FRAUDSNIFFR

Mobile Data in Court – The Final Defeat of Phone Encryption

A few years ago we saw headlines like "Apple refuses to unlock phone of domestic terrorist for FBI" but then in October, 2020 the news about encrypted phone access changed. The New York Times reported that law enforcement had acquired tools to unlock smartphones and their contents. As of last week, that same technology is available via software licenses to private investigators and insurance forensic companies.

Now that the encryption technology has been cracked for most phones, the only protection for users' data is consent. For an insurance company to download phone data, they are required to provide written consent or a court order to legally obtain the information on a phone. That's it.

In the event of defense counsel presenting a court order and a mobile phone to an investigator, what kind of data is available? Mind blowing data. All the most private data – every text message, social media post, all location history, call history, voice mails, emails, photos, videos, biometric data, financial data and more. People live on their phones and their every move is recorded in detail by these devices.

Think about the apps you have on your own phone. Do you have a health app where you track your exercise, sleep patterns, or diet? Do you use the Amazon app that keeps a history of all your purchases? The Air BnB and Uber / Lyft apps show every place you have stayed and every ride you've taken. The Good RX app shows your prescriptions search history. If you use a family tracker to keep a digital eye on your kids, this information is now available for download as well. The depth and variety of data captured by a mobile phone provides a comprehensive look inside someone's life.

It is interesting that technology has not been able to maintain privacy protection on these devices in a meaningful way. The axiom "if the data is valuable enough, it will be gathered" is proven out through the defeat of impressive encryption on these devices in just a few years. And the fact that we are back to legal protection, governed by human decision-making is an irony not lost on the tech community.

Is a human/legal barrier consistent and robust enough to provide actual privacy protection? The debate on this topic rages on. The legal system has faced challenges regarding fairness, bias and the impact of decades of Precedent that is currently in dispute based on new views about race and privilege. But for all its flaws, the law is the final layer of protection for those in disputes centered around personal activity.

The use of mobile data in court and insurance disputes is worth monitoring. Mobile phone data provides the potential for massive gains in the accuracy and volume of useful data presented in trial. More truth, less story telling. It will be interesting to watch how the courts dole out permission and admissibility over the next few years.