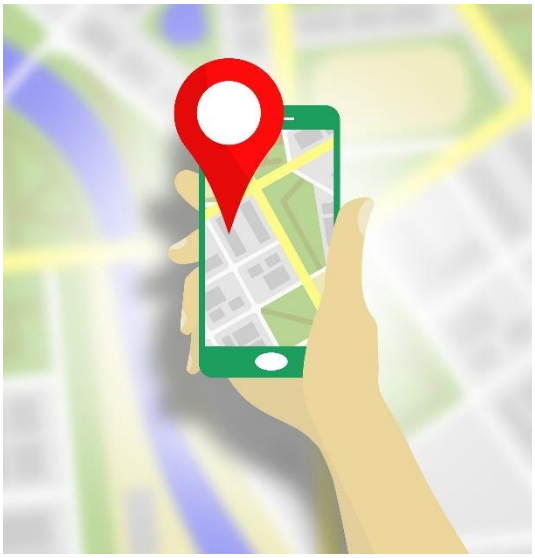
2020 Vision: The Future of Privacy Risk

Personal data is a profitable commodity. This is not a new paradigm; participants in legal (licensed private detectives), quasi-legal (state sponsored intelligence operatives or "spies"), and downright illicit markets (blackmail/extortion artists) have for centuries understood the value inherent to personal data. Our environment today, however, is different. We have entered an age where computing power, the prominence of social media, and advanced algorithmic capabilities have turned personal data into an economy of scale. The collection, use, and disclosure of personal information is no longer a targeted tactic towards only those with secrets worth learning and adversaries driven enough to accomplish the goal. Today, extracting value from personal data is done increasingly by people and groups you consider friendly, through information you think you don't care about, for objectives you seem to agree with. After all, who wouldn't prefer all their online ads to be for products they actually like and can afford.

You may find this shift comforting, but you shouldn't. Today's Data Privacy Day 2019 article is a look into burgeoning privacy threats of the not-so-distant-future. I'm not here to tell you that it is axiomatically a bad thing that Netflix knows which shows you will like and dislike before you watch them, or that Amazon shouldn't notify you when your favorite author publishes another book. I am here to tell you that the personal data collection, use, and disclosure practices utilized to accomplish those tasks ***won't stop there***. There is a preponderance of your data available to the world at large, and that pool of data grows quite literally every time you leave the house, look at your phone, or turn on the tv. The tools capable of manipulating and extracting actionable knowledge from your data get smarter and more powerful by the day. And for every benign lesson learned about your cereal or reality tv preferences, there will be other actors utilizing your data for purposes that will, rightfully, put you at unease.

At the end of each workday as I prepare to leave the office I receive a notification on my phone, from Google, telling me the condition of traffic and the estimated time required for my commute home. Cool stuff, no argument from me. But, seriously, how did they do that? How much personal data was utilized to inform me that today's commute is 4 minutes longer than average, and to notify me at the right moment? Google needed to know the address of my office, the address of my home, my usual route of travel, my work schedule and standard departure time from the office, and my real time physical location on the earth. All of the above should give you pause, but the last one is the kicker. Google needs to know my exact geographic location at this very moment to confirm that I am indeed at my office and will have the standard departure point for my journey. But, once confirmed, in order to inform me of how the flow of traffic will actually impact my commute, Google needs the real time physical location of **EVERYONE ELSE ON AND AROUND THE ROADS I DRIVE**.



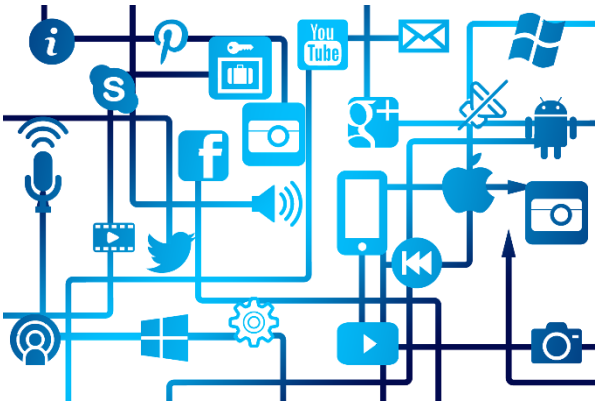
Woah. That's a lot.

It does make sense though. How else would traffic reports work other than to collect the quantity, location, and speed of the other drivers. And I do remember turning on the location services for my phone (because seriously, everyone uses their phone's GPS) so I guess I opted in.

And there, as the bard tells us, lies the rub. Opted in to ***what*** exactly? Sure, I wanted the GPS to work on my phone, just like you want Netflix to show you the best content and Amazon to know when you are running out of dog food, so we opt in. But what exactly are the personal data practices at play here? How broad is the data collection, how many things are they using my data for, and who else are they sharing it with?

Google notifies me about my commute, ok, and I opted in because I need my phone's GPS. But what is the reality of my situation? In practical terms, my comings and goings are no longer private information. How much time I spend in my home, every single place I visit, the route I took to get there, my exact physical location at all points in time, all of it collected. I am, by my own choosing, constantly surveilled, and it hardly ends there. My credit card's fraud protection service tracks every single purchase I make. Android backs up my call and message history and content, along with all my photos and videos. Multiple organizations tracking a staggering number of variables creating an astronomical amount of data about me.

Which is where our privacy journey turns towards the nightmarish, quasi-apocalyptic, Black-Mirror-meets-The-Twilight-Zone potential future. Because this much, at the very least, is certain: ***all of that data already exists***. Your conversations, transactions of all kinds, records of your entertainment consumption, medical history, and indeed the location you sit while reading this article (and the very fact that you're reading it) is all information already held by someone other than you.



The sheer scale of the personal data, from which its value is derived, is also for the time being our saving grace. This wealth of data is so disparate and the quantity so large that analyzing it for maximum potential value is beyond our capabilities. But this article is not about today, it is about tomorrow, and the analytical capacity of artificial intelligence is already dramatically altering our understanding of what is possible with vast sums of data in ways that were previously unthinkable. That, right there, is what should scare you. Because the terrifying answer to "what could google accomplish with constant real-time location data of every single google user on earth along with the most advanced artificial intelligence" is: ***we have absolutely no idea***. How much of who I am can be boiled down to data points? If some nefarious actor gathered together my various sets of data (transactions, conversations, locations) and possessed the tools to analyze it, what sort of possibilities would that create? I shudder to think.

Now, contrary to the extreme rhetoric above, I am no harbinger of the end-times, and the future of personal data use is not all doom and gloom. IBM's Watson already uses an immense amount of personal medical data to be quite simply the world's greatest doctor with the ability to utilize more information than even the smartest humans could even conceptualize. In all likelihood it will be advanced technological analysis tools with access to incredible personal data that brings us some of our next generation's greatest discoveries. The point of this article, and indeed of Data Privacy Day, is a call to be cognizant of the potential value, and the potential risk, of your personal data. ***Your ability to be proactive with regards to the data you create, where it goes, and how it is used will be a critical skill of the future***.

And hey, if you need some help on that front, that's what MBL's Privacy team is here for.