Article

BIG TECH'S MONOPOLY OVER THE GIG-ECONOMY: HOW GOOGLE, APPLE, AND MICROSOFT CONTROL ACCESS TO THE INTERNET

BY REX M. LEE

Big Tech's Monopoly over The Gig-Economy:
How Google, Apple, and Microsoft Control Access to the Internet

By Rex M. Lee

There are numerous threats to antitrust, fair competition, civil liberties, privacy, cybersecurity and the free flow of information associated with the handful of tech giants whom control access to the internet while monopolizing the "*Gig-Economy*".

These threats need to be addressed by consumers of tech & telecom products, business leaders, consumer advocate groups, government officials and law makers around the world.

Before we get into what the threats are and what needs to be done, let's take a look at the companies that dominate access to the internet plus monopolize the gig-economy including online publishing and distribution.

Today only a handful of multinational tech giants truly monopolize the gig-economy while controlling how consumers of tech access the internet by way of the operating system ("OS") and intrusive preinstalled apps that support numerous tech and telecom products such as smartphones.

People will find it interesting and concerning that the top 10 companies that are monopolizing the gig-economy are based in the USA and China.

Enclosed below is the list of the top ten tech giants including their annual revenues:

1.	Amazon	$232 Billion	USA
2.	Google	$120 Billion	USA
3.	JD.Com	$67 Billion	China
4.	Alibaba	$56 Billion	China
5.	Facebook	$55 Billion	USA
6.	Tencent	$44 Billion	China
7.	Netflix	$15 Billion	USA
8.	Bookings	$12 Billion	USA
9.	Baidu	$12 Billion	China
10.	e-Bay	$10 Billion	USA

*Source Wikipedia

Major Threats Associated with Limited Competition

There are many threats to tech and telecom product users that need to be addressed due to the fact that only a handful of companies from the U.S. and China are monopolizing the gig-economy.

Major threats include the following:

1. The Surveillance Capitalism Business Model. Many people view most tech giants as application and platform developers such as Google, Facebook, Amazon, Baidu, Tencent (WeChat) and ByteDance (TikTok).

However people need to realize that these tech giants have adopted a Surveillance Capitalism business model. This means that these tech giants are in the business of acquiring personal and professional information ("Digital DNA") from consumers of tech/telecom products and services by way of surveillance and data mining business practices.

Tech and telecom products that are supported by surveillance and data mining business practices include:

- Operating Systems- android OS (Google), Apple iOS and Microsoft Windows OS
- Applications & Social Media Platforms
- Smartphones
- Tablet PCs
- Internet subscriptions- music, TV, movies, books, news media and so on
- Voice automated assistants- Amazon Alexa, Google Assistant, Apple Siri and MS Crotona
- IoT/IIoT devices
- PCs in general
- Electronics- TVs, appliances, toys, gaming systems and so on
- In-home security & environmental control systems- Amazon Ring, Google Nest and so on
- Wearables
- Connected Vehicles
- Connected products in general

All of this means that the use of smartphones, PCs, electronics, automobiles, TVs and other products of necessity are no longer private or secure due to surveillance and data mining business practices.

2. Threats to Civil Liberties, Privacy, Cybersecurity and Safety. There are numerous threats associated with the collection of personal and professional Digital DNA that include threats to civil liberties, privacy, cybersecurity, and safety.

Most smartphones, PCs, TVs, and connected products in general are supported by intrusive apps, GPS, cameras, microphones and voice automated assistants which enable tech giants to conduct audio, video and physical (track by location) surveillance on the product user while being able to data mine the product user 24x7/365 days per year whether the user is an adult, child or business professional.

In essence our homes, vehicles, places of work, and places we go to have been invaded by intrusive tech and telecom providers who are surveilling and data mining 100% of our personal and professional lives for financial gain by way of the products and services we are paying for.

This leads to tech and telecom product user exploitation. This means that adults, teens, children and business professionals are being exploited for financial gain at the expense of privacy, cybersecurity, civil liberties and safety.

It is bad enough to lose privacy but to be exploited for financial gain at the expense of privacy should be unacceptable by any free thinking individual.

3. Acquisition of Digital DNA- Tech & Telecom Product User Exploitation. For example companies such as Google, Apple, Microsoft, Facebook and Amazon are mostly valued, by Wall Street, for their ability to conduct surveillance on their product users while data mining their product users in order to collect the

most valuable resource on earth which is a person's "Digital DNA" (personal and professional information).

After collecting a tech or telecom product user's personal and professional Digital DNA, these tech giants make a digital profile of the user and then sell the user's Digital DNA for financial gain at the expense of the product user's privacy, cybersecurity, civil liberties and safety even if the product user is a child.

In essence tech and telecom product users are viewed by tech giants as *"uncompensated information producers"* whom are to be exploited for financial gain whether the product user pays for the products and services or receives the products and services for free.

Similar to the movie the Matrix, people are being enslaved by tech and telecom giants in order to produce personal and professional Digital DNA to be exploited for financial gain without being compensated for producing the Digital DNA which is illegal according to most consumer laws that are not being enforced.

This leads to forced participation and digital oppression.

4. Forced Participation & Digital Oppression- Cyber Enslavement. You can consider that tech and telecom product users are being forced to participate within a highly exploitive and oppressive business model (Surveillance Capitalism) due to a lack of consumer choice since companies such as Google, Apple and Microsoft all have adopted surveillance and data mining business practices.

This is significant because Google, Apple and Microsoft are the three dominate operating system developers which means that their operating systems support 100% of all tech and telecom products concerned giving consumers of tech and telecom products little or no choice regarding tech and telecom products that can be secured and privatized.

Don't take my word for this, Verizon and T-Mobile have admitted that products such as smartphones tablet PCs and connected products supported by the android OS, Apple iOS and Microsoft Windows OS are not private or secure forms of telecommunications and mobile 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*

This means that Google, Apple and Microsoft truly control access to the internet which means that only a handful of companies are monopolizing the gig-economy.

5. Google, Apple & Microsoft- The Gateway to the Internet and Gig-Economy.

The fact that Google, Apple and Microsoft are the three dominate operating systems in the world and offer virtually no secure and private solution leads to violations of antitrust and unfair business competition laws that need to be addressed by government agencies and law makers around the world.

Users of the android OS, Apple iOS and Microsoft Windows OS have become commodities for sale by Google, Apple and Microsoft whom sell access to their OS product user to other multinational tech giants.

If one can control access to the tech and telecom product user, then one can control access to the internet and monopolize the gig-economy by way of the OS, preinstalled apps and intrusive platforms.

The key to controlling access to the internet resides within the OS and intrusive preinstalled apps that cannot be uninstalled or controlled by the tech and telecom product owner and/or user.

5. Buying Access to the Google, Apple & Microsoft OS Product User. Companies such as Amazon, Facebook, Twitter, Baidu, Tencent and ByteDance pay Google, Apple and Microsoft billions of dollars to gain access to the OS product user by way of intrusive preinstalled apps and platforms.

Additionally, intrusive tech and telecom giants can buy access to the OS product user by way of third-party apps and platforms that are distributed via Google Play, Apple App Store and Microsoft App Store.

That fact that only three companies, Google, Apple & Microsoft, dominate the OS market leads to potential violations of existing antitrust and unfair competition laws due to the fact that Google, Apple and Microsoft are truly the gate keepers to the internet and the gig-economy.

6. Violation of Antitrust and Unfair Competition Laws. Due to this monopoly over access to the internet and the gig-economy, government agencies and law makers around the world need to address these threats and potential violations of existing antitrust and unfair competition laws.

Aside from threats to privacy and civil liberties, limited competition also leads to threats to innovation, since smaller companies and/or startups do not have the financial resources to pay billions of dollars to Google, Apple and Microsoft for access to the OS product user by way of preinstalled apps that cannot be uninstalled by the product owner and/or user.

One of the major factors other than dominance over the OS, is the fact that preinstalled apps developed by companies such as Facebook and Amazon cannot be uninstalled from products such as smartphones due to exclusive agreements with companies such as Google, Apple and Microsoft.

The inability to pay for access to compete against companies such as Facebook and Amazon leads to limited competition which leads to threats innovation, civil liberties, privacy, safety and the free flow of information regarding online publishers and news organizations.

7. Cybersecurity Threats to Corporate Information- Unfair Competition. An example of unfair competition is the fact that tech giants Google, Apple, Microsoft, Amazon, Baidu, Tencent and Facebook compete in hundreds of industries worldwide yet governments around the world are enabling these companies to surveil and data mine tech and telecom products users by way of the user's smartphone and PC.

This means that employees, managers and executives whom work for companies that compete against these tech giants are being forced into using intrusive tech and telecom products developed by their business competitors due to a lack of choice regarding an operating system that can be truly secured and privatized.

This means that companies that compete against these tech giants are actually exposing their confidential and protected corporate information to their business competitors especially companies that employ bring your own device ("BYOD") programs.

Companies such as Google, Apple and Microsoft have a huge advantage over their business competitors simply by the fact that they are the developers of the OS plus numerous intrusive apps and platforms that are intentionally designed to enable these OS developer to monitor, track and data mine their OS product user's for financial gain by way of tech and telecom products such smartphones and PCs.

How do you not become the most powerful companies in the world when you are enabled to monitor, track and data mine adults, teens, children and business professionals by way of smartphones and PCs?

The Need for Law Enforcement and an Electronic Bill of Rights

Regarding the U.S., it is time for government agencies such as the Federal Trade Commission ("FTC") and state attorney generals ("AGs") to enforce existing antitrust and unfair competition laws.

Additionally, law makers at the state and federal level need to pass new legislation in the form of an "Electronic Bill of Rights" that will give the consumer of tech and telecom products full control over their personal and professional Digital DNA while protecting the consumer from predatory surveillance and data mining business practices that are rooted in Surveillance Capitalism.

If government agencies, state AGs and law makers do not address these critical threats and violations of the law, consumers of tech and telecom products will continue to be exploited for financial gain at the expense of civil liberties, privacy, cybersecurity and safety.

In closing, predatory surveillance and data mining business practices rooted in Surveillance Capitalism pose additional threats to online publishers, competition, innovation and the free flow of information.

Consumers of tech and telecom products are entitled to choice plus control over their personal and professional Digital DNA.

It is time for the digital oppression and cyber tyranny to stop or we will continue to lose our civil liberties one liberty at a time while being dominated by oppressive tech and telecom providers bent on exploiting their paying customers for profits.

My next article for the Vision Times will be centered on Digital Authoritarianism and Cyber Oppression.

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