withersworldwide

Covid-19 creates numerous use cases for the Internet of Things, but are they legal?

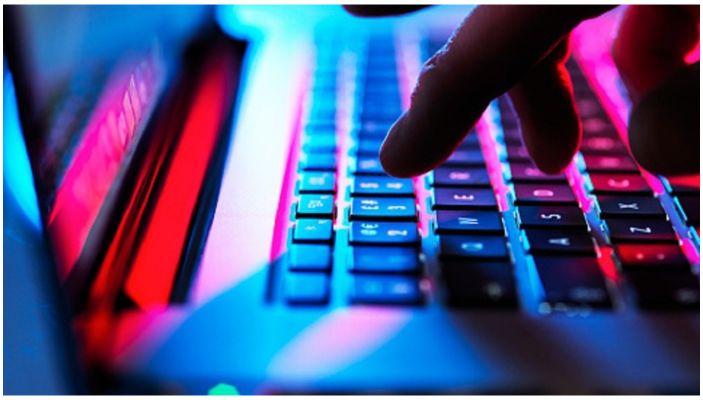
13 JULY 2020

M. Ridgway Barker
PARTNER | US

CATEGORY:
ARTICLE

CLIENT TYPES:
CORPORATE

TECHNOLOGY



Ridgway Barker co-authored this article with Joseph Bambara.

The world today is facing an unprecedented situation. Few imagined that a virus could paralyze our world. With respect to IoT and Covid-19, how do we safely return to normalcy and how do we recognize it when and if it returns. Perhaps as important, how do we efficiently and legally monitor, track and gain insight into Covid-19 without intruding on privacy or exposing sensitive personal data. To control any exponential spread of Covid-19, the solution is understanding where, how long, and who are symptomatic people congregate. This is easily done today with technology known as Geofencing, which creates a virtual perimeter using GPS, RFID, Wi-Fi, BlueTooth signal, and cellular network. This technology can recognize the patterns of infection. If we respond early, we avoid or disable pandemics in the future.

The Internet of Things ("IoT"), as coined by Kevin Ashtock back in 1999, is a system of connected things. Things are interrelated computing devices, such as beacons, air, and temperature sensors, and even people that are provided with unique identifiers, known as IP addresses. Using these identifiers and IoT, we can detect, record, and respond to any event without requiring human-to-human or human-to-computer interaction. For example, an event may be recording the IP of someone who has just passed a temperature sensor with fever symptoms.

Many countries are using IoT in the form of GPS enabled applications to track and restrict people's movements. Russia, Poland, Singapore, South Korea are in this grouping. Hong Kong started its quarantine efforts from the airport. Arriving passengers were given wristbands along with a unique QR to track their movements. Passengers downloaded an application known as 'StayHome Safe' on their smartphones and scanned the QR. After calibrating, the mobile device now tracks their every movement. Is this degree of surveillance tracking an acceptable tradeoff? Are we willing to sacrifice a significant degree of our privacy to prevent the spread of Covid-19?

Hospitals and medical centers quickly adapted and used Zoom and Microsoft Team to provide telemedicine services to diagnose COVID-19. Predictably, the number of calls overwhelmed the available human resources. According to Partner Healthcare in Boston and Providence St. Joseph Health System in Seattle, the average wait time was extremely long, and many callers dropped out. Here again, IoT developed software that was implemented to provide chatbots for pre-screening visitors. The bots determine the severity of the visitor's condition and route casework to the available pool of telemedicine professionals. IoT, when properly implemented, can provide valuable efficiencies.

According to Providence St. Joseph Health System in Seattle, which created a similar tool in collaboration with Microsoft, this system served almost 40,000 patients in the first week itself. Bespoke, a Japanese company, launched 'Bebot,' a chatbot that answers coronavirus related questions via a mobile application. Many other hospitals are looking at similar solutions.

In the US, IoT in the form of self-driving robots is used by companies like TMiRob, UVD, and Xenex Disinfection Services to cleaning, sanitizing, and disinfect medical facilities. They disinfect the surfaces by emitting high-intensity ultraviolet light, which destroys the virus by tearing apart their DNA. They are Wi-Fi based and can be controlled through a mobile application. Currently, these are being used in China, Italy, and the USA.

With social distancing becoming the new normal, drones have found some innovative uses:

- To monitor and enforce the stay at home orders in Spain and China.
- To disinfect the highly contaminated hotspot of Daegu, South Korea.
- To fly medical samples and quarantine materials in Xinchang, China.
- To check temperatures of those in quarantine through infrared thermometers mounted on drones while the patients stand on their

balcony.

There is also an increasing awareness among people to avoid touching vulnerable surfaces like doorknobs, light switches, etc. particularly after touching mails or packages. Instead, they use IoT enabled smart speakers, lights, security systems, etc. to open doors and switch on lights.

We can use smart security systems to request deliveries to leave a package inside the house while the user unlocks the door from their phone. That said, with these conveniences comes risk.

Technologies like IoT will face legal and regulatory challenges. IoT will create cybersecurity risks. How will governments regulate systems combining AI and the IoT? Our privacy and security will be at considerable risk if we do not address intruders hacking IoT with malicious intent. When it comes to controlling data, the US government has been, comparatively speaking, reluctant to regulate. There exists no US legislation as far-reaching as the European Union's Global Data Protection Regulation (GDPR) enacted in May 2018. This "hands-off" approach is perhaps a proper action (or inaction), as early regulatory intervention can forestall or even foreclose specific paths to innovation. The hope is that innovators will develop a code of conduct and a culture of self-enforcement to avoid hindering the widespread adoption of these technologies, thereby avoiding restrictive and stringent government regulation. Key among these considerations is how to regulate, and cyber protect how IoT data is collected and maintained.

The core issues to consider are the misuse of data resulting in the following:

- The risk of bias and discrimination
- The potential for intrusions of privacy
- Mass surveillance that may infringe on democratic freedom
- Secure key infrastructure and governmental operations from all adversaries

Data is, of course, the lifeblood of IoT. IoT algorithms need data to learn and become asymptotically accurate. We will need to design these new IoT solutions with ethics in mind. We need to ensure that they are implemented with compliance to the laws and regulations which will evolve and keep us secure.

As we have learned from this current crisis, going forward, we need to be proactive and not reactive. We need technologies like IoT that perform intelligent review and consumption of data to provide a change in behavior to address each issue. Stay in touch with us at Withersworldwide to learn how to prepare your businesses both technically and legally to incorporate emerging technology trends safely and efficiently. The Withers team can help their financial partners with the legal and technology expertise to stay ahead of these developments.

Authors

M. Ridgway Barker

PARTNER | GREENWICH

Corporate

☎ +1 203 302 4084

✉ mr.barker@withersworldwide.com