Nov 2017- Money Masters

Connected Product- Electronic Bill of Rights Part 1.

By Rex M. Lee

My last two installments centered on the FTC and getting answers to privacy and consumer exploitation concerns pertaining to intrusive preinstalled technology that supports connected products such as smartphones. The FTC has since declined to answer any more questions so now I'm appealing to law makers. Since I live in the state of Texas, I've contacted the office Ted Cruz, U.S. Senator- Texas.

On November 14th, 2017 I was able to meet with a representative for Senator Ted Cruz at the Senator's office in San Antonio, TX. The representative was surprised at how much personal and professional information preinstalled technology (apps, widgets, etc.) developers were acquiring from smartphones.

She suggested that I author a "Policy Change Proposal" centered on an electronic bill of rights which is something I've been working on for several years. She asked me to submit the proposal to the Senator's office and she would make sure it was circulated to law makers in Washington D.C. to be considered for a bill.

Due to my findings coupled with an admission from a big four carrier that smartphones are not a private form to telecommunications and mobile computing, I believe it is time law makers pass a bill centered on an electronic bill of rights designed to protect consumers from aggressive data driven companies that employ nontransparent surveillance and data acquisition ("data mining") business practices that seek to exploit connected product users for financial gain.

The enclosed "Connected Product- Electronic Bill of Rights" is based on several smartphone terms of use and installed ("preinstalled/install-by-update") technology (apps, widgets, etc.) analysis authored by myself (Rex M. Lee).

My research, documentation, and analysis of connected products coupled with the terms of use that support the products have exposed numerous privacy concerns, cyber security threats, consumer & child exploitation concerns, child privacy & safety concerns, and unfair business & deceptive trade practices that need to be addressed by law makers, the FCC, FTC, DHS, DOJ, State Attorney Generals, and other relevant agencies.

Due to my findings, I'm appealing to the office of Ted Cruz in an effort to lobby for an *Electronic Bill of Rights* protecting U.S. citizens, children, business professionals, and businesses from predatory data driven tech giants that employ nontransparent surveillance and data acquisition ("data mining") business practices.

I'm a consumer of connected products and services that I purchased from my telecom providers. I'm a *telecommunications subscriber* ("paying customer") who simply analyzed the smartphones, the terms of use, and the installed technology associated with the devices I had purchased from my telecom providers for my wife, children and myself.

Analyzing the products that one has purchased may sound simple but the process to research the installed technology (apps, widgets, content) and read the terms of use was torturous to say the least due to the sheer number of apps, widgets, and content preinstalled into the device.

In short, it took me nearly 4 months to read my cellular phone contract, research the preinstalled technology that supported the devices, and understand my business relationship between all parties concerned due to the exploitive and torturous terms of use and the sheer number of preinstalled apps that support the products and services I had purchased from my telecom providers.

The telecom subscriber is also tasked with researching the preinstalled technology developers which could be as many as 15 more multinational companies pending the OS and the preinstalled content that supports the device.

When a person, business, or government entity purchases a connected product such as a smartphone they are forming a business relationship with many companies and/or entities other than their telecom provider. Some of the entities come from countries such as China.

A telecom subscriber and/or authorized device user (spouse, child, employee, etc.) needs to understand that connected products such as smartphones are neither a private nor secure form of telecommunications and computing.

A connected product user needs to understand that connected products such as a smartphone have been commercialized meaning that multiple entities can extract highly confidential personal and professional telecom related information from the device to use for financial gain at the expense of the product user's privacy whether the user is an individual, child, business professional, public servant, government official, or a law maker.

A connected product user needs to understand there is no privacy nor cyber security to be expected when using any app driven connected product whether that product is telecom related or not. Connected smartphones, PCs, TVs, tablet PCs, wearable technology, toys, automated voice products, climate control & security systems, and other connected products that have been commercialized.

A connected product such as a smartphone is actually a corporate surveillance tool used by the technology developers to exploit the product user for financial gain at the expense of the product user's privacy while the telecom subscriber is obligated to pay the bills.

Figure 1- Corporate Surveillance Tool (Smartphone)

Connected Products- "Electronic Bill of Rights" (Part 1) Draft 1.0

Nov 2017- Money Masters

Technology developers include the operating system ("OS") developer, original equipment manufacturer ("OEM"), and preinstalled technology (apps, widgets, etc.) developers.

Telecom providers have figured out how to monetize their customer base ("telecom subscribers & authorized device users") by enabling predatory data driven tech giants ability to monitor, track, and data mine the telecom subscriber and/or authorized device user for financial gain via connected products such as smartphones.

In other words, the connect product user has been turned into "*product"* that can be exploited for financial gain via a connected product that requires payment to participate such as a smartphone, PC, TV, tablet or any other product or service that requires payment.

Turning your embedded base of customers into products to be sold to the highest bidder is part of the strategy that makes up the *"Connected Product Business Model".* Aside from telecom providers, other companies such as TV manufactures, automobile manufactures, toy manufactures, appliance manufactures and others technology developers are adopting this highly exploitive business model due to the fact that connected products enable the monetization of individual product users.

The connected product business model is a highly profitable business model that seeks to exploit the paying customer and/or product user at the expense of the product user's privacy whether that user is an individual, child, business professional, public servant, or elected official.

The connected product user is valued as an "*uncompensated information producer*" that produces a highly valuable commodity in the form of "*connected product user data*" which is used by technology developers for predictive technology, artificial intelligence ("AI"), and other uses that can drive revenue for the technology developers.

Connected product user data ("Digital DNA") is considered to be priceless and consists of:

a) Surveillance data- location data, motion data, health data, fitness data, geofence data, auto telematics, photos, audio recordings, videos, recordings of conversations (home, car, on the go), etc. Geofence technology enables technology developers to track the time when a persona arrives and departs from a specific location. This technology has been deployed in products such as smartphones and wearable technology. Geofence technology is used to track mainly criminals and terrorists.

b) Sensitive user data- personal & professional information such as personal ID, personal contact information, employment information, earnings information, education, employment history, medical information, legal information, political affiliation, banking information, social media information, web browsing, friends, family, contacts (address book), calendar data, text messages, instant messages, email attachments, key logging data (touch screen activity), entertainment (books, news, music, movies, etc.) and other highly confidential information that can be gleaned from app driven products such as smartphones & PCs.

c) Multisource syncing data- Surveillance and Sensitive User Data collected from any source that can sync and/or connect to a connected product such as a smartphone. This means connected products are supported by preinstalled content that is programmed to hack information from multiple sources owned by the product user and/or other connected devices that are connected to the product user's device such as the product user's friends devices. This ability gives the technology developers the ability to hack information from multiple sources owned by their customers and/or sources that are synced to their customer's device such as an exchange server owned by the product user's employer. This is a horrifying capability to say the least.

Think of it this way, every time you use a connected product such as a smartphone, TV, table, PC, automobile, voice automated product, toys, or any other connected product you are generating cash flow at the expense of your privacy for numerous tech giants.

Due to the fact that in order for predictive technology and AI to work effectively, the technology developers need to collect as much personal and professional information from a connected product user. In addition, the technology developer needs to surveil the product user's personal and professional activities as well as collect the surveillance data which includes data such as location data, voice data, and video data.

Telecom subscribers and/or authorized device users would never freely give a technology developer total access to their lives so that the technology developer can exploit the individual's connected product user data for financial gain without compensating the connected product user.

The connected product user would demand that they have the ability to freely opt in or out of any exploitive surveillance and data acquisition business practices that support products and services that require payment to participate such as a smartphone, TV, car, toys, tablets, PCs, and other products.

However senior executives for one of the big two operating system developers think that their paying customers (e.g. smartphone users) are freely giving the tech giant the *permission* to know where the connected product user is at all times, where the product user has been, and practically knows what the product user is thinking without the connected product user needing to type anything into a key board.

Don't take my word for it, a senior executive admits it:

"With your "Permission" you give us more information about you, your friends, and we can improve the quality of our searches. We don't need you to type at all. We know where you are. We know where you've been. We can more or less guess what you're thinking about."-Executive Chairmen- Silicon Valley Tech Giant

What rational human being would give a tech giant this much access to their lives especially knowing that that the tech giant is using this much personal and professional information for financial gain at the expense of the individual's privacy?

Furthermore, what business professional would give a company such as Google this much access to their professional information and business activities especially since companies such as Google compete in many industries worldwide?

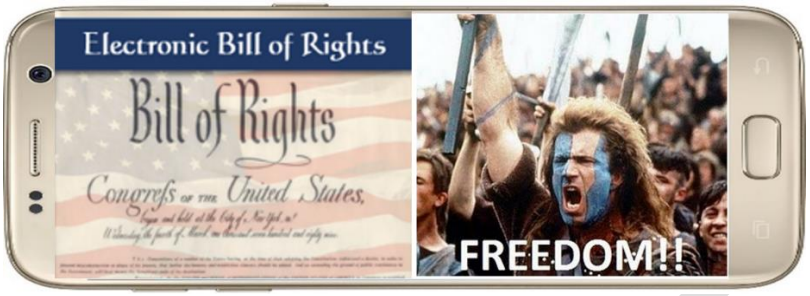
I will list the numerous privacy concerns, cyber security threats, consumer & child exploitation concerns, child privacy & safety concerns, and unfair business & deceptive trade practices that need to be addressed by an electronic bill of rights and law makers for the Dec addition of Money Masters.

Inclosing, please review all terms of use before clicking on "I Agree" without reading the fine print.

Regards- Cyber Rex

Connected Products- “Electronic Bill of Rights” (Part 1) Draft 1.0

Nov 2017- Money Masters



Contact Rex M. Lee at RLee@MySmartPrivacy.com For detailed information visit www.MySmartPrivacy.com