Surveillance Capitalism.

Furthermore, elected officials need to draft new legislation in the form of an Electronic Bill of Rights as new consumer protection laws are needed due to the evolution of technology.

The Need for an Electronic Bill of Rights

The only protection individuals have against predatory surveillance and data mining business practices is the law.

Per my research, many existing consumer laws are simply not being enforced by relevant government agencies within the U.S. or globally when it comes to tech giants such as Google, Apple, Microsoft, Amazon, Facebook and Twitter.

In closing, consumer protection laws in the form of an Electronic Bill of Rights needs to be passed by legislators at the state and federal level domestically and globally.

I will be writing follow up articles addressing many of the issues in this article plus other in great detail for the Vision Times.

Rex M. Lee is a Cybersecurity & Privacy Advisor/Tech Journalist. For more information contact Rex at RLee@MySmartPrivacy.com *or go to My Smart Privacy at: www.MySmartPrivacy.com*