ARIZONA STATE UNIVERSITY - CENTER FOR LAW, SCIENCE & INNOVATION

Machine-to-Machine Communications

A Legal Framework for Regulating Privacy in Wireless M2M Systems

Roque K. Thuo | roque.thuo@asu.edu

5/17/2013

In this article we explore possible legal frameworks that may be employed to guide the regulation of privacy in wireless machine-to-machine (M2M) systems and why such systems ought to be regulated to begin with. While we do not focus on a particular type of M2M system or a particular industry, we offer examples geared to specific industries in order to illuminate the privacy concerns.

TABLE OF CONTENTS

I. WHAT ARE WIRELESS M2M SYSTEMS?

According to the International Telecommunication Union (ITU)[1] Machine-to-Machine (hereafter "M2M") communications is the communication between two or more entities that do not necessarily need any direct human intervention. Said another way, M2M are simply machines "talking" to each other. A few examples of M2M systems include:

- implantable medical devices such as:
  - visual prosthetics to restore sight to the blind,[2] or
  - implantable defibrillators;[3]
- vehicle telematics systems: vehicle-to-road, vehicle-to-vehicle, vehicle-to-service systems;
- home automation controllers;
- smart grid and automated meter infrastructure;
- security and surveillance systems.

Wireless M2M systems are those wherein the machines communicate wirelessly via radio frequency communication. Wireless M2M systems could communicate through various wireless protocols such as Cellular 3G networks, 4G networks including WiMax and LTE networks, WiFi, Bluetooth, Zigbee, as well as any proprietary radio communication protocol. This article is not concerned with the type of wireless communication protocol actually used.

M2M is also interchangeably referred to as "Internet of Things" (IoT)[4] or as "Machine Type Communication" (MTC)[5]. In this article we distinguish IoT from M2M. We consider IoT as the abstract integration of communications processes with the Internet, and M2M as machine-to-machine interactions which may or may not integrate with the Internet. So for this article, a home automation controller that directly interfaces an alarm clock to a coffee machine with a local-area-network (LAN)

[1] ITU (International Telecommunication Union) is the United Nations specialized agency for information and communication technologies – ICTs – that, inter alia, allocates global radio spectrum and satellite orbits, and develops the technical standards that ensure networks and technologies seamlessly interconnect.

[2] For example, a surgically implanted neurostimulator from Second Sight Medical Products wirelessly communicates with eyeglasses housing a miniature video camera. External video processing unit attached to glasses via cable converts the images into instructional signals and sends signal back to the glasses to be wireless transmitted to the implant. http://2-sight.eu.

[3] See, e.g., implantable cardioverter defibrillator (ICD), implanted under patient's skin which interfaces with an external computer located in doctor's office or clinic that is used to program the heart device and autonomously retrieve information from the device. It continuously monitors the patient's heart and restores it to its normal heart rate. http://www.medtronic.com

[4] European Union Federal Ministry of Economics and Technology defines IoT as the technical vision for the integration of any kind of object into a universal digital network. EU Policy Outlook RFID, 2007.

[5] 3rd Generation Partnership Project (3GPP) nomenclature. 3GPP unites six telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TTA, TTC).

that is not connected to the Internet is regarded as a machine-to-machine system but not as part of the Internet of Things.

As might be evident, many of the example M2M systems identified above are not new. The natural question then might be why we ought to be concerned now if these systems have been around for a while with presumably little or no privacy regulation especially given the old adage "if it isn't broken don't fix it." There are a number of key reasons why it would be wise to pay critical attention to privacy in wireless M2M systems sooner rather than later.

A number of factors have contributed to the ubiquity and pervasiveness of Machine-to-Machine systems such as advances in semiconductor manufacturing, advances in wireless technology and recent government mandates.

Advances in electronics have led to smaller, cheaper, and lower power devices. One reason for this is what has come to be known as Moore's law[6] where devices sizes shrink every so often and this shrink not only leads to cheaper devices – because we can now build more devices into a single microchip – but also enables devices that could previously not work for their intended purpose due to size, e.g., miniature implantable medical devices (IMD's). Advances in circuit technology has also enabled low power devices, a critical feature for many battery-operated devices such as IMD's and remote sensors.[7]

Advances in wireless technology has been brought about by regulatory policy such as FCC freeing up unlicensed spectrum in the 2.4GHz band[8] which made it economically viable to implement wireless systems,[9] as well as innovations in wireless data communication systems which allowed for efficient reliable communications over noisy data channels.

[6] While not technically a "law," Moore's law first announced by Intel Corp's co-founder Gordon E. Moore in the 1980's, roughly holds that the number of transistors incorporated in a chip will approximately double every 2 years. See http://www.intel.com/content/www/us/en/history/museum-gordon-moore-law.html. Retrieved 2013-03-20. (The transistor is the basic building element used to create communication, control and computing devices used in M2M systems).

[7] For battery operated devices, the lower the power consumed by the device (1) the smaller the device needs to be; (2) the longer the device can operate on a single battery thus adding to convenience; (3) the smaller the battery needs to be – or even no battery at all for solar charging.

[8] Federal Communications Commission Spectrum Policy Task Force, Report of the Unlicensed Devices and Experimental Licenses Working Group, November 15, 2002. http://transition.fcc.gov/sptf/files/E&UWGFinalReport.pdf. Retrieved 2013-03-20.

[9] Unlicensed spectrum means no licensing costs needed to use the spectrum. Universal world-wide coordination of the Industrial Scientific and Medical (ISM) band (2.4GHz is in the ISM band) leads to low cost devices (economies of scale) because device manufacturers can market their wireless modules worldwide. Availability of such a high frequency band leads to smaller devices because higher frequencies require small antennas which is a critical feature for some types of M2M systems.

Government mandates have also driven the adoption of wireless M2M systems such as mandates in the National Broadband Plan, Wireless Health, and Smart Energy. These mandates have increased the number of deployed M2M systems by lowering economic barriers to entry through funding, as well as lowering investment risks. For example, a partnership between the Federal Communications Commission (FCC) and the Food and Drug Administration (FDA) aimed at ensuring that communications-related medical innovations can swiftly and safely be brought to market[10]; amendment of Parts 2 and 95 of FCC Rules[11] (47 C.F.R. 2, 95) to provide additional spectrum for the Medical Device Radio Communication Service in the 413-457 MHz band; FCC OET order to permit the retinal prosthetic device discussed above to exceed the Part 15 (47 C.F.R. 15) limits for intentional radiators[12]. Such exogenous regulatory changes have accelerated the deployment of M2M systems and thereby elevated the urgency of addressing legal issues pertaining to their privacy.

II. WHAT ARE THE PRIVACY CHALLENGES IN WIRELESS M2M?

Before we explore how wireless M2M systems should be regulated for privacy, if they should be regulated at all, it is important first to understand what exactly the privacy challenges are. Appreciation of the breadth and complexity of the privacy challenges is useful to shape the mechanisms of regulation, where trivial privacy issues may not warrant expenditure of much legislative, judicial, or regulatory agency resources.

1. Privacy challenges in wireless machine-to-machine systems greater than the sum of the challenges encountered in single-machine systems and ordinary wirelessly-connected devices.

To understand the privacy challenges inherent in wireless machine-to-machine (M2M) systems we first recognize that these systems can be thought of simply as extensions to single-machine systems, for example, single internet-connected devices. When the interconnected machines are disassociated from each other the standalone machine is itself vulnerable to privacy intrusion. What complicates privacy further is that there could potentially be hundreds or thousands of machines communicating with each

[10] FCC, FDA unveil partnership to promote wireless medical technology. Sara Jerome, 07/26/10. http://www.californiahealthline.org. Retrieved 2013-03-20.

[11] ET Docket No. 09-36. The 413-457 MHz band is suited for propagation inside the human body allowing for medical micropower networks aimed at improving lives of those who suffer from spinal cord injuries, traumatic brain injuries, strokes, and various neuromusculoskeletal disorders.

[12] ET Docket No. 11-123. The Office of Engineering and Technology (OET) granted the request of Second Sight Medical Products, Inc. (Second Sight) for waiver of Section 15.209(a) of the Commission’s rules to allow it to obtain FCC certification for and market its Argus IITM Retinal Prosthesis System (Argus II). System operates at a transmit frequency of 3.156 MHz with carrier bandwidth of 13 kHz, with external emissions not to exceed 119 µV/m at measurement distance of 30 meters.

other, for example, intelligent sensor nodes, and each of these could be a source of privacy intrusion. These systems might also be communicating in an ad hoc manner without a centralized server device which would ordinarily coordinate privacy for the entire system.

Furthermore, because these machines wirelessly communicate with each other, we have the privacy challenges associated with ordinary wirelessly-connected devices such as WiFi-connected gadgets. One of the key challenges with wireless security is that a "trespass" often does not require physical access to the machine and is thus more difficult to detect. Additionally, because the communication happens via invisible electromagnetic radiation, it is not immediately apparent to most people that communications link might be a source of vulnerability; there is no constant reminder that the system owner has left "the door wide open."

2. Privacy and security tradeoff with other system features such as cost, safety, and utility.

For machine-to-machine systems to make economic sense the individual nodes often have to be low cost because there are potentially many of them 'talking' to each other. They also often have to be low power, which not only affects operating costs, but also allows them to be battery operated and portable, but without the added inconvenience of frequent battery replacements. Some devices such as implantable medical devices also need to be small in size. An equally important consideration is ease of use which directly determines consumer satisfaction and hence consumer demand. Inclusion of security features needed to ensure privacy often is in conflict with provision of these other features.[13] Inclusion of security features leads to additional costs in design, manufacturing, and security IP licensing; larger sized devices to accommodate circuitry and memory needed for security; higher power devices to run extra security-related operations; and less simple-to-use systems because such security systems often require user input such as passwords.

3. Even where a device manufacturer considers privacy and security, lack of industry standards means privacy may be lost when a system 'talks' to another manufacturer's system.

By combining different devices we can create complex machine-to-machine systems but in so doing the strength of the privacy of the overall system is dependent on the vulnerability of its weakest link. Because there are no industry standards on M2M security, privacy features available at one level of the system may not exist at another level thus defeating the privacy of the entire system. For example, devices from one manufacturer may not understand the encryption or security protocol used by a device from another manufacturer.

4. The situs of the machine-to-machine system may not be quite as easy to ascertain.

Machine-to-machine systems may include system constituents located in different jurisdictions. For example, they may retain data storage and data crunching in one jurisdiction, and the physical machines in another jurisdiction. This makes it difficult to determine exactly what jurisdiction may exert effective

[13] See, e.g., Daniel Halperin, et. al., Security and Privacy for Implantable Medical Devices, IEEE Pervasive Computing article, Vol. 7, No. 1, Jan. 2008. Highlights some of the challenges to implementing security in M2M devices.

control on the system. This is further complicated by systems that are themselves mobile or nomadic such as mobile-ad-hoc networks (MANET's). The result is that, even where the system privacy may be sufficient for one jurisdiction, it may fall short when the M2M system enters a more stringent jurisdiction. Worse yet, constituent elements of the system may be outside the territorial reach of the United States or the individual State, while the party that might be subject to personal jurisdiction in the forum may not be vicariously liable for actions of these extra-territorial constituents.[14]

III. WHY SHOULD WE REGULATE WIRELESS M2M PRIVACY?

While regulation of wireless machine-to-machine systems may be seen as an unnecessary bureaucratic hurdle that some may argue will slow the pace of M2M system adoption, there are compelling reasons why regulation might not be such a bad thing.

1. We should regulate wireless m2m privacy because m2m systems do not lend themselves to opt-in/opt-out private contractual schemes.

By their very definition, machine-to-machine systems lack a human interface through which the system user could read and agree to privacy policies that govern the system. Even if this were possible, it would be difficult to provide for an intelligible contract to govern the complex machine-to-machine interactions each of which might be collecting different information or collecting the same information but using it in different ways. True a user could agree to privacy terms through an independent system such as by accepting privacy policy available online prior to system activation. However, it would be cumbersome to handle policy changes that might later become necessary, such as when the autonomous intelligent system determines that it needs to collect new information, or use consented to information for a different purpose not already agreed to.

2. We should regulate wireless m2m privacy because there would otherwise be little incentive to implement privacy-conscious M2M systems or to ensure externalities associated with providing such systems are addressed.

As discussed in section II, part 2 supra, ensuring system privacy often conflicts with ensuring economical, efficient, reliable and easy-to-use systems. Regulations not only lower the transaction costs associated with ensuring that privacy controls are compatible across different parts of the system, it also changes the cost-benefit calculus of inaction. Unlike other types of communication systems, there is arguably less commercial risk associated with not providing for privacy in M2M systems, primarily because privacy breaches are more difficult to detect. For example, without pressure from European regulators, Google might have continued to deny the privacy breach in its Street View Project;[15] there

[14] See also Bartnicki v. Vopper, 532 U.S. 514 (2001) (defendant not liable for an intercept in violation of the Electronic Communications Privacy Act committed by a third party).

[15] NAL Forfeiture, DA 12-592, April 13, 2012.

was little incentive for individual action because there unlikely was much individual compensable damages. Furthermore, standardization and global harmonization is much easier under a regulatory framework. Standardization would eliminate one of the barriers to privacy in M2M systems identified above because now different parts of the system could 'talk' to each other 'in one language.' Global harmonization would also address the challenges associated with mobile and nomadic cross-jurisdictional systems.

3. **We should regulate wireless m2m privacy because growing M2M system complexity will make it much harder for individuals to police the systems or even discover any potential privacy intrusions.**

As M2M systems become more pervasive and ubiquitous, more and more people will increasingly rely on these systems for increasingly critical functions. Devices will also become more complex with continued advancement in technology. As a result, common day-to-day non-technical users of such systems will find it increasingly harder to police the systems to prevent privacy intrusions or even to understand when or how available privacy control mechanisms have been breached. For example, in the Google Street View privacy intrusion[16] discussed in section III, part 6 infra, the "culprit" was a software engineer whose code to capture "public" information about Wi-Fi networks inadvertently collected private data. Because of the complicated interrelation between the hardware and software collection element of the system, it would have been very difficult for a member of Google's legal team to "audit" the software code to determine that it did not collect private data. It was also difficult for individual affected citizens to detect that an intrusion had taken place, let alone have an incentive or wherewithal to complain about it.

Equipment manufacturers and Standard's bodies are more concerned with security. While security is intertwined with privacy[17] and may be viewed as two sides of the same coin, security in wireless m2m systems has traditionally not been a major concern because devices were not as intricately interconnected as they are today.

4. **We should regulate wireless m2m privacy because the privacy of data in certain M2M systems is just too sensitive not to regulate.**

It is not hard to imagine just how grave a privacy intrusion would be on, for example, the retinal prosthetic device discussed in section I. Imagine for a minute if someone were able to gain access to the

[16] Where Google's WiFi data collection initiative as part of the Street View Project was to capture information about Wi-Fi networks for location-based services (LBS) but the Company inadvertently collected "payload" data including e-mail and text messages, passwords, Internet usage history, and other highly sensitive personal information. See FCC NAL Forfeiture, DA 12-592, April 13, 2012.

[17] See, e.g., Daniel Halperin, et. al., Security and Privacy for Implantable Medical Devices, IEEE Pervasive Computing article, Vol. 7, No. 1, Jan. 2008.

video images transmitted between the glasses and the video processing unit. In effect everything that the glasses-wearer had viewed would be retrievable.

Some category of information might conceivably be deemed too critical that they should completely be out of reach to autonomous M2M systems. For example, location information of high-profile VIPs or individuals under witness protection programs should not be made available to certain types of M2M systems.

5. **We should regulate wireless m2m privacy because privacy regulation may have a positive effect on the growth of wireless M2M systems.**

Paternalistic regulation would instill confidence in consumers encouraging adoption of M2M systems. For example, doctors and healthcare funders list privacy and security concerns as barriers to greater use of mobile health systems (mHealth)[18] so the reassurance that the systems are required to meet some minimum threshold or privacy control might be sufficient to overcome this barrier.

While United States laws and regulation could not control wireless m2m privacy outside its jurisdiction, international harmonization would very likely be furthered indirectly. Because of the relative dominance of the United States on the International stage, other governments, especially those with considerably less resources to expend on researching the right balance of regulation, might follow the lead of the United States. Furthermore, because of the size and importance of the U.S. consumer market, the requirement that equipment manufacturers and service providers abide by the regulations in the U.S. would likely create *de facto* standards of privacy and security features that would be bundled in the wireless m2m systems sold in other countries.

6. **We should regulate wireless m2m privacy because we already have some real-life examples of exactly what could go wrong if privacy in wireless m2m systems was left unregulated.**

In 2012, Google Inc. was subject to forfeiture for noncompliance with FCC information and document requests in investigation regarding collection of data from Wi-Fi networks by its Street View project.[19] The purpose of Google's WiFi data collection initiative was to capture information about Wi-Fi networks for location-based services (LBS) but the Company inadvertently collected "payload" data including e-mail and text messages, passwords, Internet usage history, and other highly sensitive personal information.

What was equally noteworthy was Google's argument in its defense. Google claimed that the Wiretap Act did not apply. It noted that the Wiretap Act provides that "[i]t shall not be unlawful under

[18] Evaluating mHealth Adoption Barriers: Privacy and Regulation. http://mhealthregulatorycoalition.org/wp-content/uploads/2013/01/VodafoneGlobalEnterprise-mHealth-Insights-Guide-Evaluating-mHealth-Adoption-Privacy-and-Regulation.pdf. Retrieved 2013-05-16.

[19] NAL Forfeiture, DA 12-592, April 13, 2012.

this chapter or chapter 121[20] of this title for any person . . . to intercept or access an electronic communication made through an *electronic communication system* that is configured so that such electronic communication is *readily accessible to the general public*."[21] (emphasis added). Google then asserted that "electronic communications system" covered Wi-Fi communications and networks, and "readily accessible to the general public" was already defined in the Wiretap Act for radio communication, as communication that was not scrambled or encrypted.[22] Google thus claimed that the "readily accessible" exception to the Wiretap Act applied to the entirety of section 705(a) of the Communications Act[23] by virtue of section 705(a)'s introductory proviso.[24] Unfortunately we are unable to determine how much merit such an argument would have with the FCC or in a district court because the FCC dropped enforcement action under section 705(a) of the Communications Act due in part to lack of clear precedent in applying this section to the Wi-Fi communications at issue in this case.[25]

7. We should regulate wireless m2m privacy because other countries are already doing it and we would not want to be at a competitive disadvantage.

The European Union appears to be ahead of the United States in regulatory efforts in regulating machine-to-machine systems, dubbed "Internet of Things" (IoT).[26] The European Commission aims to protect individual rights from all the data that M2M systems collect as well as "unleash the [promised] potential economic and societal benefits."[27] The European Commission (EC) wants to know what framework is needed to unleash the potential economic and societal benefits of the systems, whilst ensuring an adequate level of control of the devices gathering, processing and storing information. The information concerned includes users' behavioral patterns, location and preferences. The EC recognizes the importance of consultation and thus sought public comment on "privacy, safety, security of critical supported infrastructure, ethics, interoperability, governance, and standards."

[20] 18 U.S.C. §§ 2701-2712. Stored Wire and Electronics Communications and Transactional Records Access.

[21] 18 U.S.C. § 2511(2)(g)(i).

[22] 18 U.S.C. § 2510(16)(A)

[23] 47 U.S.C. § 605(a). Interception and Divulgence of Radio Communications.

[24] The first sentence of Section 705(a) of the Communications Act prohibits certain conduct "[e]xcept as authorized by chapter 119, title 18." "Chapter 119, title 18" is a reference to the Wiretap Act, which governs, among other things, the interception of electronic communications. NAL Forfeiture, DA 12-592, April 13, 2012 at 3.

[25] But also because the engineer who developed the software code Google used to collect the payload data exercised his Fifth Amendment privilege against self-incrimination and declined to testify.

[26] Internet of Things – An Action Plan for Europe. Brussels, 18.6.2009 COM(2009) 278 final. Communication from the European Commission (EC) to the European Parliament et al. providing policy reason for EC's involvement.

[27] Id.

The reason the United States should take action as well is not merely as a bandwagon. Because of benefits arising out of economies of scale, original equipment manufacturers (OEMs) and service providers will often prefer to make a one-size-fits-all system that may be sold and deployed in different markets. Unless the United States takes action, it would be stuck with de facto privacy schemes that may not reflect the peculiarities of its citizenry. If it does not take the lead on regulation, it may find that M2M systems that its citizens come to rely on may be subjected to increasingly onerous international regulation while international systems obtain a free-ride for system components located within the U.S. In fact this might lead to instances where the United States may be used as a proxy to circumvent regulations in other countries by providing a “friendly” jurisdiction to park key M2M system components. Furthermore, coming late into the game will deprive the United States of a seat at the table in determining what the regulatory framework ought to be, leading to costly catch-up by U.S. equipment vendors and service providers.[28]

8. We should regulate wireless m2m privacy so as to provide clarity as to whether many of the existing statutes and regulations that appear to somewhat be on point do in fact apply.

Several statutes appear to address different aspects of privacy in wireless m2m systems in one way or another.

Section 705(a) of the Communications Act[29] deals with interception of electronic communications. This could govern the wireless communication from m2m sensors to base stations and bars the interception, divulging and use of that communication. However, if the wireless communication is unsecured one could make the same argument that Google made in its inadvertent collection of private information in WiFi networks that the communication is “readily accessible to the general public.”

Title I of the **Electronic Communications Privacy Act of 1986** (**ECPA),**[30] the **Wiretap Act,** protects electronic communications while in transit. This would govern the communication between local m2m nodes and remote nodes or remote controllers. It sets down requirements for search warrants that are more stringent than in other settings. Title II of the ECPA, the **Stored Communications Act** (SCA), which protects communications held in electronic storage, would govern the information collected by the wireless m2m systems. For example, the medical information collected by Implantable Medical Devices or status and error logs for systems that do not typically collect information. The SCA’s protections are weaker than those of Title I, however, and do not impose heightened standards for warrants. Title III

[28] Similar perhaps to what happened when the United States increasingly used CDMA cellular systems while the rest of the world used GSM systems. Because there was a large market for GSM devices, U.S. consumers were paying more for cellular communication (both for the handsets and for the cellular infrastructure) than the rest of the world. As an example of playing catch-up, note that next generation 4G data systems have now converged to LTE (Long Term Evolution) which offered a more natural and less costly transition from GSM-based networks.

[29] 47 U.S.C. § 605(a). Interception and Divulgence of Radio Communications.

[30] 18 U.S.C. §§ 2510-2522.

prohibits the use of **pen register and/or trap and trace devices** to record dialing, routing, addressing, and signaling information used in the process of transmitting electronic communications without a court order.[31] While Title III, trap and trace prohibitions are the least restrictive, information on when and with whom a wireless m2m system is communicating with, without revealing the contents of the communication, can reveal a great deal of information. For example, communication from one's residence to a known Medtronic server might suggest use of the implantable defibrillator discussed in section I.[32]

A.R.S. 13-3005 makes it a felony to intercept electronics communications.[33] California goes further and declares in its Constitution that privacy is an inalienable right.[34] CA SB 1386 expands on privacy law and guarantees that if a company exposes a Californian's sensitive information this exposure must be reported to the citizen.[35]

Case law establishing the "third party disclosure" doctrine makes it relatively easy to trample on privacy interests in wireless m2m systems.[36] Some wireless m2m systems would necessarily require disclosure of information to third party systems to be functional, e.g., a vehicle-to-road system would necessarily reveal its location information in order to receive traffic or road condition updates.

IV. WHO SHOULD REGULATE WIRELESS M2M PRIVACY?

Having concluded in section III that it would perhaps be prudent to regulate privacy in Wireless M2M systems, the next logical question is exactly what entity should do the regulating. This section discusses what branch of the government should "regulate" this field.

[31] Need not show probable cause to obtain a court order; just need a statement that the pen register will uncover information relevant to a criminal investigation – a very lax standard. Furthermore, violations of the court order requirement will not trigger exclusion of evidence in the prosecutions case-in-chief.

[32] Raw data from the defibrillator transmitted from the patient's implants to the device manufacturer who then processes the data and forwards it to the patient's doctor.

[33] "[A] person is guilty of a class 5 felony who . . . [i]ntentionally intercepts a wire or electronic communication to which he is not a party, or aids, authorizes, employs, procures or permits another to so do, without the consent of either a sender or receiver thereof." A.R.S. 13-3005.

[34] "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and *privacy*." California Const. Article I, § 1. (emphasis added).

[35] California's "Shine the Light" law (CA Civil Code § 1798.83) outlines specific rules regarding how and when a business that deals with any California resident must disclose use of a customer's personal information and imposes civil damages for violation of the law.

[36] See, e.g., Smith v. Maryland, 442 U.S. 735, 744 (1979) ("a person has no legitimate expectation of privacy in information that he voluntarily turns over to a third party").

Because of the need to ensure national uniformity and indeed, if possible, global harmonization, wireless m2m privacy should be regulated by the national government rather than state government; the national government has power under the Commerce Clause to do so.

One significant power, among the numerous limited and enumerated powers granted to the Federal Government by the United States Constitution, is the power "[t]o regulate Commerce with foreign Nations, and among the several States."[37] The federal government's "Commerce Clause" power, when read together with the "Necessary and Proper"[38] Clause, grants the national government power to regulate privacy in wireless m2m systems. Even under United States v. Lopez's recent tightening of Congress's power under the Commerce Clause, limits not seen since the New Deal, regulation of privacy in wireless m2m systems would likely be easily justified. This is because these systems typically comprise *channels* of interstate commerce, and often may involve activities that have a *substantial effect* on interstate commerce to allow for federal regulation under Lopez.[39]

Unless the federal regulations in wireless m2m were impermissibly coercive as for example under New York v. United States,[40] or a State alleged that it was deprived of the right to participate in the national political process or that in was singled out in a way that left it politically isolated and powerless to control wireless m2m privacy regulation at a national level,[41] it would not likely be successful in any

[37] U.S.Const. art. I, § 8, Cl. 3.

[38] "The Congress shall have Power . . . [t]o make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof." U.S.Const. art. I, § 8, Cl. 18.

[39] United States v. Alfonso Lopez, 514 U.S. 549 (1995) held that Congress may regulate under the Commerce Clause (1) the channels of interstate; (2) the instrumentalities of interstate commerce, or persons or things in interstate commerce; and (3) activities that substantially affect or substantially relate to interstate commerce. Factors to determine whether legislation represents a valid effort to use the Commerce Clause power to regulate activities that substantially affect interstate commerce include (i) whether the activity is non-economic as opposed to economic; (ii) whether the item had moved in interstate commerce [jurisdictional element]; (iii) whether there had been Congressional findings of an economic link between the regulated item and effect; (iv) how attenuated the link is between the regulated activity and interstate commerce.

[40] New York v. United States, 505 U.S. 144 (1992) (the provision in the Low-Level Radioactive Waste Policy Amendments Act of 1985 requiring states to "take title" and assume liability for waste generated within their borders if they failed to comply, was held to be impermissibly coercive and a threat to state sovereignty, thereby violating the 10th Amendment and exceeded Congress's power under the Commerce Clause; the "take title" incentive was an attempt to "commandeer" the state governments by directly compelling them to participate in the federal regulatory program and such coercion counter to the federalist structure of government, in which a "core of state sovereignty" is enshrined in the 10th Amendment).

[41] See Garcia v. San Antonio Metropolitan Transit Authority, 469 U.S. 528 (1985) (the limits on Congress's power are structural, not substantive; states must find their protection from congressional regulation through the national political process, not through judicially defined spheres of unregulable state activity).

judicial federalism-based challenges to federal regulation of wireless m2m systems. It is also unlikely that States would want to take up such an expensive and complex task as regulating wireless m2m privacy without the benefit of federal resources.

Because of the highly technical aspect of wireless M2M systems, a federal regulatory agency is better suited to regulate this field as opposed to the federal legislative or judicial branches.

The adjunct theory posits that when there are highly advanced facts, it is usually typical for the courts and legislatures to delegate to another entity or adjuncts to adjudicate the facts – usually called special masters[42]. In fact, some regulatory agencies possess quasi-legislative and quasi-judicial power and such a regulatory agency would seem to provide greater advantages at regulating wireless M2M as compared to purely legislative regulation or purely judicial regulation.

There are some notable disadvantages related to agency regulation of wireless M2M. Courts may be more neutral because they could not be threatened by Congressional interference through appropriations and oversight. Additionally, judges, particularly federal judges, are arguably more independent than Administrative Law Judges (ALJ's) because they are guaranteed lifetime tenure under Article III, §1 of the U.S. Constitution and because they must be appointed in accordance with the Appointments Clause in Art. II, §2, cl. 2[43]. Furthermore, there will likely always be partisan interference by the President, and, as the public choice theory suggests, agency personnel may desire to maintain their job tenure and act such that the agency is not stripped of power. However, many of these deficiencies may be overcome by relegating the regulation of wireless M2M privacy to an independent regulatory agency[44].

An executive-branch agency may also adjudicate instances of privacy intrusions in wireless M2M systems in addition to creating rules regulating privacy in wireless M2M.

Public rights, which arise between the government and others, could be conclusively determined by Executive and Legislative Branches of government and hence the danger on encroaching on traditional Article III judicial power is less than when private rights are administratively adjudicated. Private rights involve liability of one individual to another. Schor's[45] adjudicatory delegation test establishes if the

[42] This is the reason why agency findings of fact rarely pose delegation problems and Article III courts are very deferential to agency finding of fact by applying the substantial evidence standard of review – where reviewing court needs just more than a mere scintilla of evidence, or such relevant evidence as a reasonable mind might accept to support a conclusion. See, e.g., Universal Camera Corp. v. NLRB, 340 U.S. 474 (1951).

[43] Where they are nominated by the President and confirmed by the U.S. Senate.

[44] An independent regulatory agency or independent regulatory commission, like the Federal Communication Commission or the Federal Trade Commission, is not headed by one person but rather by commissioners with fixed and staggered terms that don't coincide with the President's term. The commissioners are bipartisan, requiring no more than a simple majority from any single party and are removable only for cause unlike heads of executive agencies who serve at the President's pleasure.

[45] Commodity Futures Trading Commission v. Schor, 478 U.S. 833 (1986).

agency can adjudicate traditional Article III claims arising out of privacy intrusions in wireless M2M systems. For example, whether an Administrative Law Judge (ALJ)[46] may adjudicate tort claims brought by the individual whose M2M system has been breached or contract claims against network or service providers who violate their privacy policy.

In Schor, an Administrative Law Judge (ALJ) in the Commodity Futures Trading Commission (CFTC) proceeding adjudicated a state law contract claim.[47] The court held that Congress could constitutionally grant to an agency the power to adjudicate ordinary state law contract claims between two individuals.[48] The court reasoned that the question to ask is whether the delegation impairs either (1) an *individual interest* in having a claim adjudicated by an impartial Article III judge, or (2) the *structural interest* in having an independent judicial branch decide matters that have traditionally fallen with the core of Article III courts. [49]

The legislative necessity in delegating the very complex area of wireless machine-to-machine systems, and the broad availability of judicial review of agency adjudication guaranteed by § 702 of the Administrative Procedure Act (APA)[50], means that the agency would be constitutionally authorized to adjudicate matters arising from privacy intrusion in wireless M2M systems. The agency would thus be in a unique position to develop rules and policies related to this nascent field by either using adjudication or rulemaking. By resorting to Notice-and-Comment Rulemaking (NCRM), the agency may assure that the rules it formulates would receive great deference from the courts, known as Chevron deference.[51] Chevron requires a two-step process for judicial review of agency interpretation of law. First the court must decide if the statute is clear; if Congress has directly decided the precise question at issue.[52] If the statute is ambiguous, the court then asks whether the agency's interpretation is permissible or reasonable.[53] It will be likely that agency enabling statutes will often be ambiguous as regards such a

[46] Administrative Law Judges (ALJ's) may arguable not have the same level of judicial independence as for example federal judges. Federal judges have lifetime tenure guaranteed by Article III, §1 of the U.S. Constitution, and must be appointed in accordance with the Appointments Clause in Art. II, §2, cl. 2. ALJ's on the other hand are not "officers" under the Constitution, but rather agency employees. See Landry v. FDIC, 204 F.3d 1125 (2000).

[47] Id. at 3252.

[48] Id. at 3260.

[49] Id. at 3265.

[50] 5 U.S.C. § 702 grants broad standing to any "person suffering legal wrong or adversely affected or aggrieved by agency action within the meaning of a relevant statute."

[51] See Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc., 467 U.S. 837 (1984).

[52] Id.

[53] Id.

novel field as privacy in wireless machine-to-machine systems. It will also be equally likely that the agency interpretation will often be reasonable particularly given the agency's expertise in this area and especially if the agency conducts a cost-benefit-analysis ahead of rulemaking.[54]

Having the same agency that made the rules on wireless m2m privacy adjudicate violations of the rules eliminates many of the challenges encountered when courts try to interpret the legislature's intent. The very reason that justifies agency rulemaking, i.e., agency expertise in the area regulated, also justifies agency adjudication of violations of the rules. Although it may be argued that this poses a risk that the agency might enforce rules commonly understood by the agency but not otherwise clearly stated such as to give sufficient notice to the public, this risk is not very significant considering the possibility of obtaining advisory or clarifying opinions from the agency – something that m2m system owners could not do with the courts because of the statutory and constitutional "case or controversy" requirement.[55] In fact, such advisory opinions are awarded persuasive deference by the judicial branch in later article III adjudications.[56]

Having executive-branch agencies regulate wireless M2M privacy, together with judicial deference to agency actions, ensures that privacy in wireless M2M systems can be dealt with promptly and uniformly across the United States.

Judicial deference limits the occurrence of federal circuit splits which would otherwise lead to the disparateness and balkanization on wireless M2M regulations. Uniformity is particularly important given the discussion in section II addressing the privacy challenges introduced by the inability to easily identify the situs of the machine-to-machine system – different components located in different jurisdictions.

Furthermore, an executive-branch agency can respond faster to changes in the wireless M2M than can the legislature or the judiciary. Article III of the U.S. Constitution limits the jurisdiction of the federal courts on what cases or controversies it may hear. Such justiciability concerns require that parties not be seeking an advisory opinion, have an actual controversy, and that they are not seeking judgment upon a political question. On the other hand many agencies allow for advisory opinions. These opinions regarded as having the force of law and are afforded judicial deference under Mead,[57] if made by a high level officer in the agency, if meant to establish a binding precedent, if opinion later relied upon for a

[54] See Entergy v. Riverkeeper, 129 S.Ct. 1498 (2009). See also EO 12866 – Regulatory Impact Analysis (RIA) – which makes Cost-Benefit Analysis (CBA) a component of every rulemaking.

[55] See U.S.Const. art. III, § 2, cl. 1; 28 U.S.C. § 1331, "The district courts shall have original jurisdiction of all civil actions *arising under* the Constitution, laws, or treaties of the United States," (emphasis added).

[56] See Skidmore v. Swift & Co., 323 U.S. 134 (1944) (adopting an approach to agency interpretation under which the agency's views are not "binding" but have merely persuasive authority, whose weight depends on the circumstances; FLSA Administrator's suggestion on what part of idle time at a fire hall would be considered to be hours worked held to be persuasive).

[57] United States v. Mead Corp., 533 U.S. 218 (2001)

long duration and is otherwise efficient and has no practical concerns. Agencies are also able to address generalized grievances which are barred by the prudential requirements of Article III standing. This ability to rapidly respond to changes in wireless M2M systems would ensure that privacy provisions do not significantly lag regulation.

Because reasonableness of an expectation of privacy is determined by existing laws, regulations and practices, agency rulemaking relating to privacy in wireless M2M prevents the diminution of protected privacy interests.

Katz v. United States,[58] establishes when government conduct constitutes a 4th Amendment search. Under Katz, to qualify as a 4th Amendment search, the government conduct (1) must offend the citizen's subjective manifestation of privacy, and (2) the privacy interest invaded must be one that society is prepared to accept as "reasonable" or legitimate.[59] Although Katz, involves government conduct, it provides a useful definition of privacy. But what exactly are the privacy interests in wireless M2M systems that society would be prepared to accept as reasonable? One advantage of having an administrative agency regulate privacy in M2M systems is that, by resorting to notice-and-comment rulemaking[60], citizens get to answer this question through public comment[61] versus having judges decide what "society is willing to accept as reasonable." Citizen participation ensures that resulting regulations do not cede privacy ground too rapidly, particularly in novel M2M systems. The regulations legitimize the privacy interests they protect and make unreasonable any subjective manifestation of privacy that they do not recognize. For example, if regulation was passed that required video captured by vehicle visual anti-collision sensors be made available to a publicly accessible database, as more vehicles with such systems came into the market, the pervasive video surveillance in public streets would eventually lower the public's expectation of privacy in this area.

As an illustration of how this diminution in protected privacy interest might play out without citizen participation consider two relatively recent Supreme Court cases. In Florida v. Riley,[62] the police aerially circled greenhouse with helicopter and with naked eye could see what looked like a marijuana grow operation.[63] The helicopter was flying at 400 feet, well within the navigable airspace, and there was no intimation that it interfered with resident's normal use of the greenhouse or of other parts of the

[58] Katz v. United States, 389 U.S. 347 (1967).

[59] Id.

[60] Preferred approach to rulemaking so that agency can benefit from Chevron deference.

[61] Under United States v. Nova Scotia Food Products Corp., 568 F.2d 240 (2d Cir. 1977), citizens may judicially challenge the agency rule if the agency did not genuinely consider vital questions of cogent materiality sent in by citizens through the public comment process.

[62] Florida v. Riley, 488 U.S. 445 (1989).

[63] Id.

curtilage.[64] The plurality opinion held that the officer's observation, with his naked eye, of interior of partially covered greenhouse in residential backyard from vantage point of helicopter circling 400ft above did not constitute a "search" for which a warrant was required.[65] Justice O'Conner's concurring opinion held that, so long as it was in the public airways at an altitude at which the *public travel with sufficient regularity*, defendant's expectation of privacy from aerial observation was not one that society was prepared to recognize as reasonable.[66] The Court affirmed California v. Ciraolo**[67]** which involved aerial surveillance of yet another marijuana grow operation but this time at 1000 feet with a fixed wing aircraft. The Court reasoned that as long as any member of the public could have been lawfully flying at that altitude and could have observed what the police officer did observe, there was no 4th Amendment search.[68]

Likewise in Kyllo v. United States,[69] a thermal-imaging device was aimed at a private home from a public street to detect relative amounts of heat within the home which was indicative of a marijuana grow operation.[70] The Court held that obtaining (1) by sense-enhancing technology (2) any information regarding the interior of the home (3) that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, constitutes a search (4) at least where (as here) *the technology in question was not in general public use*.[71] The court reasoned that because the sophisticated surveillance equipment was not commonly available to the public, the warrantless search was presumptively unreasonable and hence unconstitutional.[72]

Both Riley and Kyllo left open the idea that those technologies that were seen to invade a reasonable expectation of privacy only did so because there were not in pervasive use. Now consider that the Federal Aviation Administration (FAA) recently predicted about 7,500 civilian drones will be in use within five years after the agency grants them greater access to U.S. skies.[73] According to Riley, once

[64] Id.

[65] Id.

[66] Id.

[67] California v. Ciraolo, 476 U.S. 207 (1986).

[68] Florida v. Riley, 488 U.S. 445 (1989).

[69] Kyllo v. United States, 533 U.S. 27 (2001).

[70] Id.

[71] Id.

[72] Id.

[73] Congress directed FAA to provide drones with widespread access to domestic airspace by 2015. See http://www.businessweek.com/ap/2013-03-20/drones-will-require-new-privacy-laws-senate-told. Joan Lowy, March 20, 2013. Retrieved 2013-05-16.

such drones become pervasive and are capable of video surveillance then perhaps homeowners would not have a reasonable expectation of privacy in their curtilage even against over-flights at 100 feet. However, if the public, through notice-and-comment rulemaking, prevent this and other potential privacy shrinking regulation in wireless m2m systems, we will not end up with a status quo where little to no privacy exists in such systems.

To determine what independent regulatory agency would be apt to the task we need to examine agency enabling statutes and determine if we can discern an intelligible principle that would guide the executive branch in wireless M2M privacy regulation.

In J.W. Hampton, Jr., & Co.,[74] the Supreme Court held that Congressional delegation of legislative authority is an implied power of Congress that is constitutional so long as Congress provides an "intelligible principle" to guide the executive branch. In fact, ever since the mid 1930's, following the expansion of executive branch agencies by President Roosevelt to support New Deal initiatives, the Supreme Court has found unconstitutional delegation in very rare instances such as in Panama Refining [Hot Oil][75] and Schechter Poultry [Sick Chicken][76]. Thus, if we assume that there will be no additional enabling statutes passed by Congress, or no amendments thereto, we would need to examine the existing agency enabling statutes and determine which one can justify an intelligible principle vis-à-vis wireless M2M privacy regulation.

No single regulatory agency would be apt to the task of broadly regulating wireless m2m systems; the ideal regulatory scheme requires cooperation between multiple agencies but under a uniform pre-established regulatory framework.

As is evident from the examples introduced in section I, wireless m2m systems occupy different vertical markets and serve varied purposes. Depending on what exactly the m2m system does, one agency may be better at regulating privacy than another. This should not pose much difficulty because it is in fact the regulatory scheme used in many existing technologies. For example, medical equipment typically requires approval by the Food and Drug Administration (FDA) for medical use, and the Federal Communication Commission (FCC) for at least Part 15 approval[77] regulating spurious emissions[78].

[74] J.W. Hampton, Jr., & Co. v. United States, 276 U.S. 394 (1928).

[75] Panama Refining Co. v. Ryan, 293 U.S. 388 (1935).

[76] A.L.A. Schechter Poultry Corp. v. United States, 295 U.S. 495 (1935).

[77] 47 C.F.R. 15.5 requires that devices may not cause harmful interference and must accept interference from other sources.

[78] More FCC approvals required if actually an intentional radiator.

To prevent haphazard regulation and externalities therefrom, it is important to have a common regulatory framework that all agencies may use as a basis for their privacy regulation of wireless m2m systems. In fact, having a common regulatory scheme makes it difficult to attack the regulations in an Article III court because courts are reluctant to strike down agency action that arises under a broad public regulatory scheme.[79]

The FCC is a natural choice because of the "wireless" in "wireless m2m privacy." To "maintain the control of the United States over all the channels of radio transmission," 47 U.S.C. §301, Congress allows the FCC to grant licenses to use radio spectrum insofar as doing so would serve the "public convenience, interest, or necessity," 47 U.S.C. §307(a). The authority granted by Congress was intentionally designed to accommodate "the dynamic aspects" of communications technology,[80] while allows it to easily adapt to the novel issues facing wireless m2m systems. The FCC has already allocated unlicensed spectrum in the 900MHz and 2.4GHz that is already in use with many wireless m2m systems. The FCC is also specifically mandated by Congress to remove barriers to infrastructure investment and to "encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans."[81]

Other agencies such as the Federal Trade Commission (FTC) (Consumer Protection), Department of Transportation (DOT) (vehicle telematics systems particularly vehicle-to-road systems), Department of Energy (DOE) (home automation systems and smart grid regulation) may also participate in regulating privacy in pertinent wireless m2m systems.

V. JUST HOW SHOULD WE REGULATE WIRELESS M2M PRIVACY?

In section I we discussed why we should pay particular attention to wireless m2m systems and in section III why we should regulate privacy in wireless m2m systems at all. Section IV concluded that a federal administrative agency would have the authority, capability, and advantage in regulating privacy in wireless m2m system. This section proposes various ways in which such an agency or agencies would go about doing it.

A. Regulation of privacy in wireless m2m systems might be based on <u>what</u> data is collected or transmitted by the system.

The content of the data in wireless m2m systems is perhaps one of the most important determinants on how the system should be regulated. For example, consider the retinal prosthesis device illustrated in section I where a visually impaired person wears eyeglasses housing a miniature

[79] See, e.g., Thomas v. Union Carbide Agricultural Products Co., 473 U.S. 568 (1985).

[80] FCC v. Pottsville Broadcasting Co., 309 U.S. 134, 138 (1940).

[81] Section 706(a) of Telecommunications Act of 1996, 47 U.S.C. § 1302(a).

video camera that captures images which are processed by an external unit and wirelessly transmitted back to a retinal prosthetic implant. Suppose that the video processing unit, in addition to converting the captured image into signals that the prosthetic can understand also stores the captured video images. Should commercial entities be liberally allowed access to parse this data to determine say where the visually impaired person has been in order to customize targeted ads for him? If the video is voluntarily uploaded to participating merchants or to the equipment manufacturer or his agents for diagnostics purposes, should the government be allowed warrantless access to it? Should such historical data even be accessible with a search warrant? The case against such data being protected by the 5th Amendment's Privilege Against Self-Incrimination is even better than for diaries because here not only was the video image capture not compelled by the government, it cannot be fairly said to be testimonial.[82]

But what of self-learning systems that need to collect new data that was not previously anticipated or consented to? For example, in the coffee maker example above, a repair company may suspect a correlation between failure of a certain electronic component and ambient temperature and now wish to collect ambient temperature data – assuming the system has the capability to do so. In this scenario, "why" the data is collected is an equally relevant consideration in deciding how privacy should be regulated.

B. Regulation of privacy in wireless m2m systems might be based on why the data is collected or the system exists in the first place.

The same data may have different "value" depending on why it is collected by the wireless m2m system. Knowledge of why it is collected might itself require privacy protection just as much as what actually is collected. This might suggest that the level of mandated privacy controls would depend on what the m2m system was used for. For example, an Implantable Medical Device collecting ambient temperature data to calibrate or compare with collected body temperature might be regulated differently from a home automation sensor regulating HVAC thermostats, or a smart grid sensor programmed to collect the same data so as to anticipate and respond to heavier electricity demands.

The problem with this framework is that as m2m systems get more pervasive and standardized, it would be inefficient to have different systems collect the same data when a single central system could do so and share the data across different m2m systems. Having such a single-source of common data used across multiple m2m systems is problematic. By giving different systems access to the same data we increase the risk of a rogue system gaining access to the data or an already authenticated system using the data for an unauthorized purpose. Furthermore, if we are to regulate privacy based on the purpose, then the system requesting the data would need to report what it needs it for which adds complexity and may by so doing divulge private information.

[82] See, e.g., Schmerber v. California, 384 U.S. 757 (1966) (the 5th Amendment privilege protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence *of a testimonial or communicative nature*).

C. Regulation of privacy in wireless m2m systems might be based on who has actual or constructive access or control of the system itself or the data.

One notable distinction on accessibility of wireless m2m systems depends on whether the government is the entity seeking access or whether it is a private entity. The government has Fourth Amendment[83] restrictions, not possessed by private parties, which severely limits their warrantless access to wireless m2m systems.

The privacy regulatory framework may also depend on whether a commercial entity has access or control of the wireless m2m system, whether a private individual does, or whether the public at large has access. Whether a 3rd party commercial entity or person has access to the wireless m2m system is typically determined by contract. The complication with such contractual determinations is that for complex systems with many hierarchical layers it is not always clear what level of hierarchy is contractually accessible. Moreover, with dynamically reconfigurable and autonomous systems, different hierarchies may blend together giving the 3rd party access to previously unapproved data, or blocking them from previously approved data. Additionally, the 3rd party may allow its agents access to the system even when there is no clear contract privity. The need to protect consumers would thus be at odds with notions of freedom to contract.

For example, consider a coffee maker that interfaces to an alarm clock and also to the manufacturer for automatic downloads of firmware updates or uploads of diagnostic data for use in product improvement. Because the homeowner bought the coffee maker from an appliance store he has no contract privity with the manufacturer. Say the homeowner nevertheless allows the manufacturer access to his coffee maker, what happens when down the road the manufacturer outsources the firmware update development or diagnostics monitoring to another entity? Should that entity automatically be allowed access to the system without a specific contract with the homeowner?

Consider also the recent case of Medtronic's implantable defibrillator data access[84]. A patient was denied access to the data collected by his implanted device when he lost their his insurance. Under the Health Insurance Portability Accountability Act (HIPAA), patients have the right to access information held by doctors and hospitals. The problem here was that the raw data gathered by the implant was not held by the doctor or the hospital but by the device maker who provided a summary report to the doctor. Because of this, the raw data fell outside the scope of HIPAA's patient-access requirements. In addition, business agreements between the device maker (Medtronic) and doctors and hospitals restricted it to relaying information only to them and not to the patient. In this case, a better regulatory framework might have been to consider the doctor as having constructive access to the raw data thus bringing the data within the scope of HIPAA's privacy protections and patient access provisions.

[83] "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures shall not be violated, and no Warrants shall issue, but upon probably cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend IV.

[84] "Heart Gadgets Test Limits Of Privacy Laws on Health," page A1, The Wall Street Journal, November 29, 2012.

Publicly accessible data might be for example where the m2m system owner knowingly broadcasts data say to a social network, or agrees to let potential advertisers gain access to it possibly as a quid-pro-quo for some "free" service. In this case, the system owner would not retain a legally cognizable expectation of privacy to prevent the government access to that data just like the general public[85].

Finally, when a sovereign entity such as a State or an Indian Tribe has control of the wireless m2m system, federal regulation of privacy may run afoul of the entities sovereignty. While Congress can readily abrogate tribal sovereignty, the 11th Amendment bars any action against a state for violating privacy regulation in wireless m2m systems. Under Seminole Tribe,[86] Congress can only waive sovereign immunity using power granted after the 11th Amendment[87] and specifically applying to the state, i.e., 14th & 15th Amendments.[88] While Ex parte Young,[89] would allow State officials to be sued in their official capacity to enjoin breach of privacy in wireless m2m systems, the aggrieved individuals whose privacy was breached would likely be unable to collect monetary damages.

D. Regulation of privacy in wireless m2m systems might be based on where the system or the data is located.

The situs of the wireless m2m system or data determines if an administrative agency or a federal or state court would have jurisdiction to adjudicate any privacy intrusion. Because wireless m2m systems may have elements located in different geographic locations, it becomes difficult to determine precisely where the system "resides." For example, should jurisdiction be based on the situs of (1) the entity consuming the data; (2) the point of collection of the data, i.e., where the sensors are located; or (3) where the entity processing or aggregating the data resides?

If the system is deemed to reside outside the territorial limits of the United States then it is unambiguous that neither a federal or state court nor an administrative agency would have jurisdiction to regulate it. While a State court would likely lack subject matter jurisdiction because of either express preemption in federal statutes or field preemption arising out of pervasive federal regulation of wireless

[85] See, e.g., California v. Greenwood, 486 U.S. 35 (1988) (holding that what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection).

[86] Seminole Tribe of Florida v. Florida, 517 U.S. 44 (1996)

[87] But see Central Virginia Community College v. Katz (2006) (narrowing scope of Seminole Tribe by holding that the Bankruptcy Clause of Article I abrogated state sovereign immunity).

[88] For example, where it is necessary to enforce the rights of citizens guaranteed under the Fourteenth Amendment as per Fitzpatrick v. Bitzer, 427 U.S. 445 (1976).

[89] Ex parte Young, 209 U.S. 123 (1908).

m2m systems, it is still important to determine what State the system is deemed to reside as this is necessary to establish in personam jurisdiction under Fed.R.Civ.P. 4(k)(1)(A)[90].

For example, suppose a plaintiff sued to enjoin the autonomous collection of private data in a wireless m2m system located in Arizona but operated by an out-of-state entity. Under State of Arizona v. Western Union,[91] if those with interests in the property are subject to in personam jurisdiction in the forum state, a court in that state undoubtedly has jurisdiction consistent with the Due Process Clause to enter orders relating to the property.[92] However, when the plaintiff proceeds in rem, the solution as to whether the court has in rem jurisdiction over intangible property must be sought in the general principles governing jurisdiction over persons and property rather than in an attempt to assign a fictional situs to intangibles.[93] So while the district court in Arizona could order the seizure of the physical data collection sensors or nodes, it would lack personal jurisdiction over the out-of-state persons or entities responsible for the data collection unless they exhibited such minimum contacts with Arizona that subjecting them to Arizona's jurisdiction would not offend the traditional notions of fair play and substantial justice under International Shoe.[94]

Privacy regulation based on the situs of the wireless m2m system also poses other unique challenges. For example, because under Verdugo-Urquidez[95] the 4th Amendment does not apply to searches of non-citizens outside the United States, does this mean that the government could intercept, without a warrant or even probable cause, private data of U.S. citizens that is being stored or processed in a foreign country? Additionally, considering United States v. Jones'[96]return to trespass rules to supplement the Katz[97] test, does this mean that the government could legally obtain private data

[90] Under Fed.R.Civ.P. 4(k)(1)(A), a district court must first look at whether the defendant is subject to the jurisdiction of a court of general jurisdiction in the state where the district court is located, i.e., look at the State Long Arm Statute.

[91] State of Arizona v. Western Union, 208 P.3d 218 (Ariz. 2009) (en banc).

[92] Id. at 225.

[93] Id.

[94] International Shoe Co. v. Washington, 326 U.S. 310 (1945).

[95] United States v. Verdugo-Urquidez, 494 U.S. 259 (1990) (holding that the 4th Amendment's "the people" was intended to refer only to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered a part of that community and therefore the non-resident alien defendant was not protected by the 4th Amendment from warrantless searches of his residences in Mexico).

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

[97] Katz v. United States, 389 U.S. 347 (1967).

without a warrant, regardless of where the data collection point was located, provided they did not trespass to obtain it?

E. Regulation of privacy in wireless m2m systems might be based on when the data was collected.

Under Section 2703 of the Stored Communication Act (SCA),[98] if a communication has been in storage for more than 180 days or is held solely for the purpose of providing storage, the government can access it without a warrant by use of a subpoena or a "specific and articulable facts" court order – a "2703(d) order". Wireless m2m systems generate data that may be deemed as subject to the SCA and hence subject to this 180 day period after which the stored data may be considered stale with respect to 4th Amendment searches. Other data collected by wireless m2m systems might also have relevance based on when exactly it was collected. For example, systems that record sleep patterns of patients suffering from Sleep Apnea may be sought by a plaintiff or insurer post-accident in an attempt to prove that the defendant was sleep-deprived.

F. Regulation of privacy in wireless m2m systems might be based on how the system is organized or configured or how the data is formatted.

How the wireless m2m system is organized, i.e., the system topology, may be used as a framework to regulate privacy. For example, the m2m system may be "vertically stacked" such that an m2m system at one hierarchy level talks to another m2m system, which talks to another m2m system, etc., which eventually talks to the human-machine interface. In such a case, data collected from one level of the system may be viewed as separate and distinct from equivalent data collected from another level. The more removed the level is from the human interface, the less the risk that any potential privacy intrusion would be of consequence; it would be less likely that such low-level sub-systems would need much private information, and even if they did, it would be unlikely that the information would be in a format comprehensible to a human.

For example, consider a smart grid m2m system that is tied into a home automation m2m system. The smart grid system may collect ambient temperature in the home to anticipate energy demand, and the home automation system might use this information to automatically adjust HVAC settings. Elevated home temperature which is readily determinable from these systems, in addition to its intended use, may also be indicative of a marijuana grow operation or when the lady of the house is taking her daily sauna.[99] Now consider alternatively a home appliance m2m system that periodically transmits diagnostic data to an appliance repair service. Part of the diagnostic data transmitted might include the ambient temperature which the service repair shop may use to diagnose erratic appliance behavior. In this latter case, the same ambient temperature may not be as readily determinable because it would be embedded with other diagnostic data and possibly formatted in a proprietary manner.

[98] 18 U.S.C. §§ 2701–2712.

[99] See Kyllo v. United States, 533 U.S. 27 (2001).

Regulation of privacy in wireless m2m systems based on how the system is organized thus goes hand in hand with regulation based on the form of the data in the system. For example, some data can only be consumed by a machine and cannot be perceived by a human. This is particularly true where the wireless m2m system communicates through a proprietary protocol understood only by other components from the same manufacturer. The data might also be useless in its raw form, requiring post-processing or specialized skill to decipher it, a skill that might only be available to a regulated professional such as a physician.[100] Yet other times the data is useful or meaningful only after it is aggregated with data from other independent m2m systems or after it is collected over time to establish trends. In these cases, there is little that can be gained from access to a snapshot of such data.

VI. CONCLUSION

When machines talk to each other there are unique challenges to securing the privacy of the data flowing through such machine-to-machine systems. Section II considered some of these unique challenges to privacy, and Section III discussed the merits of regulating privacy in such systems. In Section IV we concluded that a federal administrative agency would have the authority, capability, and advantage in such regulation and in Section V we proposed different legal frameworks by which such an agency would go about regulating privacy. This includes considerations of what data was collected, why it was collected, how it was collected, when it was collected, who collected it, or where it was collected.

[100] See, e.g., Medtronic defibrillator raw data is transmitted from the patient's implants to the device manufacturer who then processes the data and forwards it to the patient's doctor.

*This paper contains **8820** words (inclusive of this line).*