NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 18, ISSUE 1: OCTOBER 2016

OPEN HOUSE: CONNECTED HOMES AND THE CURTILAGE KEYNOTE, UNC JOLT 2016 SYMPOSIUM

Mary Ellen Callahan

We have heard all morning about legal issues with the Internet of Things; I want to begin with acknowledging the human aspects and human interests in Internet-enabled homes, which are more visceral and personal than IoT devices monitoring other interactions. I have worked in privacy for almost 20 years, and I passionately believe we need to think carefully about the privacy implications that come with technology, especially when we are dealing with the home.

The rapid increase of technology is re-defining our very concept of "home," and that raises several crucial questions:

1) what do we mean by "home,"

2) why do we expect more privacy in our homes, and

3) if that is a legitimate expectation under the current legal doctrine, is that expectation sustainable – or even reasonable – in a sensor-laden world where actions inside and outside the house are documented, gauged and stored?

CURTILAGE OF THE HOME

More than 50 years ago, Justice Potter Stewart wrote that the right to retreat into the home lies "at the very core" of the Fourth Amendment protections from unreasonable searches and seizures. But the concept of "home" extends beyond the walls of our houses – there is an old common law and constitutional concept that persons have a heightened sense of privacy in, and among the "curtilage" of, one's home, which is land attached to a house, surrounding it to "form one enclosure with it." The curtilage is the area created by the actions the property owner to define a ***protected space*** – even if outside the house. Think of raising fences and walls, and creating a sense of privacy or intimacy. There is a four-

factor test (under *United States v. Dunn* from 1987[1]*)* that asks: (1) how close the claimed curtilage is to the home; (2) whether the area and the home share a common fence or barrier; (3) how the residents use the area; and (4) what steps the resident took to protect the area from observation by passersby.

The protection of curtilage in a Fourth Amendment analysis has been reaffirmed in the 21st century, by Justice Scalia, who was a champion of protecting the curtilage of the home; his Fourth Amendment jurisprudence will be missed. In *Florida v. Jardines*[2] in 2013, Justice Scalia, writing for the majority, held that a trained dog, sniffing for marijuana scent outside a home but inside the fence, conducted an unauthorized search under the Fourth Amendment, because it violated the curtilage of the home. The fence and space defined by the homeowner were among the calculations that Justice Scalia made.

Reasonable Expectation of Privacy

Mr. Jardines had a reasonable expectation of privacy at his front door – but as many people in this audience know, the "reasonable expectation of privacy" test has had its ups and downs in appellate jurisprudence – a photograph from the air may not trigger reasonable expectations of privacy, but an infrared scanner to see the heat emissions within the house may.

In fact, in the 2001 *Kyllo* decision (involving infrared scanners to see whether a homeowner was using marijuana grow lamps), Justice Scalia posited that one of the questions the Court used to determine whether the search was unreasonable was asking whether the device the government used was generally available to the public. When "the government uses a device that is not in general public use . . . [then it is] unreasonable without a warrant."

We would all agree that the devices the general public use today are very different than they were 15 years ago when Justice Scalia wrote those words. And, as technology has evolved over that time, the amount of data collected using that technology has increased exponentially. The Court will be hard-pressed to rely on

[1] United States v. Dunn, 480 U.S. 294 (1987).
[2] Florida v. Jardines, 569 U.S. 1 (2013).

its "general-population-using-the-technology" test to determine whether a search is unreasonable. As Chris Ayers pointed out, in South Carolina, the AMI smart meters installed by the public utility were able to identify individuals growing marijuana, reporting them to the police. There was no Fourth Amendment search or seizure because the investigation was not performed by the government. As we will discuss later, these indirect disclosures will increase with more private companies collecting more unique and detailed data.

Furthermore, given all the sensors within the Internet of Things-enabled technologies that are designed to collect, store and transmit information, can we even have a reasonable expectation of privacy? This is particularly true if the ubiquity of the use itself is part of the reasonableness test. This tautological logic is frustrating.

But then again, even if we do have a reasonable expectation of privacy, with smart fridges and smart thermostats and other smart-home devices, we are inviting someone into the house – and they never leave. In the seminal Fourth Amendment decision in *Katz,* Justice Stewart wrote that the reasonable expectation of privacy could extend to the inside of a public phone booth – but that was because Charles Katz – who was using the phone booth to make illegal bets all over the country – "knowingly [sought] to preserve [his conversations] as private."

Then again, who are we being secure from? The Fourth Amendment – and government access to data – is an important consideration, but the sharing between and among private companies also must be contemplated.

Third Party Doctrine

As I mentioned earlier, an additional constitutional standard could make protecting the curtilage increasingly difficult – the third-party doctrine. The third-party doctrine is a Supreme Court principle that holds that people who voluntarily give information to third parties—such as banks, phone companies, Internet Service Providers (ISPs) and e-mail servers—have "no reasonable expectation of privacy." Some legal theorists feel the third-party

doctrine was wrongly decided in the previous century, forty years ago in an analog world. That was back when you had to go to a bank to open an account. When the only "third party" involved in sharing photos with family and friends was a leather-bound album.

Not so today. Given how interconnected and electronic our information and assets are today, there are few things – including all the devices we talked about this morning – that would not have some element of interaction with a third party.

Justice Sotomayor recognized this, in her 2012 concurrence in *United States v. Jones*[3], opining: that "[m]ore fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."

These "mundane tasks" could include every aspect of home living – reading, cooking, movement within a home, using electricity throughout the home, and home security monitoring with alarm systems, cameras and sensors. Ironically, taking steps to increase our home and curtilage security may actually reduce our legal protection, since most of us will have to use a third-party system (like Sawyers Control Systems) to protect our homes. The call to re-evaluate the third-party doctrine by Justice Sotomayor is essential if we are to remain safe and secure – physically and under the law – in our 21st century homes and our curtilage.

BIG DATA'S HOUSE

Part of the conundrum of the IoT Home is that much of the activity that is being recorded, gathered and analyzed had previously taken place, but they had not been previously analyzed. Kids playing in the basement. Parents making dinner. Doing laundry. Yardwork. Sleeping. All activities that have occurred since homes were first built, but the data-ification of these activities – and the crunching of that data, on the individual and

[3] United States v. Jones, 132 S. Ct. 945 (2012).

aggregate levels – has only just begun. Previously, a single day, or event, would generally be fleeting, a passing moment that was not memorialized, unless it was a special event. This obscurity made us less aware of individual days, and more aware of unique events.

With connected homes and ubiquitous sensors, every day is special, unique, categorized and memorialized. Professor Hartzog used the phrase "fixation of a moment designed to be fleeting" in another context – surveillance – but the concept is the same. These snapshots of data are fixations on moments, on processes. The ubiquity of these Internet-enabled devices (currently at 4.9 billion devices and increasing to 25 billion by 2020, according to Gartner) add layers of complexity and analysis on these mundane tasks previously undocumented.

That analysis can be useful, effective, and improve not only the lives within the connected home but also having a societal impact. The sensors and the smart homes are looking for ways to save money, looking for patterns and ways to improve your quality of life along with non-obvious relationships.

When I was at the Department of Homeland Security, we spent a lot of time looking for non-obvious relationships, patterns that appeared through the analysis of big data. Non-obvious relationships do not always appear, and therefore the collection and analysis of a great deal of information without demonstrating any rewards can be ineffective if not analyzing the right data.

With that said, major benefits can be had from collecting and crunching lots of data. But, with any collection of data, even the seemingly benign, we have to ask questions that are usually a lot trickier to answer than it seems: "Who else gets the data?" "Is the data being shared with other parties?" You know you are sharing data with a first third party, Company X, only for Intended Purpose Y, but is that information being shared with Company Z, too? And if that data is being shared with other parties, what rights do those parties have to your individual and aggregated data?

Obviously, under the third-party doctrine, you no longer have a reasonable expectation of privacy to your data that has been shared with your first third party. However, you still have other expectations about that data, including keeping it safe and secure,

and using it only for the purposes intended. In this situation, the third-party doctrine may say that you no longer have a privacy interest in information about your own home, but human nature and consumer expectations would differ.

Since the biggest threat to connected homes is the risk of secondary or unknown uses, we as purchasers of the devices and sensors need to understand what this all means for us and our homes.

INTER-CONNECTED WORLDS

Sensors are useful, helpful, maybe even crucial, but they also fundamentally shift how we interact with our surroundings. They enter with little, if any, real notice and choice, and then blend into the scenery: unobtrusive, silent and passive. Once they are woven into the fabric of our lives and homes (and sometimes literally woven into the fabric), it's easy to forget they are there.

We must pay close attention to this issue, before we lose control of our homes, hearts and welfare. We are monitoring, gauging, storing and sharing data about personal activities and processes; we are sharing elements of the curtilage with strangers in the cloud, online and in social networks.

In this always-on world, the ecosystem is the crux, and the weakest link in that ecosystem is the vulnerability. The fragmentation in software ecosystems, and the need to have multiple systems and software inter-connections, leads to inconsistencies, vulnerabilities and opened networks, subject to unauthorized access.

Transparency

Mary Culnan and Paula Bruening have outlined a detailed theory on how transparency and choice can be effectuated in a sensored world where the ability to convey appropriate notice may be constrained.

But such transparency and choice are not required; it is only a best practice, consistent with the fair information practice principles ("FIPPs") set forth by the Federal Trade Commission and other enforcement agencies (as David Hoffman discussed

earlier). In fact, in one of the few laws that govern the collection of online personal information, under the California Online Privacy Protection Act (CalOPPA), an "online service" only requires a privacy policy for the collection of personal information, narrowly defined to include name, address, and phone number among other data elements. The sensors we are discussing today do not meet these legislative definitions.

The devices we are considering today are not online services – they're not asking us to enter our social security numbers – they are sensing, storing and collecting data without us lifting a finger. We are considering devices for which passive data collection is part of the appeal. And there is often no way to provide a checkbox to require the consumer to click "agree" before the data starts to be generated. As Paula Bruening discussed, moving to a transparency regime is important. But it also may be difficult.

And that is part of the problem – smart homes and sensors are not governed by legislation; they do not fall into the sectorial approach to privacy that the U.S. has adopted. Instead, we are relying on FIPPs and best practices and reasonable expectations. These are all well-intended, but as discussed earlier with reasonable expectations, the scale can shift, and furthermore we have put a great burden on individual consumers to wade through systems, programs and choices.

Choices

A reasonable expectation of privacy, coupled with notice from the company and some "choice" associated with the data collection, is consistent with industry best practices, and the FIPPs. And even though there may be notice and choice in discrete instances, that choice is often illusory – it is impossible to use certain brands of connected televisions without agreeing to the collection and use of browsing and viewing information for targeted advertising, for example, and the choice is controlled at the individual device level rather than holistically. Professor Hartzog talked about focusing first on the technology, how it is designed, how it is supposed to be sharing the information. I think that is part of the process, but I think the portion of the IoT

analysis that is under-emphasized is the interconnectivity between the technologies and the choices.

The Online Trust Alliance has established Internet of Things principles for companies developing IoT products. Among the principles are allowing sharing only with opt in, and allowing people to delete the collected information. The Federal Trade Commission (FTC) highlighted notice and choice, data security and data minimization in its IoT guidance last year. These are important principles, but I worry about overloading consumers with choices for multiple devices (even at multiple points in time). And as much as I like my job, most lawyers who write privacy policies and consents for just-in-time notices are looking at this as a compliance exercise, not an educational one.

The FTC recommends writing policies, notices and other consumer-facing documents at the reading level of an eighth grader. Who here has read a privacy policy recently? That must be one heck of an 8th grade teacher; hats off to her or him.

The test I usually apply is: "Will my mother understand it?" My mom is a great person, clearly, since she raised [my brother Tom Callahan] and me as well as our five other siblings. She also only has a high school degree, and is 82 years old. She can operate her iPhone, and can do some stuff on her computer, but for anything else, Tom's business partner and our brother Pat has to remote into her computer in order to accomplish what Mom is trying to do. (That is a whole different type of connected home). So using her as a baseline is helpful to think about whether consumers are understanding the choices put in front of them.

One way choice can be provided is by these "just-in-time" notices and choices. The notices appear at the time you want to engage or data is going to be collected. It is one thing to provide notice via a cell phone map or application, but how does just-in-time notice work for sensors and other devices that are not directly interacting with you but still collecting data? And, with the growth of sensors and the ubiquity of the devices, providing any just-in-time notices or choices could overwhelm a person.

Another deficiency in a choice model for IoT devices in that choice is often thought of at the individual device level, when in

reality, it is the interconnectivity and the entire system that should be considered. These patchwork, fragmented software systems impede our ability to make knowing choices.

Privacy by Design

Paula Bruening earlier discussed Privacy by Design. The concept of Privacy by Design is an important element of the development of any device, much less one that is connected to your life, and your home. Privacy by Design is an approach that takes privacy into account throughout the whole engineering and lifecycle of a product. Privacy by Design can and should be incorporated proactively into Internet-enabled devices. With that said, the individual devices need to work together in an ecosystem in order to provide effective Privacy by Design. Once the process starts, including the addition of new devices and sensors, consumers have no idea how they will connect and what data they will share. The problem of the weakest link can undermine an ecosystem of devices that individually incorporated Privacy by Design, but did not consider the interconnections.

IOT SECURITY

Finally, I get to speak about the elephant in the room, or in the IoT devices – security. There are two aspects of security that are important for the connected home: 1) government access to IoT data; and 2) inherent security flaws in the devices, or in the device ecosystems that create vulnerabilities.

Government Access to Data

In addition to the struggle with connected devices and understanding the choice paradigm, the security of the sensors and their data – particularly those we use in the home – can raise alarms. Networked sensors are willing mechanisms for surveillance. That is what the devices are designed to do.

Recently, a policy debate has emerged about whether using strong encryption for communications and data storage would hinder important law enforcement investigations. The term used most frequently among law enforcement is “going dark” – unable

to see vital communications. The current debate between Apple and the FBI with regard to the San Bernardino attacks has been discussed at length this morning so I will not discuss it. With regard to the question of whether the government is losing access to certain information, there's a whole other universe of data that is not dark at all – IoT data. As Harvard's Berkman Center's Cybersecurity Project recently pointed out, the Internet of Things allows insights into aspects of society that previously were not ever monitored or stored.

Just as we are creating and collecting exponentially more data due to these connected devices, so too does the government have the ability to gain legal access to that information. And of course, under the third-party doctrine, individuals do not have a privacy interest in that data they self-generated and volunteered to third parties. The amount of data generated each day demonstrates that law enforcement is not going dark, but instead shining a different color light. As we collect, store and analyze information within our home, we are undermining the protection of the curtilage, and could be allowing law enforcement to gain access to our data – and to look for obvious or non-obvious relationships in a way they could not have absent the ubiquity of data collected in our homes.

Just last week, as part of his annual unclassified Worldwide Threat Assessment of the U.S. Intelligence Community testimony before the Senate Select Committee on Intelligence, the Director of National Intelligence James Clapper confirmed that the 15 intelligence agencies under his purview are increasingly looking to Internet-enabled devices for surveillance opportunities. "In the future, intelligence services might use the IoT for identification, surveillance, monitoring, location tracking and targeting for recruitment, or to gain access to networks or user credentials."

The risk is real. The interest from law enforcement and intelligence (and of course nefarious bad actors) is high.

And remember, one of the tests for reasonableness under the Fourth Amendment is whether the device the government used is also used by the general public. The more devices we have monitoring our actions, the narrower that test becomes.

Security Flaws

We have already discussed the patchwork, fragmented software systems. We often do not wholly understand what the devices are doing, but we understand that we need to keep the ports open in order to transmit the data. The security defaults on devices are frequently lax, or designed for open communications.

Shodan, the self-styled "search engine for the Internet of Things" is a stark example of how many Internet-enabled devices are discoverable and searchable. That includes, by the way, traffic lights and industrial control systems, along with webcams and home routers.

Of course, Shodan now markets itself partly as a vehicle to monitor network security, and to discover your own Internet-enabled devices, but in reality, the search engine facilitates our most prurient interests, allowing us to step past the curtilage of other homes, as we sit in the relative security of our own.

Just as making choices at a granular level for each of the connected devices blurs the overarching question about controlling one's own information, so too does relying on each connected device to keep your information secure, and to keep the connections between each device secure.

The impact of not having good security in a smart home could mean the home itself turns against you. Ransomware – a hacker taking control of a computer or Internet-enabled device, and holding it hostage until you pay a ransom to unlock it – has been a common problem over the past few years for personal computers and other unprotected devices. There have been apocryphal stories of hackers taking over your house via refrigerator. But that actually may not be too farfetched. The security of a connected home is only as secure as the weakest device, the device with the worst security. As we add more sensors, devices and computers into our homes, we introduce many more potential "weakest links."

TRAGEDY OF THE COMMONS

What I worry about is that our homes may become an Internet-enabled tragedy of the commons. As you all likely know, the tragedy of the commons is a situation where individuals acting

independently and rationally according to their own self-interest behave contrary to the best interests of the whole by depleting some common resource. We most frequently heard about this principle in law school with sheep and cows grazing on common lands in pre-Victorian England. But this principle may be ready for a refresh.

It is strange to think of our homes as "common" territory, even with the third-party doctrine. We keep our home safe and secure, we lock it, we establish the curtilage that helps define the boundaries of our home. How could this be a common area?

The commons that the devices are using (for their own self interest) are our homes themselves. Yes, they use bandwidth and they use electricity, but I am not talking about the physical drain on your home. Instead, I am talking about how the devices, sensors and computers documenting each of our movements, steps and activities may actually be depleting the common resource – the sanctity of our home itself.

The sensors we have installed are recording, documenting and itemizing our lives.

But by doing so, we expose ourselves to third parties with whom we have contracted (and thus diminish our privacy interest in the information in the first place).

We expose ourselves to other third parties we don't know about, maybe there by invitation, and maybe there by deceit.

We expose ourselves by relying on the security of the devices, and how they interconnect.

We expose ourselves because we may not be able to comprehend the sheer amount of information coming from the devices.

Our minds, and our homes, are the commons. We have finite resources to understand, manage and take action, but we have potentially infinite metrics to gauge.

How do we solve this? As Justice Sotomayor noted in *U.S. v. Jones*[4], allowing the third-party doctrine to continue in the 21st

[4] United States v. Jones, 132 S. Ct. 945 (2012).

century "is ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." A review and recalibration of the third-party doctrine is an important step for protecting our homes, and our curtilages, even as we collect and store more data within the home.

With that said, although I mentioned legislation earlier, I do not think it would be useful to create legislation to govern IoT. Legislation is often reactive, and cannot anticipate all uses or developments. And just thinking about Congress trying to define IoT gives me a headache.

I think self-regulation can help to a certain extent. Companies agreeing to baseline principles can be a good thing in this environment, for the companies and consumers alike, and I think having some agreed-upon baseline standards will be important for the growth of the industry, and for the protection of our own homes. As I stated earlier, the ecosystem is the crux, and the weakest link in that ecosystem is the vulnerability.

We need to take steps to protect our curtilage – physical or digital – from unwelcome observers. We can use systems and software and end-to-end encryption to secure our home, but we need to feel comfortable with these steps taken. Think about security, consider end-to-end encryption and other active steps to re-take our curtilage.

I started this talk asking why do we expect more privacy in our homes, and is that expectation sustainable in a sensor-laden world. The answer on why we expect more privacy in our homes – in addition to the legal discussion – is an emotional one. Because it is emotional, it also means that, regardless of legal jargon, the desire to keep safe and secure in one's home will continue, even in this sensor-laden world. In fact, maybe because of the sensors, we will work to protect our curtilage even more effectively. Think about our connected homes as the lifecycle of not just data, but of living.