Artificial Intelligence and Data Privacy: Are We Sufficiently Protected? (Part 2 of 3)

Dec 11, 2017

Categories:

Blogs
Publications
Technology Blog

This is the second article in a series on the legal issues surrounding artificial intelligence (AI), based on an fbtTECH webinar held in November 2017.

Part 1 – AI is Surging: Are We Ready for the Fallout?
Part 2 – Artificial Intelligence and Data Privacy: Are We Sufficiently Protected?
Part 3 – You Can't Sue a Robot: Are Existing Tort Theories Ready for Artificial Intelligence?

The use of artificial intelligence and autonomous systems in consumer product development has been grabbing headlines in recent months. Self-driving vehicles, smart internet-connected toys, and wearable technology are some of the more prominent examples of products where AI technology is being deployed. And with holiday shopping in full swing, it is worth considering the extent to which these products provide the necessary privacy controls, and whether sufficient consideration has been given to cybersecurity risks associated with this technology.

Internet-connected toys and wearables using AI have become increasingly ubiquitous, causing sufficient concern for both the Federal Trade Commission (FTC) and the Federal Bureau of Investigation (FBI) to issue announcements urging consumers to consider cybersecurity prior to introducing such products into their homes or trusted environments.

The FBI's public service announcement issued in July of this year explained that communications connections where unencrypted data is transmitted between the toy, Wi-Fi access points, and Internet services that store data create risks that hackers could exploit the toy or possibly eavesdrop on conversations and audio messages. Bluetooth-connected toys carry the risk of unauthorized access if authentication requirements are not employed. A simple

internet search returns numerous "how-to-hack-a toy" results. The FBI provided a list of precautions for consumers to take, such as researching where data is stored, what rights the company has to retain and transfer the data, who else has access to the data, and whether the company will notify a consumer if the company's system is hacked.

The FTC reissued its COPPA Compliance Plan for Business in 2017, which assists businesses with compliance with the Children's Online Privacy Protection Act. According to its announcement, the update was necessary to reflect developments in the marketplace – for example, the introduction of internet-connected toys and other devices for kids. Long recognized as applicable to websites and mobile apps, the FTC expressly affirmed that COPPA also applies to the collection of personal information of children under 13 by such toys and devices, including voice recordings and geolocation data, necessitating the need for explicit and verifiable prior parental consent in connection with the use of those products.

The Privacy Concerns of Self-Driving Vehicles

However, the autonomous vehicle has grabbed the most attention from the public, legislators, and the press, and cybersecurity risks continue to be a major concern. Several high profile automotive cybersecurity breaches have raised alarm bells concerning these risks. German researchers spoofed a cell phone station and sent fake messages to a SIM card used by an autonomous vehicle's telematics system. This permitted them access to the car's convenience features so they could unlock doors or turn off headlights. Further, the researchers were able to remotely take control of essential features so that they could remotely stop the vehicle on the highway. Malware can also threaten the safety of autonomous vehicles by stopping operation of the vehicle until a ransom is paid.

An intelligent and informed consumer will want to consider that any product that connects to the internet is vulnerable to a cybersecurity attack. Autonomous vehicles and other products will of necessity have at least one internet connection. Further, such

products and devices collect and process personal data due to the wide variety of sensors installed in them. While some developers of the different technologies have made the effort to be sensitive to the privacy and security risks associated with the use of AI and connected technology, others have not given sufficient consideration to these risks in the rush to get products to market. Presently, the lack of government regulation in this area has led to academic and industry based initiatives to encourage incorporating privacy protections during the design phase of the products, or the use of "privacy by design." Adopting privacy protection measures in the creation and development of new devices will do much to reduce public anxiety with the products' collection and use of personal data.

Industry Self-Regulation on the Horizon?

At a recent international conference of data protection and privacy commissioners in Hong Kong, the officials passed a resolution on data protection in automated vehicles which urged that vehicle users be provided with "granular and easy to use privacy controls," and the technical means to erase personal data when a vehicle is sold, and to afford a consumer access and control over personal data collected. The recommendations were aimed at a variety of organizations in the market: vehicle and parts manufacturers, personal transportation and car rental providers, providers of data driven services, such as speech recognition, navigation and other telematics services, as well as standardization bodies and public authorities. The resolution also urged the use of anonymization measures to minimize the amount of personal data used, and pseudonymization where feasible.

The U.S. Department of Transportation (DOT) issued automated vehicle guidelines in 2016 and followed up with a voluntary guidance in 2017, titled, "Automated Driving Systems 2.0: A Vision for Safety." This Guidance promotes the further development and safe deployment of driver assistance technologies, and calls for industry, state and local governments, safety and mobility advocates and the public to continue the advancement of driver assistance technology. It reflects the DOT's belief that such technologies will

help eliminate motor vehicle-related deaths in America, and contains 12 priority safety design elements for consideration, including vehicle cybersecurity. It encourages entities to design their vehicles following established best practices for cyber vehicle physical systems established by the National Institute of Standards and Technology (NIST), among others. Its primary recommendation encourages industry sharing of information on vehicle cybersecurity vulnerabilities, and the prompt reporting of incidents, threats and vulnerabilities to the Automotive Information Sharing and Analysis Center and other relevant organizations. It suggests using layered solutions to ensure vehicles are designed to take appropriate and safe actions in response to a cyberattack.

In addition to the Guidance, 2017 saw the approval by the House of Representatives of the SELF DRIVE Act. This bill also pushes for the rollout of automated vehicles based on the belief that such vehicles will be beneficial to both the public and the economy. Thus, the emphasis is again on product safety rather than on data privacy and cybersecurity. It calls for a "light regulatory framework," which includes requiring manufacturers "to develop plans to thwart cyberattacks on the digitally-run vehicles." With more pressing matters facing Congress, however, it is unlikely the bill will be taken up by the Senate before year end.

Lost in the regulatory and House legislative discussions are privacy and security concepts such as giving drivers greater control over the collection, use and destruction of their personal data; mandating disclosure to vehicle owners or to an industry body of cybersecurity breaches and attacks; and requiring critical software systems be separated from noncritical software systems. Ignoring privacy protections and cybersecurity risks in the push to get consumer products to market could result in delaying acceptance of the technology by an already skeptical public, and in high profile cybersecurity attacks that will doom acceptance of the products by a public concerned with cybersecurity attacks. Industry would do well not to ignore these risks, and to collaborate to develop self-regulatory guidelines to help shape the federal and state legislation that is surely to come.

FBT Gibbons