



The Internet of Things meets Data Infrastructure – Is the law ready to protect our privacy?

Sep 01, 2022

Categories:

[Publications](#)

Authors:

[Joseph J. Dehner](#)

[Daniel A. Murray](#)

Although most countries have an overall data privacy law, the U.S. does not. Some states have data privacy statutes, but there's a mishmash of differing state codes about different things. Global laws differ and sometimes clash. And there is no one approach to the balance between privacy and governmental control. What all data privacy laws have in common, however, is that they assume that the target is to regulate data infrastructure – how data flows through computer and IT systems. Enter the Internet of Things (IoT). It challenges the very assumptions of regulating and protecting personal privacy. Data privacy laws were written as smartphones proliferated, and more and more data was collected by smartphones and IT systems. But now devices monitor us 24/7 in every home, car, and office. And they collect and transmit data about us, our children, and our guests.

Inadvertent Collection

We know that smartphones collect data about us. The IoT is creating collectors we don't think of the same way – smart speakers, air conditioning systems, light bulbs, refrigerators, garage openers, home security cameras, automobiles, smart watches, and more, all collecting and sending data about us. The devices track more than their owners. A home smart speaker in a house can track conversations of any visitor. If someone borrows a friend's car, it may include smart-speaker-like functionality and location tracking. Words, actions, facial expression, and other data can be tracked without everyone's knowledge. If children go to a friend's house for a birthday party, their data may be recorded and shared without parental or their consent.

Many data privacy laws aim to give consumers some measure of control over their data and with whom it can be shared. But how is this done when IoT devices collect and share information? How

does the typical data privacy regulation work when a person doesn't know data is being collected and shared?

Complicated Licensing and Interoperability

Some tech companies openly claim their business plan is to “[own the home](#).” But we interact, voluntarily, with multiple companies. A consumer may be Apple-centric, using Apple computers, iPhones, and iTV. But, that same person may drive a car with different data collection technology and services. A consumer may use Google Nest for thermostat control and security but use Amazon Prime and have a Fire TV account and a Roku device. A smart speaker that is interoperable with an iTV or Fire TV device might be made by Polk or LG. When a car is running Apple CarPlay or Android Auto, it can act just like a smart speaker. When multiple devices are involved in the exact same act of data collection, there will be a need for complicated business licensing strategies and agreements. Because data collection is so valuable, each company wants a piece of the data collection pie and as much freedom as possible to share and profit from that if permitted and consistent with its reputation. How each company tries to slice and derive value from the IoT data collection pie will be a scramble and a tangle, and our right to control our personal data will be affected unless law catches up to reality.

Next Generation Tech

Blockchain technology and the metaverse arise as the IoT comes of age.

The metaverse, not yet a word within Merriam-Webster, is [defined by Wikipedia](#) as “a hypothetical iteration of the internet as a single, universal and immersive virtual world that is facilitated by the use of virtual reality (VR) and augmented reality (AR) headsets.” It's a guess how prevalent the metaverse will be. But it's not uncommon to hear some informed people theorize that one day people will spend half or more of their life in the metaverse. Data collected by VR or AR headsets will be valuable. Will a consumer using an Apple headset be able to interact with another consumer with an Android

headset? Can a headset wearer object to collection or sharing? Who will “own” such data and what will be the rules on its sharing?

Bitcoin, and other cryptocurrencies offer distributed ledger technologies. A benefit is being incorruptible by any single user because the ledger is agreed to and recorded by all system nodes. If a ledger can’t be changed, it may not be compatible with data privacy laws that give users control over their data. And we know from attacks on crypto businesses that blockchain does not guarantee privacy. Implementations of an IoT device with distributed ledger aspects will encounter challenging regulations. How can the General Data protection Regulation (GDPR) “[right to be forgotten](#)” be workable with distributed ledgers? Creating products which incorporate distributed ledgers may require the partition of collected personal data features to meet personal data privacy standards.

Data Localization and Societal Control

And then there’s George Orwell’s warning – technology advance and privacy may be incompatible. Data localization is on the rise, as many nations claim the right to control their residents’ creation, sharing, and use of data across borders. There’s China’s social credit system and “Great Firewall.” Indonesia insists that global social media and payment systems that offer services to Indonesians must register with its government and provide personal data to the government upon request within four hours. Russia seizes the bank account of Google’s Russian subsidiary on the ground that Google is not in sync with Russia’s data localization laws. When IoT devices and data flows involve a multi-country supply chain, is there any protection of privacy in sight? International trade at least has the World Trade Organization. There is no World Data Privacy Organization, and none in sight. The challenges to our personal data privacy abound, as we enter a new stage of data collection, sharing, and use.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.