05.02.2024

Rex M. Lee
Security Advisor
My Smart Privacy
[redacted]
Rlee@MySmartPrivacy.com

Barbara Cuthill
IoT Advisory Board Secretariat
Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899
barbara.cuthill@nist.gov

Subject: Support for Privacy Information Inclusion on Monroney Stickers

Dear Ms. Cuthill,

I am writing to express my support for the IoT Advisory Board's recommendation to include privacy information regarding the use of personal data on the Monroney stickers for new and used vehicle sales.

This recommendation is a great step forward in enhancing transparency and empowering consumers in the rapidly evolving connected vehicle market.

Given my background in cybersecurity, and as an enterprise application/platform developer, the issue here is *forced participation regarding surveillance and data mining business practices employed by all of the OS, app, platform, and AI developers* responsible for collecting, monetizing, and selling the information collected from the vehicle owner, and/or the driver of the vehicle which includes teens.

Today, consumers, business owners, corporations, and government agencies mistakenly view tech giants such as Alphabet/Google, Apple, Microsoft, Meta/Facebook, and ByteDance/TikTok as tech companies, that may be true to some extent, however by definition of their surveillance and data mining business practices, these tech giants, and others, are in fact the largest data brokers in the world.

They compete in the global trillion dollar information trafficking industry whereas they develop leaky operating systems, intrusive apps, addictive social media platforms, and AI more for their benefit rather than the benefit of the consumer and/or end user.

They in fact develop surveillance and data mining apps and platforms that use applications such as gaming or social media as vehicles in order to monitor, track, and data mine the product owner, paying customer, and/or end user for profits.

The OS, app, and platform developers force the vehicle owner, and/or the end user to participate weithin a highly exploitive surveillance business model rooted in “Surveillance Capitalism” which is a predatory business model centered on exploiting the vehicle owner, and/or driver at the expense of privacy, security, and safety.

The safety concerns are centered on addictive/manipulative technologies baked into the apps/platforms, plus the fact that the predatory terms of service do not indemnify (protect) the product owner and/or end user from harm, even if the app/platform developer is negligent.

The forced participation is done through contracts of adhesion (take-it-or-leave-it), which are the predatory terms of use that support the OS, apps, and platforms that support the vehicle electronic system.

The terms of service enables all developers concerned, including those from China and Russia, to conduct audio, video, and physical surveillance on the vehicle owner, and/or driver while data mining thousands of highly confidential data points that are collected, aggregated, packaged, monetized, and sold to targeted advertisers and/or other third parties that include data brokers, even entities from foreign countries.

If the vehicle owner does not accept the predatory terms of service by clicking on “I Agree”, then the vehicle owner may not be able to use core features of the OS, apps, and platforms that support the vehicle’s electronic system, in some cases, pending the operating system (Android or Apple iOS), the vehicle owner may not be able to use any features even though they paid for all products and services concerned.

This is the case today regarding smartphones, tablet PCs, connected products, smartTVs, connected vehicles, wearable tech, IoT devices, connected appliances, and PCs supported by the Android OS, Apple iOS, or Microsoft Windows which all support intrusive apps that are designed to enable the app developer to monitor, track, data mine, and exploit the end user for profit whether the end user is an adult, teen, or child.

If the product owner, and/or end user does not click on “I Agree”, they simply cannot use any of the products I mentioned above even though the product owner paid money for all products and services which this is a clear definition of consumer/child exploitation and oppression.

Due to this oppressive and exploitive business model, Surveillance Capitalism, it is paramount that automobile manufacturers be transparent regarding their surveillance business practices, as well as their partners’ surveillance business practices that include

the OS, app, and platform developers which include Alphabet/Google (Android OS-Android Auto) or Apple (iOS- CarPlay), plus all preinstalled app developers, which could include companies from China pending preinstalled app agreements between the OS developers and third party app developers.

With over 35 years of experience within the app/platform development industry, plus within telecommunications and cybersecurity industries, I have witnessed firsthand the complexities and challenges that come with the integration of connected technologies that are necessities within our daily lives.

The rise of personal data collection in vehicles is no exception, raising significant concerns about privacy, security, and safety.

This fact is, there is no privacy within the vehicle due to the fact that the surveillance and data mining is indiscriminate and 24/7 365 days per year meaning that most of the information collected from the vehicle owner and/or driver as nothing to do with consumerism, nor the use of all apps/platforms concerned.

The highly confidential information collected by all OS and app developers concerned includes personal, business, medical, legal, biometric, employment, and location data to be exploited for financial gain by all developers concerned.

The Monroney sticker, which has traditionally served as a trusted source of information for consumers purchasing vehicles, presents an ideal opportunity to address these concerns.

By creating transparency that personal data is collected and sold we can provide consumers with the knowledge they need to make informed decisions about their privacy as long as the developers terms of service enable the consumer to decline the terms of service, yet still be able to use the product they paid for.

As a security advisor to major corporations, government agencies, and lawmakers, I consistently advocated for transparency policies prioritizing consumer privacy and data protection, plus safety as many apps today are purposely designed to be addictive.

Some apps are intentionally designed using brain-hijacking technology associated with manipulative advertising technology, such as gaming apps, entertainment apps, and social media platforms.

Brain-hijacking technology includes highly addictive technology associated with social validation feedback loops, intermittent variable rewards, and other addictive technology of which is also used in popular slot-machines to addict people to gambling.

For more information, please take the time to see the Netflix documentary, The Social Dilemma, in which numerous executives and product designers for Meta, Google, and other app and social media developers expose how they intentionally addict end users to the apps and platforms for the sole purpose of exploiting the end user for profits, even at the expense of safety.

For reference, please see the astonishing apology by Meta CEO, Mark Zuckerberg, who recently apologized to the parents of teens and children who were addicted, exploited, harmed, and in some cases killed as a result of the addictive nature of Facebook and Instagram pertaining to the dangers of sexual exploitation, and other dangers such as the TikTok challenges that have resulted in violence, crimes, harm, human/drug trafficking, and even death.

The Senate Judiciary hearing took place in January of 2024, and was tilted “Big Tech and Online Child Sexual Exploitation Crisis, which involved 4 other CEOs of social media platforms that included Shou Zi Chew, ByteDance (TikTok), Linda Yaccarino, X (formerly Twitter) and Evan Spiegel, Snapchat.

Many of these apps, platforms, including those from China such as TikTok, are now accessible through Android Auto and/or Apple iOS-CarPlay which are the two most popular operating systems that support connected vehicles today.

Also note, that mobile devices such as smartphones and tablet PCs also sync with Android Auto and/or Apple iOS-CarPlay, as well as connect to cars that are equipped with 5-G and Wi-Fi connectivity, of which OS and app developers use to surveil and data mine connected end users to the in-vehicle OS, apps, platforms, etc.

The proposed recommendation aligns with these principles, offering a proactive and transparent approach to address potential privacy, security, and safety issues before they become problematic for automakers, auto dealers, and consumers, if these issues are not already problematic today.

As a professional speaker and technology journalist, I understand the importance of clear and accessible communication.

When I speak, write, or report on these subject matters, I do so from an app/platform developer’s perspective, someone who works within the industry.

The Monroney sticker can serve as an effective tool to communicate basic privacy, security, and safety information in a straightforward manner, making it accessible to all consumers.

I support the IoT Advisory Board's recommendation and urge its inclusion in the final report.

By doing so, we protect consumer privacy, security, and safety while enhancing the overall integrity and trustworthiness of the automotive industry.

Thank you for considering this important recommendation.

Please contact me if you have any questions.

Sincerely,

/s/

Rex M. Lee
Tech Journalist | Security Advisor | Advisory Board Member | Speaker
My Smart Privacy
https://mysmartprivacy.com/
[redacted]
Rlee@MySmartPrivacy.com