AT&T Comments on Ofcom Consultation Document, *Promoting Investment and Innovation in the Internet of Things*

1 October 2014

AT&T is pleased to provide these comments on the Consultation Document, *Promoting Investment and Innovation in the Internet of Things*, issued by Ofcom on 23 July 2014 (the "Consultation").

AT&T, given its leadership in working with customers to develop machine-to-machine (M2M) solutions,[1] welcomes the opportunity to inform policies that will further promote the Internet of Things (IoT)[2] in the UK. Although the policy issues that Ofcom raises in the Consultation are relevant to the IoT's transformative potential, AT&T focuses its comments on a subset of priority topics: the use of numbering resources (Consultation, at 1.9.3), specifically, the need for extra-territorial use of numbering resources or the "Global SIM" model, and data management-related issues (*i.e.*, security, privacy, and analytics),[3] which are best served by collaborative self-regulatory efforts. AT&T also addresses themes Ofcom identifies for input, namely, IoT definition, applications and demand (Consultation, at 1.46); Numbering and addressing (Consultation, at 1.51) and Ofcom's role (Consultation, at 1.56).

1. The Internet of Things: Promising Economic and Societal Opportunities Supported by New Business Models

In the 1990s, the privatisation and commercialisation of the Internet led to the greatest advance in human communications ever experienced. In the nearly two decades that followed, the move from narrowband to broadband and fixed to mobile further enhanced the value and ubiquity of the Internet. We are now positioned for the next wave of the Internet—the "Internet of Things." The IoT encompasses M2M communications, typically wireless. AT&T defines M2M communications as a set of diverse and expanding networking and IT technologies, which connects the physical systems of the world such as power meters, vehicles, containers, pipelines, wind-farm turbines, vending machines, personal accessories—essentially, any electronic device that would benefit from two-way

[1] AT&T has a proven M2M success record, with 1,800 certified connected devices, more than 17 million endpoints in active service and industry analyst recognition for solution deployment experience and capability. For example, in a recent iteration of Current Analysis' Global M2M Service provider rankings, principal analyst Kitty Weldon wrote that "AT&T is positioned as a global leader in providing M2M services and has demonstrated excellent traction for its initiatives with customers" (*Current Analysis, "AT&T - Global M2M Services and Strategies Vendor Profile," September 2013).* Moreover, AT&T has relationships with other U.S. industry leaders such as Cisco, GE, IBM, and Intel.

[2] Following Ofcom's practice (Consultation, at 1.5), in these comments AT&T generally refers to M2M as a subset (*i.e.,* type of communications or connection) of the IoT.

[3] Security and resilience (Consultation, at 1.49); Data privacy (Consultation, at 1.50); and Data analysis and exploitation (Consultation, at 1.54).

communications. The IoT also includes a complex ecosystem of innovative players[4]—most notably connectivity providers (mobile and fixed network operators), hardware manufacturers (equipment manufacturers and device manufacturers), software/application service providers (telematics, data analytics, billing solutions, etc.), and system integrators—that are developing new services and capabilities for the benefit of consumers and to facilitate the emergence of the real-time, adaptive enterprise. Incredibly, the proliferation of IoT applications is having an impact to such a degree, that companies the world over are turning to technology not only to transform the way they do business, but to become leaders in their respective industries. Although at a nascent stage of development, these M2M communications have already demonstrated the potential to massively improve efficiency, productivity and social welfare in fields as diverse as education, healthcare, transportation, energy, security, agriculture, and many others.[5] Indeed, as Ofcom noted, this new connectivity "could change the way we lead our lives."[6]

Examples of IoT Applications

IoT solutions are particularly critical to Europe after the economic crisis and the subsequent introduction of austerity measures that influenced public investment, including public services. With pressure to reduce costs, the introduction of more efficient ways of delivering high quality and sustainable public services is increasingly important. Therefore smart technologies using M2M connectivity are being deployed. According to U.S. industrial Internet leader GE,[7] Europe is well-positioned to reap the gains from the IoT revolution, and is especially in need of doing so to restore growth and contribute to ongoing debt reduction. Many manufacturers in Europe are advancing IoT applications with investments in smart grids/meters,[8] smart cites,[9] and smart homes.[10] In the UK, the

[4] There are also new players entering the IoT ecosystem. For example, several companies announced plans to create a network exclusively for M2M communications. One French start-up plans to develop a low-cost, energy-efficient ultra-narrowband cellular network dedicated to the IoT, and it wants to deploy in 60 countries over the next five years. (*See* http://www.lightreading.com/services-apps/m2m/metal-machine-music-dedicated-m2m-networks-on-horizon/d/d-id/708656.) While such players may fall under a traditional moniker (*i.e.*, connectivity provider), their new networks may not fit neatly into traditional network concepts and regulatory frameworks. And as the industry grows, policymakers should expect and encourage further innovations that will propel the IoT ecosystem forward.

[5] According to the International M2M Council (IMC), IoT vertical markets include Healthcare (care provider, medical device manufacturer, health insurance); Logistics (asset tracking services, shipping); Energy/Utilities (electricity, water, waste; aggregator; meter manufacturer; pipeline/refinery management); Public Infrastructure (traffic control, facilities management, emergency services, security/defence); Building/Construction (energy management, security); Transportation (automotive, infotainment, hardware, services; fleet management, transportation insurance; mass transportation); Retail/Consumer (appliances/housewares, personal device manufacturer, signage, vending); and Industrial (manufacturing/fabrication, laboratory/pharmaceutical, agribusiness/farming). *See* http://www.im2mc.org/imcmarkets

[6] Consultation Document, at page 1.

[7] *See* http://www.genewscenter.com/imagelibrary/downloadmedia.ashx?MediaDetailsID=5901&SizeId=-1

[8] *See* http://ses.jrc.ec.europa.eu/smart-grids-observatory

[9] *See* http://ec.europa.eu/eip/smartcities/

Department of Energy and Climate Change (DECC), recognising the benefits of energy efficiency and consumer control, developed plans to roll out smart meters to most households from 2015 through 2020.[11]

Likewise, healthcare stands out as a sector that will be transformed more than any other by IoT technologies in the coming years, and the transformation is well under way.[12] IoT healthcare technologies have the potential to improve health outcomes, reduce health expenditures and facilitate the offering of care in more patient-friendly ways.[13] For instance, wireless, body-worn sensors will increasingly allow the healthcare industry to free patients from a "tethered" hospital stay, which in many cases restricts patient mobility. Similar technologies are migrating into homes, allowing the remote and continuous monitoring of patients' blood-pressure, respiration rate and a variety of other biometric information. This information typically flows across a short, unlicensed wireless link to a monitoring hub (*i.e.*, from a device to a router) in the patient's home, which then passes the information to the broadband network, routing it to the cloud where analytics continuously monitor a patient's status, notifying a healthcare provider of any anomalies. Other applications work with smart-phone apps. For example, fitness applications help individuals keep track of daily miles walked, calories burned, and monitor pulse and respiration rates at different intervals. More broadly, the pharmaceutical supply chain continues to evolve and will require greater IoT visibility of products being distributed around the world. The field of telehealth also holds the promise of extending the reach of healthcare practitioners into remote, underserved and high-risk areas.

Another major IoT application is the connected car. According to Pyramid Research, telematics is the fastest growing segment of the mobile M2M market and the firm predicts Europe will become the largest telematics market in 2016, overtaking the United States.[14] To facilitate the expected growth relative to connected car, early this year the European Commission announced the establishment of a basic set of standards to ensure that vehicles made by different manufacturers can communicate with each other. The standards are expected to accelerate the European car industry's development of the next generation cars.[15] The market impact promises to be significant, as Europe currently has more than

[10] According to a 2013 Berg Insight report forecast, by 2017 there will be 17.4 million installed smart home systems in Europe with annual revenues reaching $3.4 billion. *See* http://blogs.wsj.com/digits/2014/08/15/in-the-battle-for-the-connected-home-stakeholders-are-lining-up/

[11] *See* https://www.gov.uk/smart-meters and https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/197794/smart_meters_programme.pdf

[12] According to the European Commission, ICT can be the most powerful tool to maintain costs and high-quality health and social care. Moreover, given the growth forecast for telehealth, Europe can achieve economic benefits, as well as quality of life improvements. *See* http://ec.europa.eu/digital-agenda/ehealth-and-ageing

[13] In the UK, under the leadership of NHS England Medical Directorate, a programme called *3millionlives* combines clinical services and technology to improve access to health services. *See* http://3millionlives.co.uk/about-3ml#3millionlives_-_nhs_england_vision_statement

[14] *See* http://www.prnewswire.com/news-releases/europe-to-overtake-us-in-cellular-telematics-market-by-2016---mobile-operators-go-after-the-connected-car-opportunity-255076341.html

[15] *See* http://europa.eu/rapid/press-release_IP-14-141_en.htm

200 million vehicles in use. And in the UK, the government announced a commitment to fund "real world" trials of driverless cars.[16] AT&T is also contributing to the advancement of next generation cars. AT&T recently introduced the AT&T Drive studio, a dedicated facility for connected car innovation and research. It is a working lab where AT&T tests and develops technologies to enhance the driving experience by improving safety, convenience and entertainment. AT&T also introduced its global connected car platform called AT&T Drive. AT&T Drive allows automakers to develop the services and capabilities to differentiate their solutions in the marketplace.[17] In addition to these technical initiatives, AT&T announced several connected car agreements with automotive makers, including deals covering North America with General Motors (GM),[18] Tesla[19] and Volvo.[20]

Whether it is smart cities, health monitoring or connected cars, IoT applications—limited only by the imagination—continue to accelerate. In fact, according to Innovate UK, Britain's Internet economy is growing at 10 percent per year and by 2016 will contribute 10 percent of GDP.[21] By any measure, the IoT is positioned for exponential growth and profound societal impact.

That impact will be far reaching, with global cross-border opportunities. That is, IoT solutions not only create social welfare benefits in the UK, but can create economic benefits to the UK's industry at large, by, for example, enabling manufacturers to have success with exports to world markets. Cisco, one of the major participants in the IoT, estimates that the IoT will create up to 14 trillion dollars in turnover opportunities over the next decade.[22] Therefore, in countries with regulatory policies that encourage new M2M technologies and business models, the IoT is poised to deliver significant economic and social benefits. Notably, supportive M2M policies must be based on the premise that the new business models for the IoT differ greatly from the traditional business models that have supported the mobile phone and tablet industry segments in the past.

---

[16] See, https://www.innovateuk.org/-/green-light-for-trials-of-driverless-cars-on-uk-roads?redirect=https%3A%2F%2Fwww.innovateuk.org%2Fnews%3Fp_p_id%3D101_INSTANCE_7rd70tdk5JFd%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-1%26p_p_col_pos%3D1%26p_p_col_count%3D2

[17] *See* http://www.prnewswire.com/news-releases/att-leads-the-future-of-the-connected-car---announces-new-att-drive-studio-and-global-att-drive-platform-238904071.html

[18] http://www.prnewswire.com/news-releases/general-motors-selects-atts-4g-lte-network-to-deliver-enhanced-services-to-millions-of-vehicles-192939601.html

[19] *See* http://www.prnewswire.com/news-releases/tesla-and-att-enter-multi-year-exclusive-agreement-to-connect-current-and-future-models-in-north-america-239064921.html

[20] *See* http://www.prnewswire.com/news-releases/volvo-cars-and-att-enter-multi-year-agreement-to-connect-future-models-in-us-and-canada-255479991.html

[21] *See* https://www.innovateuk.org/digital-economy

[22] J. Bradley/J. Barbier/D. Handler, *Embracing the Internet of Everything to Capture Your Share of $14.4 Trillion*, Cisco, 2013, at page 6. *See* http://www.cisco.com/web/about/ac79/innov/IoE.html. Note: in its latest Visual Networking Index, Cisco reported that there will be "7.3 billion M2M connections globally, or nearly one M2M connection per capita, based on a 7.6 billon population by 2018." *See* http://www.nasdaq.com/press-release/cisco-visual-networking-index-predicts-global-ip-traffic-to-grow-nearly-threefold-reaching-16-20140610-00298

The new business models vary both in terms of the nature of the wireless connectivity provided to the end user, and the economics of providing that connectivity. For example, with most M2M devices, mobile network operators (MNOs) do not provide a communications service directly to individual end users. Rather, MNOs provide wireless connectivity to manufacturers, who distribute wirelessly-enabled products and services to end users. The manufacturer does not consider itself a provider of traditional communications services. Instead, the manufacturer develops a product that may be enhanced via the integration of wireless connectivity. For instance, an M2M-enabled smart meter fundamentally measures electricity usage; the M2M enhancement allows the near real-time transmission of that usage information to the electric utility company.

Manufacturers of products that contain a communications capability between two devices or machines typically do not view themselves as the provider of an electronic communications service to the end user and therefore generally do not charge the end user for a communications service. Rather, data transport is merely an ancillary component, not a principal feature, of the overall product or featured service (*e.g.*, data analytics, fleet management) sold to the end user customer. Therefore, in the M2M environment, economies of scale are essential:

- Compared to mobile phones and tablets, M2M devices typically have low data consumption and very low average revenue per user (ARPU) (*e.g.*, a smart meter sending a few hundred bytes of data per day vs. a smartphone or tablet consuming tens of megabytes).
- Manufacturers typically do not sell, or charge end users separately, for wireless connectivity. Instead, wireless connectivity is a cost of doing business that may be included in the overall price of the M2M product.
- Because their products usually have very low ARPU, manufacturers are *extremely sensitive* to development and deployment input costs.
- To efficiently amortise their costs, manufacturers tend to develop standardised products with long useful lives that can be sold in significant volumes across many countries.
- In sum, to be economically viable, M2M device manufacturers must be able to "build it once, sell it everywhere."

The emergence of new IoT business models pose unique challenges that require fresh thinking and innovative solutions, such as those relating to the allocation and use of numbering resources.

2. Extra-Territorial Use of Numbering Resources (Global SIM): An Innovative Approach to New Business Models

As noted above, when compared to traditional business models, the business models for the IoT typically have significantly lower ARPU and high input cost sensitivities. Given these realities, M2M device manufacturers would face an almost insurmountable obstacle when seeking to deploy M2M products and services on a global scale if they followed traditional handset or tablet business models. To obtain wireless connectivity under traditional business models, a manufacturer would need to contract with at least one MNO in each country into which it sells its goods, which could mean incurring transaction costs for negotiating and then implementing dozens or hundreds of individual agreements.

Moreover, for each country, the manufacturer would need a SIM card with a country-specific International Mobile Subscriber Identity (IMSI) code[23] embedded in each M2M device to be distributed in that particular country. This would mean maintaining country-specific inventory at each place of manufacture, leading to greatly increased inventory management costs. In cases where the M2M devices use E.164 numbers (*i.e.*, Mobile Subscriber ISDN (MSISDN) numbers or mobile telephone numbers), the manufacturer would also need country-specific E.164 numbers in each country where it seeks to distribute its products, further increasing its costs and increasing pressure on limited numbering resources.

IoT business models also require delivery of services on a globally consistent manner, including being able to operationalise centralised manufacturing and plant resources, and establishing common management systems for consistent policy controls (*e.g.*, ordering, provisioning, customer care, cyber security, billing and reporting). A fragmented distribution model, involving a separate SIM/IMSI per country and integration with each national MNO "platform," would require the manufacturer to use multiple platforms that would not be integrated and therefore would not work together. Instead of one platform, the manufacturer would need to work with dozens or even hundreds of different carrier platforms that would generate disparate reports that capture different information, depending on what the individual MNO offers. Requiring IMSIs for each country where a product is used would prohibitively raise costs and stifle IoT innovation and deployment in most markets (*e.g.*, automotive companies may not know the final destination of each vehicle at the time of manufacture, nor would a typical manufacturer of connected watches, soil moisture detectors, etc.). This will impact citizens in large and small markets, depriving them of leading-edge innovation and competition. Even across the 28 EU markets, if a nationally fragmented approach for SIM/IMSI use were to occur, there is a high risk that many markets could miss out on new IoT innovations due to the added expense and risk of needing to support a distinct IMSI platform for each country. This is also true for UK device manufacturers intending to export around the world but finding their distribution model constrained by a precedent that requires a separate IMSI platform for each export market.

The new business models for M2M services necessitate innovative numbering solutions to accommodate the requirements of M2M customers and their product manufacturers. While a number of possible solutions to address the potential concerns relative to the needs of these stakeholders exist,[24] AT&T believes that the most effective solution for global M2M services is to explicitly allow the

[23] The IMSI consists of the Mobile Country Code (MCC), Mobile Network Code (MNC) and Mobile Subscriber Identity Number (MSIN).

[24] Numbering solutions for M2M services include a shared national mobile customer number for M2M customers, a unique national MNC for each M2M customer, a unique MNC under MCC 901 for each M2M customer that requires roaming or who operates in a minimum of two different countries, and a unique MNC under a new shared MCC 90X for M2M services. (ITU Recommendation E.212 Annex A provides for a shared country code 901.) However, a Global SIM approach using roaming can be just as efficiently implemented with the extra-territorial use of a national MCC+MNC code as it can on an MCC 901 (or a new shared MCC 90X) MNC. While the shared MCC 901 or a new 90X code may be a potential long-term solution, a Global SIM approach based on a national IMSI is

extra-territorial use of numbering resources, such as E.212 (*i.e.*, MCC+MNC) as well as E.164 number ranges. Such extra-territorial use of numbering resources for M2M services should not be confined to traditional roaming scenarios[25] and should work in both directions—that is, national regulators should allow use of their MCC+MNC and MSISDN numbers outside their national territories, as well as allowing the use of foreign numbering codes within their national territories. In fact, this is an existing operational model already successfully in use in the incipient field of IoT, and it is enabling the goals of a digital single market in Europe.[26] Notably, acknowledging this, the CEPT/Electronic Communications Committee (ECC) Working Group on Numbering and Addressing in its final Report 212 on evolution of E.212 Mobile Network Codes[27] added a recommendation that "[t]he ECC should further analyse the concepts of roaming and extra-territorial use of E.212 resources to examine the implications of such use on national numbering plan management."[28] The inclusion of this directive recognises the role the Global SIM model contributes to the IoT.

To elaborate, there are existing, well-defined and well-established commercial models used between mobile operators that provide a practical basis for accommodating and facilitating the extra-territorial use of IMSIs and MSISDNs on a bilateral commercial basis. Foremost among these is the international M2M roaming framework that addresses and makes transparent international roaming used explicitly for M2M services. The roaming framework, currently the most efficient manner of delivering global M2M services, enables the use of the home carrier's IMSI and MSISDN to provide services on a global basis through a single SIM architecture. This architecture allows the most innovative devices, from large or small companies, to be deployed to any country in the world, thereby bringing the benefits of leading-edge technology to all countries, businesses, mobile operators and citizens. With the business models used for M2M, where end users often pay no data transport charge, the traditional policy considerations relative to the level of roaming charges are not an issue. Under the M2M roaming framework—recognised by the wireless industry's leading trade association, the GSM Association (GSMA), and endorsed through the MNOs' adoption of an M2M Annex—procedures are in place to transparently identify, measure and distinguish M2M roaming traffic from traditional handset or tablet

preferable, because the shared MCC 901 or new 90X code could involve considerable cost and time, up to 2 years, to get the necessary support structures and agreements in place.

[25] In ITU-T E.212 Amendment 3 (06/2011), the ITU established procedures for the extra-territorial use of an MCC+MNC in a "base station" in a foreign jurisdiction (*i.e.*, in a situation where a network located in one country broadcasts an MCC+MNC assigned to a network in another country). The ITU clarified, however, that these procedures do not apply to roaming.

[26] AT&T just introduced an enhanced Global SIM that is designed to meet GSMA specifications for M2M and device manufacturers. In doing so, AT&T became the first carrier to offer a GSMA-certified globally connected SIM. *See* http://about.att.com/story/att_launches_enhanced_global_sim_designed_to_meet_gsma_specifications_for_m2m_and_connected_device_manufacturers.html

[27] ECC Report 212, *Evolution in the Use of E.212 Mobile Network Codes*, CEPT/Electronic Communications Committee (ECC) Working Group on Numbering and Addressing, (April 2014). *See* http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP212.PDF

[28] *Id.*, at page 29.

roaming traffic.[29] The international roaming framework has been globally adopted by hundreds of mobile network operators who today enjoy the bilateral benefits of offering these services. And this bilateral framework has enabled large and small manufacturers alike to develop and export devices around the world, and to scale their business without the upfront entry barrier of establishing a distinct platform for each country before selling a single device. Thus, global numbering use promotes robust competition, and ensures competitive telecommunications markets because MNOs will continue to compete with each other to provide an international roaming platform for M2M service providers. Meanwhile, visited network MNOs benefit from the roaming traffic on their network.

Finally, the administration and regulation of numbers and electronic communications services rightly remains within the scope of authority and interest of Ofcom. Allowing the extra-territorial use of national numbering resources does not diminish or restrict that authority. Nor is there any precedent preventing the use of global numbering resources from either the International Telecommunications Union (ITU) or EU. National regulators retain oversight mechanisms, and can endorse a flexible numbering policy, while addressing policy interests in other areas. The truly global nature of the IoT requires the use of an appropriate SIM solution; therefore, numbering policies should embrace the Global SIM approach.

(*See item number 3 below, "Numbering and Addressing: The Continued Need for Mobile Telephone Numbers," for additional comments on the use of numbering resources.*)

3. Numbering and Addressing: The Continued Need for Mobile Telephone Numbers

Machines need to be uniquely identified and addressed in order to communicate; therefore, it is likely that E.164 numbers will be necessary for a long term with IoT devices. For many devices and applications developed today, E.164 numbers are used and will continue to be used throughout the lifecycle of the product. With many consumer and industrial products having lifetimes of 10 to 20 years, an ongoing supply of E.164 numbers will be needed. For the highly integrated nature of high-volume, low-cost, electronic modules, a retrofit or upgrade to an alternate numbering resource would be uneconomical. For instance, after expending substantial effort and incurring considerable expense, IPv6 use has seen considerable growth over the last few years. While leading core network providers have reached IPv6 deployments generally in the twenties—with, for example, Deutsche Telekom AG showing

[29] Historically, MNOs have supported their customers' international wireless connectivity through roaming agreements with MNOs in other countries. To facilitate the adoption of these types of international roaming arrangements as a commercial matter, the GSMA has developed a series of roaming contract templates. These roaming templates, which are available for use by GSMA's 800+ members, contain common industry-accepted terms and conditions that expedite the negotiation of roaming agreements. Commercially negotiated roaming arrangements that enable these customers to receive service outside their home country have been in place for decades and are mutually beneficial to the MNOs: the MNOs' customers receive service in foreign countries and the MNOs receive compensation from the other party for providing the service. Moreover, building on its success in fostering traditional roaming, in 2012 GSMA adopted an "M2M Annex" template for international roaming. Among other things, the Annex mandates transparency in the provision of M2M services by requiring the parties to agree to identify their M2M traffic separately from other traffic and to exclude traditional wireless services (*e.g.*, conventional 2-way dialable PSTN voice).

26.34 percent IPv6 deployment and AT&T at 23.95 percent,[30] many operators are at an early stage of IPv6 deployment due to a variety of factors including limitations in current equipment, cost to upgrade or replace, and lack of demand. To reach a global IoT market, device manufacturers will consider the breadth of IPv6 deployment before beginning development on IPv6-only devices.

There also will be a substantial overlap period where both IPv6 and E.164 numbers are in use. It is estimated it will take 5 to 10 years for IPv6 to become widely available. If the field lifecycle of a device is 20 years, E.164 numbers could be needed for the next 30 years. However, issuance of new E.164 numbers could only begin to be phased out when IPv6 becomes widely available and then only for those devices that do not need to rely on PSTN-based addressing. [31]

AT&T notes Ofcom's initial assessment (Consultation, at 1.33) that "IoT devices are unlikely to use telephone numbers to the extent that this would put pressure on available numbers" in the UK. AT&T has no evidence to suggest that this assessment is inappropriate relative to the UK. However, if a concern should materialise, Ofcom could consider the approach of several European countries[32] which have introduced a special range of numbers for M2M communications. These special ranges typically have number blocks which use a longer number sequence (up to the full 15 digits) in the E.164 format. The length of E.164 numbers for mobile users was selected to balance the needs of the efficient use of numbering with the human factors of communicating and dialling a convenient length. To achieve that balance, in Europe (including the UK) the average length of E.164 number ranges typically does not exceed 12 digits, which includes trunk code. Machines, however, have no such need for convenience and so for M2M communications a full 15-digit number allocation, as described in ITU E.164, could be considered.

4. Data Management: Self-Regulatory Industry Collaboration to Set Standards

With the proliferation of the IoT touching every sector, a massive volume of information is being generated, transmitted, collated and stored. And the amount of available information and data will only continue to grow as users adopt more Internet-connected devices. According to industry analyst firm IDC, the installed base for the IoT will grow to approximately 212 billion devices by 2020, a number that includes 30 billion connected devices. IDC sees this growth driven largely by intelligent systems that will be installed and collecting data across consumer and enterprise applications.[33] Data from these embedded systems are projected to grow fivefold to 10 percent in 2020, from 2 percent in 2013.[34] This volume of the data, together with variety and speed, heighten awareness of security and privacy concerns. That is why the industry is proactively addressing security and privacy issues, and their

[30] As of 12 September 2014. *See* http://www.worldipv6launch.org/measurements/

[31] For example, a remote wireless temperature sensor may communicate with a centralised server platform via M2M SMS messages.

[32] For example, Belgium, Bulgaria, Croatia, Denmark, Finland, France, Netherlands, Norway, Portugal, Spain, and Sweden.

[33] IDC, "Worldwide Internet of Things 2013-2020 Forecast: Billions of Things, Trillions of Dollars," Doc #: 243661, October 2013.

[34] *See* http://idcdocserv.com/1678

interrelation with Big Data (*see Data and Analytics section below*). Indeed, there are a number of industry-led, collaborative efforts underway, such as those to develop technical security specifications and privacy seal programs (described more fully below), to address security and privacy issues particular to M2M.

Security

The industry is keenly focused on the security issues around M2M services. And as devices become ever more connected it follows that security risks are likely to increase across the ecosystem. Threats can include interception of data transmissions, network and device denial of service attacks, malware infections and other forms of threats—with some as yet unknown. IoT security, therefore, is a necessary prerequisite and any service provider or IoT solution failing to adequately address security from the outset will not have commercial success. For this reason, there are a wide variety of standards bodies working on security specifications for M2M.

One such example is the "oneM2M" initiative—an international standards body[35] established with the goal of developing technical specifications which address the need for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide. With more than 250 members, including AT&T, oneM2M is focused on technical specifications for security and privacy aspects of M2M (authentication, encryption, etc.) and involves liaison relationships with other standards bodies such as 3rd Generation Partnership Project (3GPP), Broadband Forum (BBF), Home Gateway Initiative (HGI) and the International Telecommunications Union-Telecommunications Standardization Sector (ITU-T). The Telecommunications Industry Association (TIA) and the Consumer Electronics Association (CEA) are also working on M2M standards. The Cloud Security Alliance (CSA) has published several recommendations for security in the cloud which are relevant to M2M applications that are being deployed in the cloud. More broadly, there is ongoing mobile security standards work at various industry organisations including 3GPP, GSMA, and Alliance for Telecommunications Industry Solutions (ATIS).

Privacy

An example of proactive, co-operative industry efforts on privacy issues in the United States is the development of a Smart Grid Privacy framework. In October 2012, the Future of Privacy Forum (FPF) announced a privacy seal program based upon a fundamental set of privacy principles incorporated in its Smart Grid Privacy Guidelines. Aware of the critical need for privacy and security protections for sensitive consumer energy information, industry members proactively engaged in collaborative, self-regulatory efforts. FPF convened a diverse group of companies—including AT&T,

[35] The European Telecommunications Standards Institute (ETSI) was one of seven leading ICT standards development organisations to launch oneM2M in 2012. *See* http://www.onem2m.org/press/oneM2M%20Launch%20Release.pdf

Comcast, Ecofactor, IBM, Intel, Motorola, Neustar, Opower, Tendril, Verizon, and TRUSTe—to develop the privacy framework. FPF also requested input from utilities and utility regulators as interested stakeholders. The Guidelines target companies that use consumer information (*e.g.*, companies offering home energy management, remote home control or security, smart thermostats and other services) to provide smart grid services. Furthermore, the Smart Grid Privacy Guidelines are designed to help assure consumers that organisations using their information are employing best practices for security, privacy, and dispute resolution and are using consistent approaches to obtaining consent. In order to receive a seal endorsement, participating organisations must validate that they are following Smart Grid Privacy Guidelines. TRUSTe, the company that administers the seal, checks an organisation's privacy policy, scans for potential privacy threats, reviews consumer consent processes, and conducts various business and technical assessments to verify compliance. As the Smart Grid example suggests, self-regulatory measures can deliver real progress toward a more comprehensive, consumer-centric approach to privacy. In fact, in another example of industry collaboration, the UK's Information Commissioner's Office (ICO) issued a consultation[36] on a draft framework for a consumer-facing privacy seal scheme to serve as a "stamp of approval" of an organisation's commitment to adopting sound privacy standards. Seeking industry input, the ICO is looking for proposals that include, among other principles, privacy and data as its core focus and the demonstration of good practice of information rights, rather than just compliance with the letter of the law.

AT&T has participated in a number of other industry efforts to develop privacy guidelines. For example, AT&T assisted in the development of the CTIA (The Wireless Association) Best Practices and Guidelines for Location-Based Services.[37] We also joined discussions with the FPF and the Centre for Democracy and Technology regarding the development of broader industry guidelines on privacy protections for location-based services.[38]

Data Analytics (Big Data)

The term "Big Data" is often used to refer to the very large quantity of digital information that may be collected via modern communications products and services. When Big Data from the IoT is appropriately aggregated, anonymised and safeguarded, it can be used to reveal otherwise indiscernible patterns and trends in a number of socially beneficial contexts, including medical research, energy conservation, multi-modal traffic management, agricultural, and commercial and industrial productivity. Realising the value of such data, and the need to safeguard it, this past February AT&T and multinational technology and consulting giant IBM established a global alliance that combines their analytic platforms, cloud, and security technologies with privacy in mind to gain more insight into the data derived from machines in a variety of industries. In March, AT&T—along with Cisco, GE, IBM and Intel—formed the Industrial Internet Consortium (IIC), an independently-run open-member consortium of technology

[36] The ICO expects to select a privacy seal scheme in early 2015 and to launch a first round of endorsed schemes in 2016.*See* http://ico.org.uk/about_us/consultations/our_consultations

[37] *See* http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf

[38] *See* http://www.futureofprivacy.org/best-practices-for-mobile-app-developers/

innovators, industrial companies, academia and government focused on accelerating the development and availability of intelligent industrial automation for the public good. The IIC's scope of work includes influencing the global standards development process for Internet and industrial systems and building confidence around new and innovative approaches to security. Notably, the IIC had more than 50 members from Europe, Asia, Latin America and North America only two months after launch.[39] In the UK, the Hyper/CAT Consortium is developing a new standard for secure IoT interoperability, to make it easier for businesses and government organisations to collect and analyze data traversing smart devices, regardless of their location, manufacturer or format. HyperCat, one of eight such projects funded by Innovate UK, includes industry leaders BT, Intel, and KPMG.[40]

Given that security and privacy are central to the commercial viability of the IoT, there is incentive for industry to proactively focus on such issues. Industry stakeholders like AT&T have a track record of committing to meaningful, voluntary efforts to improve privacy and security—and will continue to do so. Indeed, as demonstrated, there are many industry efforts underway—in the United States, the UK and elsewhere—to address the particular security and privacy issues of the IoT. Ultimately, the most productive approach to ensuring robust privacy and security standards is voluntary compliance with broadly accepted industry guidelines. Thus, any further standards efforts should (1) build on work already in progress relative to M2M security and privacy standards, (2) be an industry-led rather than a top-down regulatory standards-based model, (3) be flexible enough to accommodate innovation, (4) be ecosystem-wide as opposed to being narrowly focused on specific sectors such as mobile carriers, and (5) allow data controllers[41] to determine the best approach for protecting consumer privacy. A good start for any action on the matter would be to establish an inventory of already established or in-progress best practices.

5. The Role of Ofcom

One crucial regulatory role for Ofcom, and other regulators, is the oversight of finite resources like numbers and spectrum. Such management should be guided by successful market solutions to new developments (*e.g.*, the use of extra-territorial numbers) and, in the case of spectrum, technological neutrality, to the extent practicable. More generally, there is abundant evidence that the IoT's growth will be exponential and unparalleled; it is also manifest that technology drives such growth, not regulation. Therefore, as today's technological advances are happening in a more dynamic environment and with more disruption to historic business models than ever before, only flexible, globally-minded, industry-driven policies will create conditions for pioneering technologies, services and business models to flourish. Indeed, Ofcom is of the view that "industry is best placed to drive the development, standardisation and commercialisation of new technology."[42] AT&T quite agrees. The IoT, as with the

[39] *See* http://www.iiconsortium.org/press-room/06-03-14.htm
[40] *See* http://www.hypercat.io/consortium.html
[41] Data controllers may be the MNO, but could also be the device manufacturer, a third-party system integrator, a value-added reseller of ICT services, an unlicensed Wi-Fi network operator, and the like.
[42] Consultation, at 1.3.4.

Internet in general, is best served by a light-touch regulatory approach that subordinates to technology and geography. Regulatory oversight, therefore, should enable the intersection of technology with imagination to promote innovation, which drives investment and prosperity.

* * *

AT&T commends Ofcom for engaging stakeholders to advance the conversation to inform regulatory policy that maintains the trajectory and promise of the IoT. AT&T would be pleased to answer any questions concerning these comments.

Respectfully submitted,

Mike Corkerry
Executive Director, EMEA Government Affairs
AT&T
mike.corkerry@att.com
www.attpublicpolicy.com