Article

BIG TECH'S MONOPOLY OVER ACCESS TO THE ONLINE MARKET PLACE: HOW GOOGLE, APPLE, AND MICROSOFT CONTROL ACCESS TO THE INTERNET

BY REX M. LEE

Big Tech's Monopoly over Access to the Online Market Place:

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 that control access to the internet.

These threats need to be addressed by consumers of technology, consumer advocate groups, business leaders, 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 dominate the online market place including online publishing.

Today only a handful of tech companies are dominating access to the internet, online market place, and online publishing around the world which include the following top 10 companies.

The top ten* internet companies in the world today are companies from the U.S. and China which include:

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

The first major threat is associated with surveillance and data mining business practices associated with intrusive apps.

Surveillance Capitalism- Intrusive Apps

Most of the world's largest internet companies employ surveillance and data mining business practices that are rooted in Surveillance Capitalism which is a threat to civil liberties, privacy, cybersecurity and the free flow of information.

All of these companies have one thing in common which is all of these companies develop intrusive applications that support smartphones, tablet PCs, connected products and PCs that are supported by the android OS, Apple iOS, and Microsoft Windows OS.

Apps are nothing more than legal malware which means that apps are intentionally developed to enable the app developer with the ability to monitor, track, and data mine the app user for financial gain at the expense of the user's civil liberties, cybersecurity and privacy.

Intrusive apps are also supported by predatory terms of use which enable the app developers with the ability to lawfully surveil and data mine their app user's for financial gain so keep this in mind the next time that you click on "I Agree" without reading the terms of use.

Tech giants distribute their intrusive apps through online app stores such as Google Play, Apple App Store, and Microsoft App Store.

Additionally, many of these companies cut agreements with operating system (OS) developers such as Google, Apple, and Microsoft whom are responsible for developing the android OS (Google), Apple iOS and Microsoft Windows OS.

Google, Apple, and Microsoft are the dominant OS developers is the world which means that the android OS, Apple iOS and Microsoft Windows OS support billions of smartphones, tablet PCs, connected products, and PCs around the world.

This means that Google, Apple and Microsoft control access to the internet through intrusive apps, widgets, and other content that supports smartphones, tablet PCs, connected products and PCs in general.

The Death of the URL equals the Death of Fair Competition

Rarely do people physically type in a *Uniform Resource Locator (URL)* to access a website anymore, but rather people simply touch, tap or click on an app to access the internet.

Using an app to access the internet vs. using a URL is highly relevant to the strategy used by the top internet companies in regards to dominating access to the internet and online market place.

In short, eliminating the need for a person to use a URL to access a website by way of an app gives the user a convenient and easy way to access their favorite websites by simply touching, tapping or clicking on an app icon that supports their favorite device.

Apps also give the app developers a way to make sure that the app user connects to their site through the most convenient way possible which is a one touch, tap or click method.

This one touch, tap or click method, associated with apps, is the key to dominating access to the internet through agreements between app and platform developers such as Facebook and OS developers such as Google, Apple, and Microsoft.

The power brokers who really control access to the internet are Google, Apple and Microsoft because the top internet companies in the world must first go through the OS developer in order for their apps to be distributed to tech and telecom product users around the world.

Google, Apple and Microsoft- The Gateway to the Internet

For lack of a better metaphor, think of Google, Apple or Microsoft as the tech version of a mafia crime family such as the Sopranos, Gambino and Corleone families depicted in films and TV.

Google, Apple and Microsoft, by the most part, control access to the internet by virtue of the android OS, Apple iOS and Microsoft Windows which makes these companies some of the most powerful companies in the world.

Google, Apple and Microsoft control what companies are enabled to distribute their intrusive apps through Google Play, Apple App Store and Microsoft Windows App Store.

In addition, Google, Apple and Microsoft also cut deals with other tech giants regarding which companies are enabled to develop preinstalled apps, widgets, emojis and other content that support billions of tech and telecom products worldwide.

Consequently, tech giants such as Amazon, Facebook, Tencent and Baidu must first go through Google, Apple, and Microsoft in order to have their intrusive apps distributed via online app stores or distributed as preinstalled content.

OS Product Users for Sale to the Highest Bidders

Unfortunately, users of the android OS, Apple iOS and Microsoft Windows OS are sold off to the highest bidders in relation to preinstalled app developers such as Amazon, Facebook, Baidu and Tencent.

Google, Apple and Microsoft will state that they do not sell their OS product user's "identifiable" personal information to third-party advertisers which their online terms of use state.

However, what Google, Apple and Microsoft do not divulge to their OS product user is the fact that the each company will sell access to their OS product user to intrusive app developers such as Amazon, Facebook, Baidu and Tencent whom employ predatory surveillance and data mining business practices.

Companies such as Amazon, Facebook, Baidu and Tencent pay billions of dollars to Google, Apple and Microsoft in order to gain access to the android OS, Apple iOS and Microsoft Windows OS user.

Even OS developers pay each other billions of dollars in order to gain access to the OS product user such as the case with Google paying Apple billions of dollars to gain access to the Apple iOS user through Safari* and Siri**.
*Source Fortune **Source Fortune

Tim Cook, Apple CEO, likes to talk up privacy***, but at the same time Mr. Cook is not divulging the fact that Apple sells the iOS product user off to the highest bidders which include Google who also employs predatory surveillance and data mining business practices.
*** Source Time

Antitrust- Controlling the Tech Product User & Forced Participation

Tech and telecom product users, around the world, have virtually no choice but to use smartphones, tablet PCs, connected products and PCs that are supported by the android OS, Apple iOS and Microsoft Windows OS.

This means that tech and telecom product users are being forced to use smartphones, tablet PCs, connected products and PCs that are supported by intrusive preinstalled apps developed by the top tech companies in the world who employ predatory surveillance and data mining business practices.

Consequently, telecom products such as smartphones are not private or secure forms of telecommunications and computing according to T-Mobile and Verizon due preinstalled surveillance and data mining technology in the form of apps:

- 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*

Control over the OS means that Google, Apple and Microsoft are responsible for what preinstalled apps, widgets, emojis and other content that can or cannot be disabled, controlled or uninstalled from the host device such as a smartphone.

Even though a person may own a device such as a smartphone, the device owner is restricted from being able to uninstall many apps such as the Amazon or Facebook app which in essence forces the user to use Amazon as their primary online retailer or Facebook at their primary social media platform ensuring that Amazon and Facebook have a clear advantage over existing or future competitors.

The fact that tech and telecom product users cannot uninstall 100% of the preinstalled apps that support all tech and telecom products concerned is a clear example of antitrust plus unfair competition practices.

Many new tech startup simple cannot afford to pay Google, Apple or Microsoft billions of dollars to compete with established tech giants such as Amazon, Facebook, Tencent, and Baidu.

Limited Competition- Threats to Innovation, Civil Liberties, Cybersecurity, Privacy and Information

Due to the fact that only a few tech giants are controlling access to the internet, by way of operating systems and apps, has a huge impact on competition and innovation.

Unlike the 90's and early 2,000's when we saw innovation and competition driving the internet, today only a few companies are in true control over access to the internet, online market place, and online publishing.

Today we are seeing the tech giants that control access to the internet practically eliminating competition from new companies while leveraging their existing competition forcing either an acquisition or forcing the company completely out of business.

Alphabet Inc. (Google) is a great example of how Surveillance Capitalism has been successful considering they have participated in over 200 mergers and acquisitions**** since 2001 enabling Google to compete in numerous industries worldwide.
**** Source Wikipedia

Regarding mergers and acquisitions*****, Amazon is on the rise while not only forcing companies out of business but practically killing whole industries in the process as noted in numerous stories regarding traditional retailers whom are shuttering their doors and/or are in chapter 11.
***** Source Business Insider, June, 2018

Below is a list of 10 industries threatened by Amazon due to Surveillance Capitalism:

- Electronic Retailers
- Consumable Manufacturers
- Department Stores
- High-End Department Stores
- Food Delivery Business
- Book Stores
- Grocery Stores
- Healthcare Companies
- Pharmacy
- Package Delivery & Logistics

Big Tech's Advantage- Computers and Telecommunications are No Longer Private

Aside from Google and Amazon, numerous tech giants are also competing in many industries worldwide by way of mergers and questions yet government agencies such as the FTC and state AGs are ignoring the fact that these companies are enabled to surveil and data mine tech and telecom product users via smartphones, tablet PCs, connected products, and PCs.

For example, below are the total number of mergers and acquisitions associated with Google, Apple, Microsoft, Facebook, and Amazon:

- Alphabet Inc. (Google) over 200 dating back to 2001
  Source Wikipedia: https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Alphabet
- Apple over 100 dating back to 1988
  Source Wikipedia: https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Apple
- Microsoft over 200 dating back to 1987
  Source Wikipedia: https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Microsoft
- Facebook has been involved with over 75 mergers and acquisitions since 2005
  Source Wikipedia: https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Facebook
- Tencent out spent Alibaba and Baidu regarding mergers and acquisitions:
  https://www.scmp.com/business/companies/article/2098548/tencent-leads-baidu-alibaba-when-it-comes-ma-deals
- Amazon over 90 since 1998
  Source Wikipedia: https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Amazon

Think about it, when a company can lawfully monitor, track and data mine a person through physical surveillance methods such as tracking a person by way of a smartphone while monitoring and data mining

the individual's telecom related activities associated with the use of a smartphone, that company will have a huge advantage over any of their competitors.

For example in the U.S., It should be illegal for any company that competes in many industries worldwide to surveil and data mine telecom and PC product users by way of smartphones, tablet PCs, connected products, connected vehicles and PCs that are supported by protected telecom infrastructure regulated by the FCC.

Cybersecurity Threats Posed by Surveillance Capitalism- Antitrust & Unfair Business Competition

Companies that have adopted smartphones, tablet PCs, and PCs supported by the android OS, Apple iOS and Microsoft Windows OS may be leaking confidential and protected information to numerous multinational companies, including companies from China and Russia, by way of the preinstalled apps that support the tech and telecom related products.

Pending the industry companies compete in, these companies may be leaking confidential corporate information to tech giants, whom are their business competitors, while leaking confidential corporate information nation-state companies from China and Russia.

Cybersecurity Threats Posed by Great Power Competition- China & Russia

Due to Great Power Competition from China and Russia, foreign companies enabled to conduct surveillance and data mining by way of tech and telecom products would be no different than if companies from Germany, Italy and Japan were enabled to conduct surveillance and data mining on U.S. citizens, companies, government officials, and elected officials by way of electronics and telephones pre-WWII.

Imagine the treasure trove of personal, professional, corporate, and government information the Nazi's would been able to cultivate from U.S. citizens pre-WWII had a company like T-Mobile been enabled to surveil and data mine U.S. citizens by way of electronics, vehicles and telephones.

It is a huge threat to U.S. national security, cybersecurity, and the economy to allow nation-state companies from China and Russia such as Baidu, Tencent, Prisma Labs and Kaspersky Lab to monitor, track and data mine U.S. tech and telecom product users by way of tech and telecom related products such as smartphones, tablet PCs, connected products and PCs that are supported by protected telecom infrastructure regulated by the FCC.

For example, U.S. citizens do not realize that a smartphone is an integrated cellular telephone, GPS tracker and computer that is supported by protected telecom infrastructure regulated by the FCC which means that a smartphone is no less significant than a home or office phone and PC.

Domination of Digital Media and Publishing- Citizen Kane in the 21st Century

It has been no secret that companies such as Google, Facebook, Twitter, Tencent and Amazon are dominating publishing which is a threat to civil liberties that include privacy, free speech plus the free flow of information and ideas due to the fact that these companies can lawfully censor participation for any reason as stated in their terms of use.

Online publishers are running into financial problems as well due to the fact that tech giants are dominating online publishing so consequently the free flow of information and ideas plus free speech are in jeopardy.

Online publishers in are feeling the effects of tech related mergers and acquisitions along with the fact that their biggest competitors for ad dollars also control most of the access to the internet and online market place due to the ability to control access to the internet via preinstalled apps that support billions of tech and telecom related products.

By way of mergers and acquisitions, Amazon is also dominating publishing by owning book publishing companies along with media such as the Washington Times.

Amazon not only enjoys a competitive edge regarding their surveillance and data mining products such as their apps which are supported by their voice automated assistant "Alexa" but they also control the distribution of media such as books, movies, music, TV shows and news.

In regards to William Randolph Hearst, Former Media Mogul, and Jeff Bezos, Founder & President of Amazon, the movie Citizen Kane is more relevant today in regards to the domination of media by one person as it was when it was released in 1941.

If Citizen Kane was rebooted today, you could replace the character Charles Foster Kane with a figure such as Jeff Bezos.

It is astonishing how life is reflecting art in today's connected world yet governments around the world are not responding to these threats to completion, innovation, privacy, free speech or the free flow of information and ideas through new regulations and/or laws limiting the number of industries companies can compete in.

Censorship by Way of Proxy- Corporate Surveillance & Digital Tyranny

Regarding nation-state companies from China such as Tencent and Baidu, it is expected that the Chinese communist party (government) will drive censorship but in the West we are seeing the rise of censorship by proxy as governments are leaving censorship up to tech giants whom do not have to follow the same rule of law that a legitimate publisher has to follow.

We are living in the Surveillance Age which is giving the rise to Digital Tyranny and Discrimination either by governments such as China, Russia, Iran, and North Korea or by companies such as Amazon, Facebook, and Google.

In closing, limited competition regarding tech and telecom giants poses threats to innovation, civil liberties, cybersecurity, privacy plus the free flow of information and ideas.

These threats need to be addressed by consumers of tech and telecom products, consumer advocate groups, civil libertarians, business leaders, government officials and elected officials due to the numerous threats to tech and telecom product users worldwide.

Regarding the U.S., until the FTC, FCC, DOJ, state AGs, and law makers address these threats, Google, Apple, Microsoft, Facebook and Amazon will continue to rule the online world along with dominion over our politicians.

If you don't believe me, maybe you will believe Erich Schmidt*, former Chairman, Alphabet Inc. (Google) as he explains how tech giants buy influence in Washington D.C. by way of powerful lobbyist:

- *"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."*

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

Rex M. Lee is Cybersecurity and Privacy Advisor and BLACKOPS Partners Senior Tech and Telecom Analyst. For more information go to My Smart Privacy at: www.MySmartPrivacy.com Plus follow Rex on Twitter @RexMLee1