Connected Products- "Do We Know What We Are Paying For?" (Part 2) Draft 1.0

Oct 2017- Money Masters

By Rex M. Lee

What Are We Legally Bound To When We Click On "I Agree" Part 2- FTC Q&A?

For this month's addition of Connected Products- "Do We Know What We Are Paying For?", we will continue to take a close look at the legal process that support connected products such as smartphones, TVs, PCs, tablets, vehicles, home assistants, wearable tech, toys, and other connected products and services.

In the September issue, I asked a very important question: *"Why are we clicking "I Agree" accepting legal agreements without reading the fine print?"*

After all would you simply click on "I Agree" to accept a mortgage loan or a car loan without reading the fine print?"

Would a CEO of a fortune 500 company simply click on "I Agree" to accept terms for a business deal without letting their corporate legal team review the terms and conditions of the agreement?"

So why are corporate CEOs, small business professionals, government officials, attorneys, and individuals clicking on "I Agree" to accept connected product terms of use without reading the fine print?"

I believe part of the answer is due to trust in that we believe telecommunication providers would not sell and support connected app driven telephones and mobile computers (smartphones) could inadvertently bring harm to their paying customers the telecommunication subscriber.

Per the September article, I did an analysis on the installed technology that supported my smartphone found that my device was actually a corporate surveillance tool supported by installed technology that enabled numerous third-party app developers to monitor, track, and data mine all of my personal and business activities for financial gain at the expense of my privacy.

I asked myself how we got here and why do CEOs, small business professionals, government officials, attorneys, and individuals continue to simply click on "I Agree" when in fact connected product users are in fact accepting highly intrusive and exploitive legalese.

Trust in our telecom and connected product providers is only one part of the equation, my findings also exposed potential unfair business and deceptive trade practices that need to be addressed by agencies such as the FTC, FCC, DOJ, and various state AGs.

I wanted to know if "nontransparent" surveillance and data acquisition business practices employed by my telecom provider and connected product providers was legal so I conducted a terms of use analysis and found many discrepancies that needed to be addressed by agencies such as the FTC, FCC, DOJ, and various state AGs.

Connected Products- "Do We Know What We Are Paying For?" (Part 2) Draft 1.0

Oct 2017- Money Masters

I reached out to the FTC in early August and to the Texas AG, Ken Paxton, in late August to find out if they would answers some questions and concerns centered on privacy, cyber security, and consumer exploitation associated with the smartphone I did the analysis on.

The representative I contacted at the FTC, Juliana Gruenwald Henderson Technology Issues & Privacy, was very welcoming to the idea of addressing my questions and concerns.

The Texas AG's office was also welcoming but has yet to address my questions and concerns due to a delay which I believe is associated with hurricane Harvey.

On August 9th, 2017 I first submitted my questions and concerns to the FTC. The questions and concerns were centered on surveillance and data acquisition business practices employed by telecom and connected product providers.

On August 22nd, the FTC sent me some answers to some of the questions but also let me know they are still reviewing some of the other questions.

In this month's article we will review one of the FTC's answers pertaining to unfair business and deceptive trade practices.

I listed concerns prior to each question so that the FTC and Texas AG could understand the questions and why I was asking the questions.

For this article I will list the concerns prior to the questions I submitted to the FTC plus their answers. I will also include illustrations for reference plus further explanation and analysis of the FTC's answers.

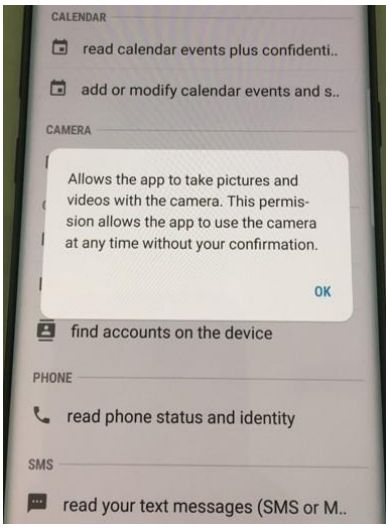
FTC Q&A- Part 1:

Question 1- Unfair Business and Deceptive Trade Practices Associated with Smartphone Terms of Use

Concerns- Third-parties such as installed OS and app developers may use unfair business and deceptive trade practices coupled with exploitive terms of use to collect and exploit surveillance and sensitive user data for financial gain at the expense of privacy while the subscriber is expected to pay the bills.

For example, connected product providers separate installed ("pre-installed/install-by-update") application permission legalese from published terms of use which include terms and conditions ("T&Cs"), privacy policies, and end user licensing agreements ("EULAs").

Figure 1- Actual picture of hidden application permission legalese which is not transparent to the product owner and/or authorized device user (spouse, children, employee, etc.):



The figure 1 example comes from a very popular smartphone I just purchased in early October 2017 from a one of the top telecom providers in the world.

For legal purposes we are not naming the smartphone manufacturer, operating system ("OS") developer, and installed app developers. However, I will provide you with a website at the end of the article that will reveal all parties concerned.

People have no idea that their connected products such as their smartphone contains numerous nontransparent installed application permissions such as the camera app permission example above.

The nontransparent camera app permission is one of many examples of deceptive trade practices I have identified. This is an example of a deceptive trade violation due to the fact that the app permission is not published in product T&Cs, privacy policies, nor EULAs.

If the user does not know where to locate the installed app permissions that support their connected products they will never know the installed app permissions exist even though they are legally bound to the app legalese at the point of using the installed app and/or when they clicked on "I Agree" to accept their product terms of use.

I believe that connected product users are forced to participate in a highly exploitive surveillance and data acquisition business model due to the fact the user has no idea the installed app permissions exist because the legalese is buried in the OS of the device rather than published in the product terms of use.

Due to forced participation by nontransparent methods, connected product users have become in-essence *"uncompensated information producers"* who are exploited for financial gain at the expense of their privacy by the companies they patronize with their loyalty, trust, and hard earned money.

The reason I use the term *"uncompensated information producer"* is because consumers of connected products purchase the products, use the products, and produce a valuable commodity in the form of location data (surveillance data) and sensitive user data (personal & professional information).

The surveillance and sensitive user data is then collected and used for financial gain by the installed technology developers who are responsible for the development of connected product OS and the preloaded apps, widgets, and other content.

This means that the installed technology developers are actually exploiting their paying customers for financial gain at the expense of the product user's privacy by virtue of not enabling the product user to freely opt in or out of any exploitive surveillance and/or data acquisition business practices.

For example, smartphone users include the telecom subscriber ("paying customer") and/or the authorized device user which often includes a spouse, children, and employee who may be using a device associated with the wireless telecom account.

I wanted the FTC to address the legality of the nontransparent intrusive and exploitive connected product business model employed by many fortune 500 telecom and connected product providers due to the fact that connected products and services contain numerous hidden application permission statements, app product warnings, and interactive application permissions. I personally believe all legalese should be published in T&Cs, privacy policies, and EULAs.

Cyber Rex Question 1: *"Is there any laws on the books that prevent predatory companies from using nontransparent unfair business and deceptive trade practices that seek to exploit the product user at the expense of the product user's privacy while the telecom subscriber is expected to pay the bills?"*

FTC Answer (Ms. Gruenwald Henderson): "The FTC Act, which the FTC enforces, bars deceptive and unfair practices in the marketplace. The Commission is vigilant, and we will take aggressive action when we see unfair or deceptive practices in the marketplace."

I believe the fact that app permissions, app product warnings, and interactive app permissions are not transparent to the product owner and/or authorized device user is a violation of the Texas Deceptive Trade Practices Act ("DTPA") and the FTC Act due to some initial analysis of the law that I've conducted.

I will follow up with the FTC and submit many examples of hidden application legalese such as the figure one camera installed app permission plus my analysis of the law to confirm my suspicions that violations of current laws have in fact occurred and are currently occurring.

I believe hidden installed app permissions, app product warnings, and interactive app permissions are examples of deceptive trade that the FTC needs to address.

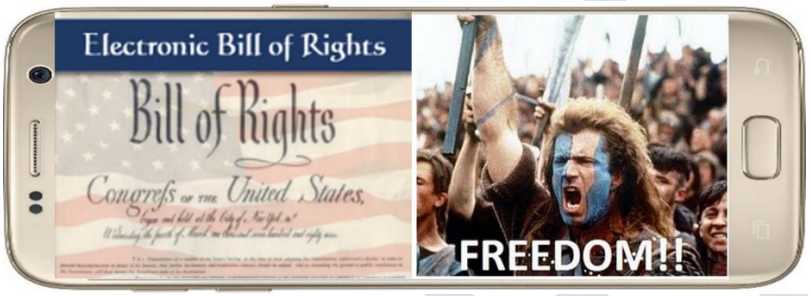
After all, who wants to purchase products and services from telecom and connected product providers who feel they have to use exploitive and torturous application legalese from their paying customers?

Due to hidden app legalese, connected product users are not given the opportunity to freely opt in or opt out of surveillance and data acquisition business practices employed by their telecom and connected product providers since they have no idea the installed app legalese exists.

In the next addition we will address more of the FTC Q&A plus safety tips on connected technology including toys for children.

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

Regards- Cyber Rex



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