The Internet of Everything: What It Means for Lawyers

by Sharon D. Nelson, Esq. and John W. Simek

What does the Internet of Everything mean for lawyers? Evidence - lots and lots of new sources of evidence. The continuing loss of privacy. A life that is so connected to the Internet that it will be hard to get through even a few minutes of our day without the Internet having an impact. But we are ahead of ourselves - so let's step back and analyze an accelerating trend.

We first became interested in the Internet of Everything (known as IoE) when wearable technology became the hot new trend. We've heard the words for a couple of years but wearable tech really started to pick up steam in 2014 as companies rushed to the marketplace with, in particular, smartwatches.

Research firm Gartner anticipates that revenues from wearable tech will more than triple by 2016, going from $1.6 billion to $5 billion. It is no wonder that companies are rushing to board that train.

A Day in the Life of an IoE Lawyer

The day is not far off when we will be awakened by a clock that we have programmed over the Internet. We will wake, by our choice, to slowly increasing light, gradually louder nature sounds, or one of many other possibilities. If you prefer, your smartwatch can do the same thing – or just pulse gently on your wrist or not so gently until you turn it off. Your "smart" home will either sense that you are up through your motion or be programmed to know your wake-up time. Lights, music, TV – everything will come on as you walk down the hall. By the time you get to the kitchen, your coffee will be ready and waiting. Your refrigerator may remind you that you are out of milk – or simply order it for you.

If you hop on the treadmill, your smartwatch will dutifully record your pulse, heart rate, miles logged, speed, etc. and place it all conveniently on the Internet for you. No data entry required.

As you check your e-mail on your smartphone, you can also remotely turn on the car to warm it up if it is cold – and no worries about thieves - the doors are locked and will not unlock until you step outside because only the proximity of your smart key can unlock them. Pull out of the driveway and your smart home will lower the heat and turn off the lights. The car itself will notify your secretary that you are on your way in – and via the car and Bluetooth, you can do a little billing by talking to clients about case strategy while you sit in traffic. In the not too distant future, the car will drive itself, constantly pinging the Internet for the fastest route in current traffic.

When you get to work, it will be to an office that a previous generation would not recognize – where the Internet is, even more than today, in constant use. Remote appearances in court will be the rule rather than the exception, with real time recording of proceedings and real time machine-assisted translation where needed. And of course, proceedings will be webcast by default.

Your smartphone or smartwatch, both of which have access to your calendar, will softly ping you from time to time so you don't forget to call a client or attend a meeting – they will know how long it will take you to get to the airport and remind you when it is time to leave. Even while clearing security, you'll be able to keep up with your e-mails and texts while standing in line thanks to your smartwatch or smartphone. Or if you prefer Google Glass, it can serve the same function – and let you videoconference with clients. And if you don't mind people thinking you're talking to yourself, you can inquire from either device about the weather at your destination. Hungry? Stop and grab a burger – and pay with your iPhone via ApplePay.

All of this is only the tip of the iceberg.

The Testimony of Your Nest Thermostat

Suddenly, everyone is talking about the Internet of Everything, many about the marvels it will provide and a fair number talking about privacy implications. We recently attended a CLE taught by digital forensics expert (and good friend) Craig Ball who pointed out that the new world has given us many new sources of evidence.

The audience was stunned when he said that one day his NEST thermostat might provide evidence against him.

The Nest Learning Thermostat learns your schedule, when you are away and when you are home – and it can be manually programmed using a browser or an app. While the machine's "evidence" that you were "likely gone" because of your customary schedule is suspect, if you have deliberately connected to the device over the Net and adjusted the temperature to reflect that you would be away for two days, that action could effectively counter your sworn testimony that you were at home when your business partner was murdered.

Smartwatches and Smartphones

By the time you read this, it is possible that the Apple Watch will be out. As we write, the release date is still showing up as "early 2015." Of course, there are plenty of smart watches available now, including, among others, the Samsung Gear, the LG G and the Moto 360.

If you've ever wondered how lawyers use a smartwatch, just Google Florida solo practitioner Rick Georges and the word "smartwatch" and you'll find articles and podcasts describing his love affair with his Samsung Gear 2. As he points out, lawyers get in trouble using their

smartphones in court, but the more subtle use of the smartwatch doesn't seem to cause a problem.

And who among you does not own a smartphone? We have already given up much of our privacy by allowing apps (and the phone manufacturer and service provider) to collect our data. But it will get worse.

Already, some smartphones can recognize a face or a voice, providing ample evidence of where you were and what you said. Technology can also analyze our voices to determine emotion. Moodies, an app developed by Beyond Verbal, is able to detect a speaker's mood based on nothing more than a voice. Worldwide call centers are testing the technology to help operators determine whether callers are upset and likely to switch their business to a competitor unless they are moved up in the queue.

Many app-makers are experimenting with software that can also analyze someone's emotions or honesty by a few facial cues. Sensors could be on your wristband activity tracker (which connects to the Net too), your smartphone or your smartwatch, continuously tracking your emotions. Software is currently being developed to analyze emotions and then project the results on a screen such as Google Glass.

What will happen to the white lies we live by? "I'm so happy to see you" to someone you can't stand. "Of course I remember you" to someone who is nowhere in your memory banks. And what about the common phenomenon of someone saying "I love you" – when they don't? The consequences there could be far more serious.

Politicians might be driven out of politics by technology that could determine whether they are lying. Hmm, now there's a thought . . .

How Big a Deal is IoE?

Pretty darn big. We referred to the company Nest above. It is fascinating that Google purchased Nest in January of 2014 for the whopping price tag of $3.2 billion. Do you think Google sees a future in IoE? At work, at home, in cars - on phones, computers, tablets, appliances – in wearable tech (on people and animals) and in machines of all descriptions. On wired or wireless networks, Google (and many others, notably including Apple) see the world through the prism of endless interconnection possibilities.

We live in a world where cars drive themselves, health monitors can interact with medical staff, and refrigerators can order food for you (they can also send out spam if compromised – yes, this has really happened). We can make sure our elderly parents take their meds and even watch or listen to them to make sure they haven't fallen. We can watch our kids at school and

our dogs at the doggie day care center. It is getting to the point where we almost lose track of all the ways in which we are connected to the Internet.

This is largely the point. When Apple representatives talk about the "Apple ecosystem", they refer to having interconnected computers everywhere in our lives.

Privacy

In a full-blown Apple ecosystem, how much would Apple know about you? A whole lot.

How safe is our data in such an interconnected world? Which laws apply to protect it? Can the U.S. protect information which will likely be scattered across the globe with domestic laws alone? Is there any realistic way for international law to govern and to be adequately enforced?

From a government snooping point of view, the IoE is a Christmas gift many times over. Data, data everywhere. The more IoE you have, the more you can analyze the resulting "big data" and even anonymized information might lead to identifying individuals and their activities. It is simply a complicated mosaic which the supercomputers can figure out – far better and faster than the humans.

Needless to say, from the point of view of commercial vendors, all the data about us will be collected, analyzed and sold. As it is often wryly observed, "If something online appears to be free, you are the product."

Security

While we used the word "privacy" as a subheader, we might just as well have used the word "security" since the two are so closely intertwined. The greater the volume of data kept on all of us, the less likely it is to be adequately secured. And we guarantee, much of the time, we will be so busy living our lives connected to the Net or functioning via the Net (sometimes without any real thought on our part) that we will be clueless about all the "evidence" we leave documenting where we are, what we are doing, thinking, buying, etc.

Cybercriminals will exploit the data, happy to know when we are not at home, or where our expensive car is. They are no doubt chortling at the constant proliferation of data about individuals that will be available to them. As noted above, they have already utilized a refrigerator to create a botnet to send out spam – and how many other smart appliances are there?

We have already seen how easy it is to hack a car to cause an accident or how simple it might be to hack a medical device like (yikes) a pacemaker. Former Vice President Dick Cheney was so concerned about this that he deactivated the Wi-Fi function on his pacemaker.

A July 2014 HP study revealed that 70% of IoE devices use unencrypted network services and 80% of devices did not require passwords of sufficient length and complexity. Why? Because the majority of IoE devices are targeted to the consumer, where convenience and ease of use are far more important than security. Adding security, authentication and logging functions will also add additional cost. Hence the resistance to go down that road.

As ever, encryption is your friend, and you should encrypt your data wherever possible, but all too often, the protection of your data, including your law firm data, is managed (or mismanaged) by a third party over whom you have no control.

IoE will mean a wealth of opportunity for legal privacy and cybersecurity experts. If you are looking for "open space" in a crowded field of horses, this is your chance to make a run for the roses.

The Future of IoE

While no one can predict the future of IoE with any certainty, the vast monies invested in it indicate that widespread adoption is inevitable. Our guess is that no more than 5-10 years will be required before IoE is the rule rather than the exception for all except the poor.

We can pretty well guarantee that the law will lag far behind the technology as it always has. Law firms, many of which don't even have "bring your own device" (BYOD) policies, will fail to adopt policies or controls governing IoE in the workplace. Privacy will continue to diminish and governments and cybercriminals will increasingly snoop on all of us, each for their own reasons.

The IoE is unstoppable. Like a global earthquake, it is sure to rattle (and open) windows into all our lives. Lawyers will need to be vigilant that their personal and professional use of the IoE doesn't result in the compromise of client data. The line between personal and professional use may blur beyond recognition in an always-connected world.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com