SUMMER 2015 E-NEWSLETTER

At Digital Mountain we assist our clients with their e-discovery, computer forensics and cybersecurity needs. With the recent Jeep Cherokee hacking incident and the evolution of the traditional car as part of the Internet of Things (IoT), we chose to theme this E-Newsletter on the impact vehicle discovery has on attorneys, litigation support professionals and investigators.

VEHICLE DISCOVERY – IT'S GO TIME

The discovery of vehicle data has historically been limited to law enforcement pursuits given the complexity and costs involved. The technology landscape for commercially available discovery tools is undergoing an evolutionary change thanks to vendors such as Berla Corporation (guest contributor) and others headquartered not too far from our nation's great capitol. The global market research and consulting company MarketsandMarkets has announced that the total In-Car Infotainment (ICI) Market is expected to reach $14.4 billion by 2016. Many companies ranging from vehicle manufacturers, social networking companies, traditional radio car systems and navigation system providers are vying for a piece of the market.

A vehicle is now part of the Internet of Things (IoT) umbrella which is connected to the Web, thereby increasing potential exposure for hacking. Depending on the car's system, a vehicle may be digitally connected through sensor systems (steering, brakes throttle, fluid levels, etc.) or by the vehicle infotainment system (geolocation, radio preferences, mapping history, social networking activity, call logs, etc.) running on a vehicle's central computing system. The systems with applications can be a potential revenue stream for carmakers or traditional Internet companies (Google, Apple, etc.). For example, if a driver is almost out of gas, an application can assess where the closest gas station is at the most reasonable price. If a vehicle needs maintenance, the system can alert the owner and locate any special deals for the make/model of car in the area. Insurance companies potentially can use vehicle data to monitor driver behavior and if the driver warrants a good driver discount or if auto insurance should be increased based on the risk profile.

There are different strategies that each car manufacturer maintains. Some car manufacturers have their own proprietary systems from the operating system to the applications running on the vehicle. Although this approach may be more secure, it presents significant hurdles to motivate standard application developers to port in-demand applications to a custom system. This was an issue Apple faced prior to having an operating system based on BSD (Unix) which is a key reason they lost market share for many years. Apple's system was too proprietary and application providers did not

want to port applications to a closed system. For manufacturers taking this approach, they have to develop their own innovative applications to stay competitive with consumer demands.

Other car manufacturers are basing their systems on a more common operating system such as Windows or Linux allowing for interoperability with application providers. However, the more open a system is, there is potentially more security risk with savvy hackers aware of vulnerabilities. Also, with the development lifecycle of a car being 3-5 years and operating system and application releases occurring much more frequently, software obsolescence as well as required patches/updates becomes a major issue for the car industry. Thus, leading to more vulnerabilities.

In the past month (July 2015), hackers took remote control of a Jeep Cherokee due to vulnerability in the Uconnect system that allowed them to kill the brakes, shut off the engine and play with the steering wheel. As a result, Chrysler recalled 1.4 million cars and trucks in order to properly update software in its vehicles. Prior to that, BMW had to offer a software patch after a breach occurred that unlocked doors of its cars. Laws are still catching up with the vehicle technology presently available in the market and future developments. On July 22, 2015, the SPY Car (The Security and Privacy in Your Car) Bill was introduced setting ground rules for connected automobiles. In the United Kingdom, The Department of Transport has recently published a non-statutory “code of practice” for testing automated vehicles to ensure proper data can be collected for investigators should an incident occur as well as to establish further security mechanisms.

The impact of vehicle infotainment systems on the rental car industry should also be considered. If a driver rents a car and uses Facebook which may be residing on the vehicle console, all the driver’s personal contacts and email addresses are presently loaded onto the vehicle’s infotainment systems. The user’s playlist may also be downloaded and other personal data such as keyword searches. Additionally, the call logs may be readily accessible. Unless the rental car company wipes this information, it remains on the car until overwritten. The same issue exists with used cars being resold. Different cars may have ports that the data can be easily accessed and preserved, while on certain vehicles the dashboard needs to be almost completely disassembled to be able to access the data making wiping almost impossible. The nuances and customization of vehicle infotainment systems and maintenance systems makes vehicle discovery much more complex than desktops, laptops, smartphones, wearables and other IoT types of devices. Unlike smart devices, there is no factory reset on automobiles. Therefore, the privacy, security and data management aspects of vehicles requires specialized expertise and remains a ripe opportunity for attorneys as well as electronic discovery and computer forensics practitioners.

COME VISIT US AT ACEDS ON SEPTEMBER 28-30, 2015

UPCOMING INDUSTRY EVENTS

August 2015
HTCIA 2015: August 30 - September 2

September 2015
ACEDS 2015 E-Discovery Conference: September 28-30

October 2015
EDI Leadership Summit: October 14-16

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at some upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: