How Tech Giants Collect Personal and Professional Info And Rape Your Family

BY REX M. LEE

Commentary

This article is part of a series on corporate surveillance highlighting civil liberty, privacy, cyber security, safety, and tech-product user exploitation threats associated with connected products that are supported by the Android (Google) OS, Apple iOS, and Microsoft Windows OS.

In the first article of this series, Surveillance Capitalism: Monetizing the Smartphone User, we learned that a person's personal and professional ("collective") digital DNA is the most valuable commodity in the world.

We also learned that data-driven technology providers such as Google, Apple, Microsoft, Facebook, Amazon, and Baidu are collecting, using, sharing, selling, purchasing, and aggregating a person's collective digital DNA for financial gain without compensating the product user who produced the collective digital DNA in the first place. This is simply called "tech-product user exploitation."

In essence, tech users have become uncompensated information producers who are being exploited for financial gain at the expense of the user's civil liberties, privacy, cyber security, and safety, whether the user is an adult, child, or business professional.

A person's collective digital DNA, associated with the use of all active smartphones around the world, is worth billions—if not trillions—of dollars on the open market, and Google, Apple, Microsoft, and other tech giants are in a race to collect and exploit that collective digital DNA.

As per my last article, data-driven technology providers do not directly sell a user's collective digital DNA to third parties such as advertisers. All parties sell access to the user via intrusive and exploitative content such as web browsers (see Apple–Google example below) and intrusive apps that are pre-installed into the product and/or distributed via app stores.

Tools to Harvest Digital DNA

There are many methods data-driven technology providers use to collect a person's collective digital DNA, including predatory operating systems (OSs), intrusive content (apps, widgets, etc.), social media platforms, and exploitative terms of use.

Let's look at operating systems and apps.

Think of the OS as prime real-estate. The OS is key in that many companies such as Google, Amazon, Facebook, and Baidu will pay the OS developers billions of dollars for access to the product user, which is the case with Google and Apple, even though Google is an OS developer as well.

In 2014, Google paid Apple $1 billion so that Google would be the default search engine on the pre-installed Safari web browser on the Apple iPhone. The iPhone user was unable to uninstall the intrusive Google product (though could switch default search engines in later

versions of iOS), forcing the iPhone user to accept Google's exploitative terms of use.

Google is reportedly set to pay Apple as much as $9 billion in 2018 and $12 billion in 2019 to maintain their status as the default search engine for the Safari web browser. The Apple-Google deal is a prime example of how the tech-product user is bought and sold on the open market.

Why is Google paying Apple billions of dollars to gain access to Apple product users? Because Google does not want anyone to escape its grasp.

Many Apple users who don't want anything to do with Google are unaware of the fact that Tim Cook—and/or Apple—sold them out to Google without asking.

World Domination

Google, Apple, and Microsoft are the three dominant OS developers, which means that these three companies are the gateway to a user's collective digital DNA associated with a product supported by the Android OS, Apple iOS, or Microsoft Windows OS.

Google, Apple, and Microsoft are all in the hardware manufacturing business as well, but all companies concerned cut deals with technology product manufacturers to have their respective operating systems adopted by the original equipment manufacturer (OEM), such as Sony, Samsung, LG, HTC, Ford, and the list goes on.

Controlling the OS of a connected product puts Google, Apple, and Microsoft in control of which companies are enabled to develop uncontrollable, pre-installed content that is programmed to give the content developer the ability to monitor, track, and data mine the product user for financial gain.

Pre-installed content developers have a huge advantage over third-party (e.g. Google Play) content developers because, in most cases, intrusive pre-installed content cannot be controlled, disabled, or uninstalled by the product user because the content is rooted.

Apple, Google, Microsoft, Amazon, and Facebook have collectively become the most valuable companies in the world due in part to the collection and use of a person's collective digital DNA rather than just driving revenues from the sale of hardware, software, automated voice technology, social media services, books, movies, and other retail products.

Companies that can surveil and data mine telecom subscribers via telecom-related products, such as smartphones, have a huge advantage over all other competitors.

Legal Malware

Think about it, companies such as Google, Apple, and Microsoft control the OS that supports billions of telecom-related products, such as smartphones and tablet PCs, that are supported by protected telecom infrastructure governed by the Federal Communications Commission (FCC). A smartphone is actually a cellular telephone with an integrated PC.

In essence, all companies concerned have found a way to wiretap the collective telephones and PCs of billions of individuals, children, businesses, professionals (doctors, attorneys, journalists), business leaders, government officials, members of the military and law enforcement, and even law makers from around the world.

How does a company not become one of the most powerful companies in the world if that company is enabled to monitor, track, and data mine telecom subscribers via telecom-related devices supported by protected telecom infrastructure governed by the FCC?

How did all parties do it? Answer: They control the OS of all products concerned, plus support them with Trojan horse malware in the form of an app.

The tech-product user has become the product for sale, but the issue is much worse, because the user is being exploited for financial gain via telecom-related and retail products that require payment to participate, such as smartphones, tablet PCs, TVs, vehicles, voice-automated products, and so on.

How did we allow ourselves to be exploited for financial gain at the expense of privacy by the very tech companies we patronize with our trust, loyalty, and hard-earned money? Answer: So-called “free stuff.”

Surveillance and data-mining business practices rooted in surveillance capitalism is a business model that initially supported “free stuff,” such as web browsers, software, apps, online services such as social media sites, and video games including Angry Birds and Candy Crush Saga.

However, connected products and services that require payment to participate, such as smartphones,

are supported by the surveillance capitalism business model that has been adopted by the three dominant OS developers Google, Apple, and Microsoft.

Now you understand the significance regarding the ability to control the OS of a connected product.

The Silicon Valley Matrix

Google, Apple, and Microsoft also develop intrusive content such as apps, widgets, and emojis, which are simply programmed to give the content developer the ability to take full control of a connected product, such as a smartphone, tablet PC, TV, vehicle, toy, voice-automated product, and so on.

Sensors, network connectivity, and hardware that can be controlled by content developers include the accelerometer (navigation, motion, etc.), Global Positioning System, cellular network, WiFi, Bluetooth, nearfield communications, secure digital (SD) card, subscriber identity module (SIM) card, power synchronization cable, bio-metric authentication, environmental sensors, camera, microphone, and volume control.

In addition, intrusive content, such as apps, is also designed to give the content developer the ability to use the sensors (e.g. GPS/accelerometer) and hardware (e.g. camera/microphone) in order to surveil the product user 24 hours a day, 7 days a week, 365 days a year, while also enabling the content developer to data mine surveillance data (e.g. location data) and sensitive user data generated by the product user.

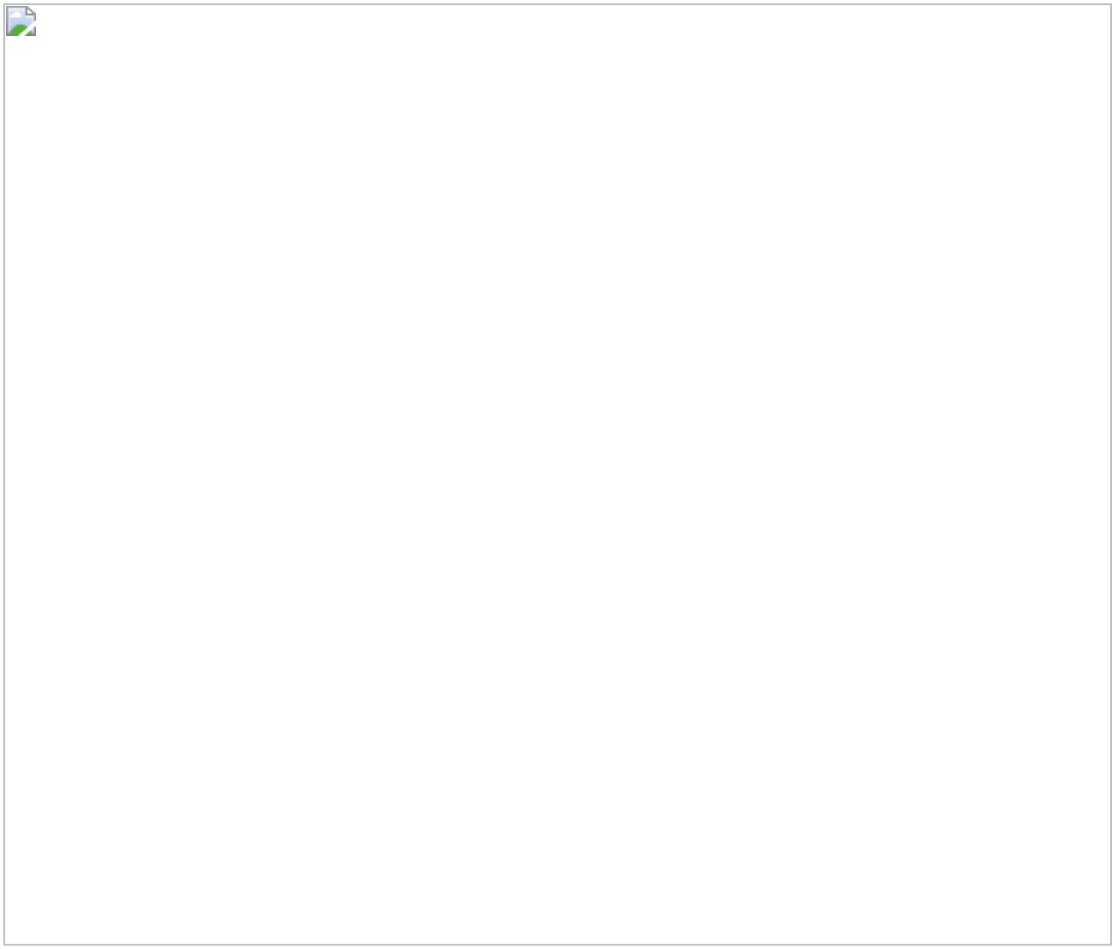
Don’t take my word for any of these claims, read the unpublished (hidden in device) Android app permissions associated with intrusive pre-installed Android (Google) apps that the product user cannot uninstall, control, or disable in many cases.

Control over hardware such as the camera, microphone, and volume control gives content developers the ability to take pictures plus record audio and video without user consent or knowledge. (Screenshot via Rex M. Lee)

Intrusive content, such as apps, is also programmed to conduct multi-source data mining, meaning that the apps are programmed with the ability to reach beyond the host device (e.g. smartphone) to collect a person’s collective digital DNA from multiple connected sources (e.g. TV, vehicles, social media services, etc.) owned by the product user.

As discussed in my previous article, companies such as Google and Facebook will exploit the addictiveness of their products for financial gain, even at the expense of the product user’s safety, whether the product user is an adult, child, or business professional.

Through the Android Baidu web browsers and apps distributed via Google Play, these companies will even sell their product users out to countries such as China.



Google distributes Chinese surveillance and data mining technology via Google Play. (Screenshot annotated by Rex. M. Lee)

Anybody who downloads Android Baidu products, such as the web browser shown above, is agreeing to give Baidu the ability to monitor, track, and data mine their collective digital DNA at all times.

A person's personal and professional digital DNA is made up of surveillance data, sensitive user data, and multisource data acquired via multisource data mining.

The collective digital DNA collected from a single smartphone user by all parties concerned is astonishing and horrifying to say the least.

As a result of uncontrollable, pre-installed content (OS, apps, etc.) that the tech-product user cannot uninstall, there can be as many as 15 or more companies from around the world, including companies from China, that are enabled to simultaneously monitor, track, and data mine a single smartphone user depending on the OS.

All companies concerned are collecting nearly 100 percent of all surveillance and sensitive user data associated with the use of the device, plus collective

digital DNA acquired from multiple sources connected to the host device.

It is clear that predatory surveillance and data-mining business practice rooted in surveillance capitalism need to be addressed by the FCC, Federal Trade Commission, Department of Homeland Security, state attorneys general, law makers, and telecom providers because of civil liberty, privacy, cyber security, safety, and tech product user exploitation threats.

In the next article, I will explain how the terms of use give all companies concerned the ability to monitor, track, and data mine a tech-product user for financial gain.

Rex M. Lee is a privacy and data security consultant and Blackops Partners analyst and researcher: www.MySmartPrivacy.com