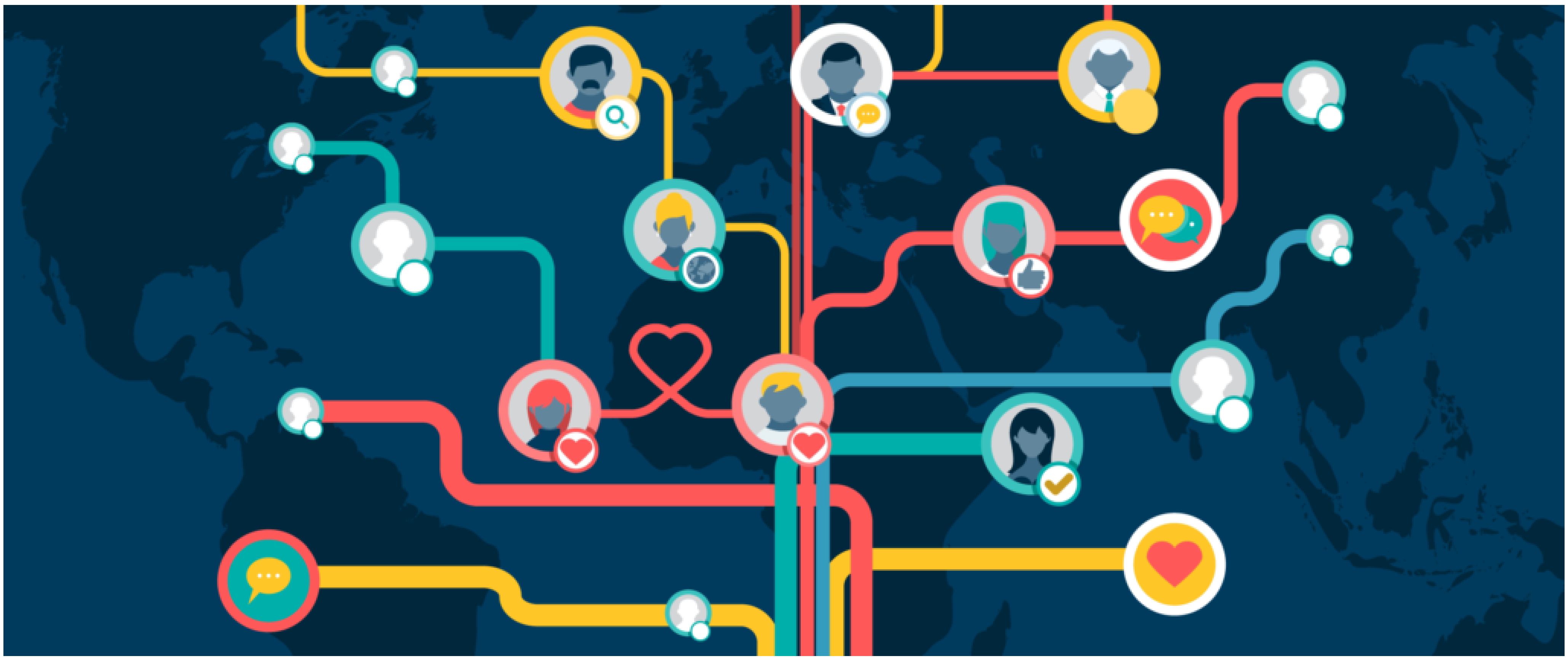
EDRM Blog

The Internet of… Bodies?

January 26, 2021 Cat Casey 0 Blog Articles, In the News, Recent News

What on earth is the IoB and should legal practitioners care?



When we think of the vast ecosystem of web-connected devices that populate our day-to-day existence, most of us think of home appliances, vehicles, and smart assistants like Alexa. But, did you know that there is an entire subgenre of the internet of things that is composed of smart devices on and sometimes inside of the human body? These smart devices are revolutionizing healthcare and often greatly improving quality of life, but there are legal and ethical issues practitioners should be aware of.

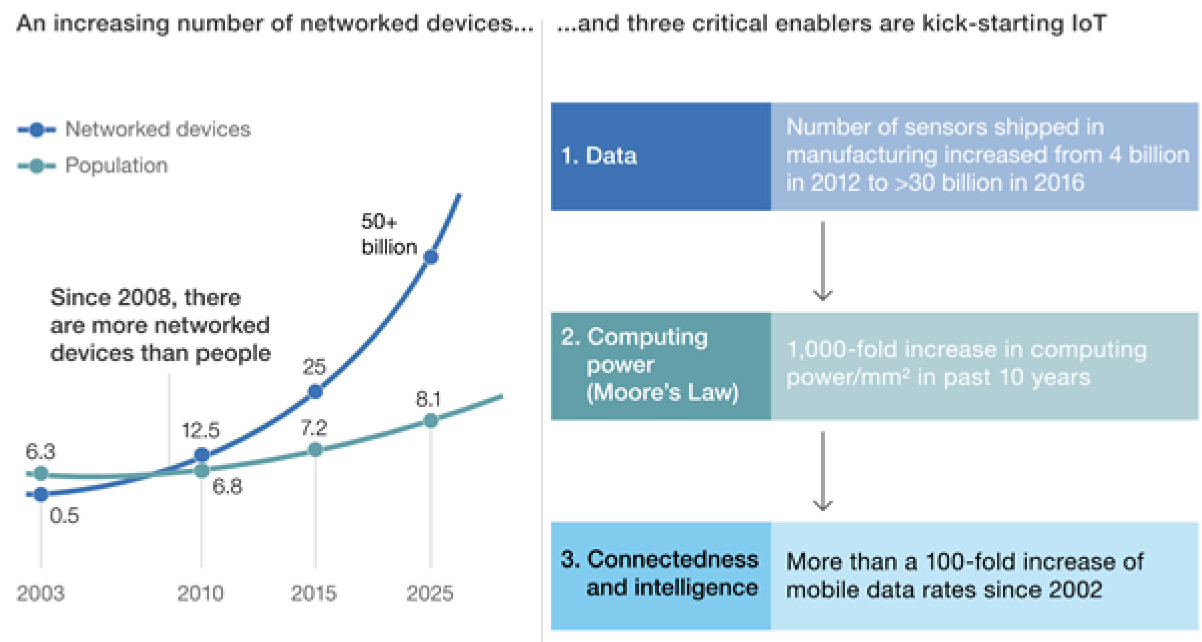
What is the Internet of Bodies (IoB)?

When I was researching for a recent post about the **Internet of Things**, the sheer scale of the **30 billion (and counting)** web-connected devices was impressive, but the realization that a large portion of those devices were physically connected to or sometime inside the human body truly shocked me. This growing industry of devices that monitor the human body and transmit the data collected via the internet is getting more vast by the moment.

Rand defines the IoB as a device that contains software or computing capabilities and can communicate with an internet-connected device or network that collects person-generated health or biometric data and/or can alter the human body's function.

While those of us who have read too much science fiction may jump to robot overlords and full-on cyborgs when thinking about the IoB, the reality is a bit more mundane. The current IoB ecosystem spans things like Fitbits, smart pacemakers and mobile device-controlled insulin pumps. IoB devices are web-connected and are worn, ingested, or surgically implanted in a human body, allowing the body to transmit information via the internet. Based on this information, the body or device can in some cases be directly modified (as in the case of a smart pacemaker or insulin pump).

English



Source: Markus Löffler, Christopher Mokwa, Björn Münstermann, and Anand Rao, "Partnerships, scale, and speed: The hallmarks of a successful IoT strategy," March 2017, McKinsey.com

Flavors of the IoB

The devices comprising the IoB operate with varying levels of intrusiveness and direct impact on the human wearing them. Monitoring everything from diet to biometric readouts and even social interactions, these devices are increasingly impacting daily life for millions to billions of people.

The IoB is divided into three generations:

Body External

Wearable devices like a Fitbit or Apple watch and more medically necessary devices like a smart insulin pump are all in this category. There were nearly **400 million wearable devices shipped in 2020** alone and that number is predicted to grow to over 600 million by 2024. Wearable tech is not limited to health and step trackers, Amazon has patented technologies for a **wristband designed to track and record workers' locations** and hand movements and even **smart contact lenses** that offer augmented reality in addition to vision correction.

Body Internal

These devices are ingested or implanted inside the body to monitor or control various aspects of our health. Cochlear implants, smart digital pills, and even artificial pancreas fall in this category.

Body Embedded

In this iteration, the embedded machines and the human body are melded together and have a real-time connection to a remote machine. Think Brain Computer Interface (BCI), where a person's brain is directly merged with an external device that can monitor and control body functions in real-time.

Holy grail or Pandora's Box?

The possible use cases for IoB technology are legion: brain implants that could allow amputees to control a smart prosthesis, artificial organs that could use tech-optimized timing to excrete enzymes, even smart diapers that let you know when a baby needs a new nappie. Unfortunately all of this upside is offset by legal, ethical, and privacy considerations. This wealth of data, in particular, poses fundamental concerns about the individual right to privacy and autonomy.

The main concerns about IoB data fall into three main categories:

IoB Security

As with any web-enabled device, the IoB devices are vulnerable to security breaches. However, in the case of IoB devices and data, the stakes are much higher. In the case of embedded medical devices in particular, data manipulation or being locked out of an account could result in grievous bodily injury and even death. Imagine if the wi-fi-enabled pacemaker of a world leader (for example, Dick Cheney) was compromised by a bad actor — the results could be even larger than just harm to the individual with the device!

IoB Privacy

The devices that snake up the IoB ecosystem have myriad privacy concerns because they track, record, and store things like users' whereabouts, bodily functions, and what they see, hear, or even think. Can a health insurance company deny coverage based on information obtained via a digital pill? Determining who can access, collect, or interact with this sort of personal information and personal health information is a key consideration with any IoB device.

IoB Discoverability

Although the IoB is a reltaitve newcomer to digital evidence, there have already been multiple cases that data from these devices has been discoverable and dispositive to cases. From a **smart pacemaker's data used to disprove an arsonist's defense** to **wearable fitness tracker's geolocation** used as evidence in a murder case, the precedent to use IoB data is growing by the day. It is important for legal practitioners to consider these IoB devices in the context of their evidence scoping as well as balance the potential violation of personal autonomy and privacy the use of the data presents.
