ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

The “Intelligence” of Things — How the Internet of Things Connects the Spaces

Technology, Privacy, and eCommerce


Do you accept the user agreement?

CHEAT SHEET

- ***The future of the IoT.*** The Internet of Things (IoT) is expected to exacerbate the role that technology places on the business as communication between platforms increases. The IoT will bridge the gap between long distances and do away with the need for physical presence.
- ***Regulatory considerations.*** Because the IoT is still rising in prominence, in-house counsel should address data protection as soon as possible. Regulatory considerations surrounding the IoT is still under development in many regions, so companies must be self-motivated to ensure security.
- ***The early bird.*** It is important to work with regulators regarding the IoT early in the process. In-house counsel should work closely with the business by framing proposed technologies around regulatory restrictions and government policies.

- ***Clearly consent.*** With all of the devices and services that the IoT enables, in-house counsel should ensure that data permissions are clearly stated to guarantee transparency.

It is the spring of 2020, and Shalini is relaxing during her weekend at home. She needs to plan her day and catch up with a few friends later in the evening. She has various errands to run before she can go to the health club for her daily workout. She remembers that the refrigerator needs to be fixed. Shalini pushes the blue button on the side of the refrigerator and requests a service call from the refrigerator company. Within the next two minutes, the service engineer calls back to set up an inspection for the following day. This is what we call the Internet of Things (IoT) and, if you may, the Intelligence of Things.

Over the past few years, the IoT has captured headlines across the world, with newspaper and magazine articles describing its potential to transform our daily lives. Historically speaking, the semantic origin of the expression (without any guesses) is in two words and concepts: “internet” and “thing” — where “internet” is the communication protocol, including the internet suite (TCP/IP), while “thing” is “an object not precisely identifiable.” Therefore, semantically, the IoT means “a worldwide network of interconnected objects uniquely addressable, based on standard communication protocols,” but are these protocols really standard, and are they governed by standard environmental rules?

Based on Cisco IBSG’s definition, the IoT didn’t exist in 2003, because the number of connected things was relatively small. Smartphones were just being introduced. Refining these numbers further, Cisco IBSG estimates that the IoT was “born” sometime between 2008 and 2009.

White Paper by Cisco on The Internet of Things, “How the Next Evolution of the Internet Is Changing Everything” – Author Dave Evans in April 2011.

The LED screen on Shalini’s refrigerator, which she ordered online last year, shows the availability of her favorite avocados at the South City mall. Shalini selects the quantity of her favorite fruits on the display unit and places her thumb impression on the biometric reader adjacent to the flashing LED. She places the order and makes the payment all in a few seconds.

It is already noon, and the beeping from her phone alerts her to a message — as does the reminder displayed on her wristband. Shalini checks the band and realizes that her health club instructor asked her to do a 30-minute warmup sprint session, based on her activity schedule before her workout. The band on her wrist also sends a diagnosis of her heart and pulse rates, which allows her instructor to plan a special weekend workout. She clicks a few buttons on her wristband and, in a couple of seconds, it records her heartbeat and sends the information to her instructor.

In its simplest form, the IoT is a state where “things” will have more and more information associated with them and may have the ability to sense, communicate, network, and produce new information, becoming an integral part of the internet — thus enabling anytime connectivity for anything and anyone. The wearable devices are just one such aspect of IoT, which has the ability to astonishingly improve health outcomes, particularly in the treatment of chronic diseases that now take an enormous human and economic toll.

As explained earlier, the IoT is the internetworking of devices over a network. Such devices or small

equipment could be pasted or fitted on various other objects. The devices are powered with sensor chips, software applications, and interior electronics. Imagine a half-thumb-sized device that has all these features and functionalities included. These super smart devices connect with other electronics, software, and sensors via network connectivity that enables each device to virtually speak to one another. Software instances and applications that form part of the IoT package receive billions and trillions of data and analyze what needs to be done to give the desired output. Network connectivity plays one of the most important roles in this chain and can be made available in the form of multiple connectivity options such as WiFi, 3G, 4G, 5G, and LoRa WAN network technologies. WiFi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed internet and network connections. While 3G, 4G, and 5G are different types of mobile communication technologies with each additional "G" indicating faster internet speed. Simply, the "G" stands for generation, as in the next generation of wireless technologies. Each generation is supposedly faster, more secure, and more reliable. LoRa WAN is a low-power, secure, and long-range network with deep indoor coverage — which can be very useful in rural areas. Relevant networking technology can be chosen depending on the kind of data, geographic limitations, network costs, administration costs, and amount of power supply required.

Imagine a world where objects use their own intelligence (popularly known as artificial intelligence) to work with each other automatically over distances. The water starts to pour the moment you step into the shower. Devices respond to your questions and read out the itinerary of the day while you prepare breakfast. Your two–wheeler drives you to work via the best available route. Your office laptop turns on the moment you switch on your workstation lights.

Thus, "things" are expected to become active participants in business, information, and social processes as they communicate among themselves as well as with the environment. With advancements in technology, these objects exchange information "sensed" about the environment while reacting autonomously to "real" or "physical world" events — with or without direct human intervention.

The IoT could eventually form part of multiple segments and verticals, which could include smart city solutions, security, the tracking of human life/body, physical security, smart metering, supply chain management, and retail/consumer durables asset tracking. The devices could also be connected over the web, which collects, processes, stores, sends, and takes action on the data that is collected, processed, or stored from its surroundings. The IoT lets these devices do most of the work with minimal human intervention. All these connected devices further generate huge amounts of internet traffic, including loads of data that can be used for various purposes such as analytics, data mining, marketing, or reaching out to potential consumers for a service or product — that could cause both security and privacy issues. The IoT will provide real-time information on various things that we've never thought of before. It will bridge the gap between long distances, and in some instances do away with physical presence of people or objects. It will also help improve the real-time monitoring of business processes in order to avoid downtimes, while keeping our homes and families safe remotely. A number of organizations, both within and outside of India, are coming up with flexible IT and work-related processes such as bring-your-own-device (BYOD), telecommunting, or work-at-any-desk policies. This enables their employees, contractors, consultants, and professionals to use their own IT equipment for work and cuts down on travel time to and from home and office, thus encouraging productive hours for work. In-house counsel should work with the HR and IT departments to frame relevant employee welfare policies and address concerns around the consent requirement to monitor all IT equipment by the organization, the compensation policy to account for the BYOD policy, and the mandatory work hours under employee welfare legislation. Also, in-house counsel have to ensure that the contractual obligations with a customer allow for such policies to be

put in place and that sufficient security measures are obtained to comply with applicable information security and data protection laws.

Shalini's lifestyle explains the kind of changes that IoT could bring to our daily lives. Her refrigerator has a mounted device that is connected to a central network base station, which is, in turn, connected to the company's backend platform. The backend platform is connected through an application programming interface with the company's call center. When Shalini pushes the button on the refrigerator, it sends an alert in the form of a message through the network. The company's service engineer receives the call from the call center executive, who informs him or her that Shalini requires a call back for service. In this case, to enable a better customer experience, the service engineer calls the customer to understand the product issues, eliminating the need for the customer to follow up with the company for support. This kind of a mounted device could be configured with any other consumer durable product. Further, the biometric reader on the refrigerator could be linked to Shalini's bank account, making it easy for her to pay for her groceries. Similarly, her wristband is linked to various other over-the-top providers in the backend. The wristband comes with a set of embedded functionalities that could detect and keep a count of a person's heartbeat and pulse rate. Such medical diagnostic data could be pushed to the medical practitioner for analysis — as illustrated in Shalini's planned workout.

Although IoT is still a nascent phenomenon, with many aspects of the regulatory environment under development, especially in India, weak security may be the most important issue for in-house counsel to address. Since the IoT industry verticals differ in many respects, their security challenges also will vary.

As in-house counsel, it becomes pertinent to understand more than just the legalities around the IoT. Where does your organization fit in the IoT solution and to what extent it will either affect or be affected by the IoT elements? With the onset of IoT products and services, operations should not remain limited to the review of contractual forms. Creative thinking, much earlier in the entire value chain, needs to occur. A good amount of handholding will be required among in-house counsel, external subject-matter experts, external counsel, organizations, government institutions, businesses, and salespeople — who will form an integral part of the stakeholder community responsible for its inception. Some of the key questions that legal counsel should think about for their organizations, either as sellers or buyers of an IoT solution are:

- Does the IoT solution require an in-depth regulatory check (if any) for components that could possibly be regulated in the near future? What should organizations watch for when working toward compliance? For instance, is the deployed network within the ambit of any applicable telecom regulations under the local applicable laws, does the seller of the IoT solution comply with those regulations? Does it have the relevant licenses or permissions to offer such a solution? Is the buyer required to observe a certain minimum standard to be able to use such a regulated network?
- What are the applicable compliance regimes that may have to followed in terms of supply or use of the object? Are there any legal or regulatory sanctions that need to be observed or adhered to when using a specific object in a specific location? Who are the end users or individuals who may be a touch point in the IoT solution? Are there any applicable data privacy laws that govern the personal or sensitive personal information of such individuals that travel over the network? Are such networks and infrastructures compliant with the minimum security and safety standards prescribed for the protecting personal or sensitive information under the applicable legislation?
- Who is responsible for seeking local permissions, including right-of-way permissions and

applicable security and access clearances for the use of specific objects at specific locations? These could either be under certain national security surveillance legislation or could be significant from a national security perspective.
- Does the manufacturing of the objects require specific permissions, such as tdepositing the source code for the objects used as part of the IoT chain — which may be responsible for legal interception monitoring?
- Is there a seller obligation or buyer remedy in case of any claims, issues, and defects with respect to components forming part of the IoT, allocation of liabilities, and commercial and legal recourses?
- What is the applicability of local or international laws depending on the type of cross-border or regional solution?
- Are there any specific intellectual property rights issues given that the solution could be global in nature? Consider the naming of the product, the granting of rights and sublicenses, as well as who owns the data, is generated inn real-time.

These questions are very basic and may change or require more introspection among think tanks, including legal counsel within and outside an organization.

This story paints an interesting picture over the years to come, as big and small developments mix together, and some old developments return with a new facade. By blending physical reality with virtual reality, the IoT vastly expands the reach of the digital revolution. The multitudinous possibilities that arise from the ability to control things in the physical world through technology have inspired a torrent of innovation. The all-embracing changes that the IoT can bring to how consumers attend to their health and fitness have also inspired visions of a very different future — as well as a good deal of hype.

That said, you are not alone. We may need to slow down the pace of IoT development or pick up the pace of standards and security. The IoT has been growing and spreading rapidly across the world, but there is one big chunk of ice that still needs to be cracked — one small incident that could cause a tsunami.

Why the IoT? Imagine a world where every human is connected to a device, which is connected to a daily health monitoring device, that’s connected through the internet. In case of a natural or unnatural mishap, an alarm is raised for healthcare units to rush immediately for aid. No phone calls are required, no delay in aid occurs, and as a result, lives are saved. That is the kind of world the IoT is capable of creating.

Kevin Ashton coined the term “Internet of Things” to describe a system where the internet is connected to the physical world via ubiquitous sensors. The “thing” could be anything from a shoe to a watch to a medical instrument to any household device. However, the “thing” needs to have certain qualities to be part of the IoT.

We’ve discussed the IoT as a futuristic something but the truth is that it is already here. We are meeting this change in a familiar manner — with genuine transformation. The forecasts predicted by the June 2016 Ericsson Mobility Report clearly state that we will have as many as 16 billion connected devices by 2021. Ericsson further reports that “IoT is set to overtake mobile phones as the largest category of connected devices by 2018.”

Press releases - Internet of Things to overtake mobile phones by 2018: Ericsson Mobility Report.

Rishi Bhatnagar, president of Aeris Communications India, says, “The IoT market in India is projected to grow over a CAGR (compound annual growth rate) of 28 percent through 2020. I believe it is an achievable projection with the government programs such as Digital India, which aims to unite the nation with high-speed digital highways and connect 1.2 billion Indians, 100 smart cities, Make in India, and other such initiatives. We are currently working on smart city projects for network infrastructure building for IoT.”

Applying IoT technologies to human activities is already showing potential for massive change in people’s lives. From giving people with chronic diseases new tools to manage their conditions to increasing fitness to avoiding disease, the IoT is beginning to demonstrate its potential to improve human health. With regard to the IoT technology that we see around us, people are the major beneficiaries — reducing commuting times, making it easier to manage domestic chores, saving money on energy, getting greater value from products designed with information obtained through the IoT, and enjoying life in safer homes and cities.

> Applying IoT technologies to human activities is already showing potential for massive change in people’s lives. From giving people with chronic diseases new tools to manage their conditions to increasing fitness to avoid disease, the IoT is beginning to demonstrate its potential to improve human health.

However, for every advantage, the IoT brings a unique set of challenges. For example, most technology experts feel that there needs to be more legal framework or policy regulation around the IoT network. The question remains as to whether the onus lies with the network provider, the device manufacturer, the monitoring authority, or the user of the technology. Countries such as the United States have created a loose regulatory framework around such technologies. The security framework for such an extensive transmission of data over the network will need implementation for protection from cybercrimes and identity theft.

With the vital infrastructure connected to the internet, security threats will multiply, and governments will need to take notice. Policymakers will also play an important role in enabling the IoT by leading and encouraging standards that will make interoperability and widespread adoption possible.

A combination of a lack of standards and a lack of security about the “connectivity” of “things” has made this phenomenon more ubiquitous over the past decade. Further, if you think the trend might be starting to overload us, this is only the beginning.

Smartness comes at a cost. In its current state, the “things” in the IoT are expensive. A great example of this is the lack of outreach to the masses. The IoT is not currently a household term.

For the IoT to deliver its maximum impact across the board in all arenas, certain conditions need to be in place, and several obstacles need to be overcome. Some of these issues are technical, some are structural, and some are behavioral. Consumers, for example, need to understand and trust the IoT-based systems, and companies need to evaluate and adopt the data-driven platform that the IoT promises. In addition, regulatory issues need to be resolved, such as determining how to report incidents, what insurance needs to be in place, what part of the system must be regulated, and what can be left unregulated.

Certain IoT applications cannot proceed without regulatory approval. Even though the technological side of things is evolving rapidly, and many companies are investing in this area, it remains unclear

where, when, and how certain technologies will be allowed to operate. In addition, regulators must establish rules about liability. Policymakers have a role to play in shaping the market rules that affect IoT adoption (i.e., creating appropriate incentives for the consumer to adapt to the everchanging landscape). The government can play a role in setting rules for practices regarding the collection, sharing, and use of IoT data — which seems to be the paramount concern for consumers in adopting any change. It is always advisable to start early in the process. In-house counsel can contribute in multiple ways to ensure that organizations are able to provide relevant input in the legislative process. Government regulators who are responsible for creating new policies are also responsible for soliciting views and suggestions from the public. As part of the corporate affairs practice, in-house counsel should observe any notifications issued by government departments that request input from the people and be part of organisations that spearhead such initiatives (e.g., National Association of Software and Services Companies (NASCOM)) and work with the government in the space for example). In-house counsel need to work closely with the business in framing the relevant input to such proposed policies that could affect the organization's business interest. A lot of organizations use "policy advocacy" as a significant tool to have a relevant say in the decision-making process so that they are heard before any major legislation is announced by government departments and or associations like NASSCOM. In-house counsel should work with their industry counterparts to form an association to have common say on industry-specific issues to enable policy advocacy not just at an individual level but at an association and industry level. We believe that ACC is one such association that may provide a platform for in-house counsel to gather and work toward policy-changing initiatives.

Clearly, the IoT offers substantial benefits for consumers, as well as a new set of risks. IoT technology has the potential to drive down the costs of goods and services and contribute to greater consumer convenience and time-saving. As they travel, consumers may benefit from IoT-managed roadways, self-driving cars, real-time transit information, and planes that land and take off on schedule. At home, they can offload housework to smart appliances, save money on energy, and improve their health. However, privacy concerns will only grow as the IoT spreads. Consumers will need to be cognizant of the data that are being gathered and how that information is used. When consumers sign up for services, they should bear in mind what kind of data permissions they are granting and push third parties for transparency. Given the additional value that interoperability can unlock, consumers can take that into account as they consider purchasing IoT systems.

Finally, with all of the devices and services that the IoT enables, consumers might be overwhelmed by the proliferation of information. When data are plentiful, the scarce resource is attention. Finding ways to manage this potential information overload will become increasingly necessary for consumers.

Miller in his 1962 study provides some extremely effective strategies for dealing with overload; strategies that in some cases work just as well today as they did in the 1960s. Here are Miller's seven strategies for dealing with information overload, updated for the times:

- Omission – The concept is simple: You can't consume everything, so just ignore some;
- Error – Respond to information without giving due consideration if it is not going to do any harm;
- Queuing – Putting information aside until there is time to catch up later;
- Filtering – This is similar to omission except filtering employs a priority scheme for processing some information while ignoring others. Automated tools are particularly well suited to help filter information;
- Employing multiple/parallel channels – Doling out information processing tasks;

- Approximation – Processing information with limited precision. Skimming is an example of approximation; and,
- Escaping from the task – Making this someone else's problem. While it sounds irresponsible, admitting you can't do it all and giving an assignment to someone else is sometimes the best strategy.

If we focus on the Indian framework alone and consider some of the steps that the Indian government has taken, one can see the enthusiasm from the Ministry of Electronics and Information Technology (MEIT), where the department stated that "one of the top most initiatives in the form of Digital India Program of the Government which aims at 'transforming India into digital empowered society and knowledge economy,' is expected to provide the required impetus for development of the IoT industry ecosystem in the country. MEIT's goal is to create an IoT industry in India of US$15 billion by 2020. It has further assumed that India would have a share of 5 to 6 percent of the global IoT industry.

Therefore, it is evident that not only the private players in software, electronics, and the telecom/network community are interested in investing in IoT products, but the Indian government is also equally committed to the industry. In fact, the government has come out with a draft IoT policy that is open for public review. India's plan to digitize the economy is seen in every sphere, including demonetization encouragement, incentive platforms for using digital wallets, mandatory Aadhar (biometric-based) electronic authentication factors for certain types of transactions, the concept of 100 smart cities, and the promotion and development of a ecommerce marketplace.

Every new sector or opportunity comes with its technical, commercial, regulatory, and legal challenges. The new age of computing will give rise to issues that deal with personal data privacy, including security, data ownership, contractual arrangements and their validity in electronic world, patents, consumer interests, service provider liability, and other services, —especially when they touch the human element. Further, jurisdictional issues, given that boundaries are increasingly blurred due to global connections, and commercial competitiveness, given that there are different taxation regimes in different geographies around the world, will create challenges.

In India, there is no state-specific or subject-specific law that may regulate or completely govern all the components of the IoT ecosystem. The subparts of the IoT would be governed or regulated by different legislative frameworks. For instance, there will be great interplay between the (Indian) Information Technology Act, 2000 (IT Act) and amendments and rules made thereunder, including data privacy rules and intermediary guidelines issued under the IT Act, the relevant intellectual property laws governing the copyrights and patents, and relevant telecom laws to the extent they regulate the network component that forms an integral part of the IoT chain. It would be interesting to see if the government of India comes out with IoT–specific regulations that govern the complete IoT vertical. Therefore, in-house counsel doing business in this part of the world (and beyond) should keep abreast of changing legislation and regulations. There is also a need to evaluate whether such nation-specific regulations need to have further interplay with international laws given the global outreach of the IoT systems.

The IoT has transformative potential for the world in general. This will not only create new sources of revenue and lines of business but will also present an opportunity to develop new and valuable systems. Even though there are areas that need attention and security standards that need to be streamlined, the general public will have the most to gain. The potential is endless: longer lives from

IoT health applications and safer transportation, greater convenience and time-savings, less costly goods and services, and more. The IoT completely redefines how we engage with the physical world.

To sum up, IoT integrates three main ingredients: devices, connectivity, and software applications. Devices collect data from their surroundings or from the environment where they are placed or installed. The data are then either collected or processed to another device or application connected over the cloud. Once the data travel to the cloud, the software applications further process them and provide the desired output. The software applications are designed in a way that they have an interface to the user of such output, where such interface could be in form of a text message, email, or other notification.

In-house legal departments are no longer considered to be a shared support services but an integral part of the line of business, where business leaders look to general counsel and their teams to work with the sales and products folks to provide a pragmatic solutions-oriented approach to regulatory compliance and legal concerns, while keeping the business interest in mind. In-house counsel now not only support the business but advise the company in the development of employees, the organization, and the external environment. In-house counsel must put in place dedicated compliance working groups within the organization that are responsible for identifying the introduction of new laws, rules, and regulations that could affect the organization’s business and practices. Such work groups could comprise leaders from each line of the business, external consultants, counsel, and subject-matter experts from within the organization.

Lastly, policymakers and governments need to recognize the growing footprint of IoT and start to update and tighten existing rules and standards for not only protecting IoT data from being stolen or abused but also to balance the needs for data privacy and intellectual property protection with the demands of national interest and security aspects related to individuals and the nation as a whole.

The digitization of machines, vehicles, and other elements of the physical world is a powerful idea. Even at this early stage, the IoT is starting to have a real impact. By examining the proliferating uses of the IoT in specific settings, we have been able to estimate the magnitude of potential economic impact from IoT applications over the next 10 years. Capturing that potential will require innovation in IoT technologies and business models and investment in new capabilities and talent. With policy actions to encourage interoperability, ensure security, and protect privacy and property rights, the IoT can begin to reach its full potential.

> Even at this early stage, the IoT is starting to have a real impact. By examining the proliferating uses of the IoT in specific settings, we have been able to estimate the magnitude of potential economic impact from IoT applications over the next 10 years.

This article was prepared by authors named below in their personal capacity. The opinions expressed in this article are the authors’ own and do not reflect the view of the organizations that they are currently or previously employed with.

Damandeep Kaur

Head of Legal

Intelenet Global Services

She has over 12 years of post-qualification experience, the majority of which has been as an in-house counsel dealing with diverse areas including mergers and acquisitions, HR advisory, compliance, intellectual property, and complex contracting in the outsourcing industry.

Nitin Suri

Senior Legal Counsel (Commercial and Litigation)

Tata Communications

He has over 12 years of diverse post-qualification experience covering working with practicing lawyers, IP boutique law firms, and organizations in the telecom space and those delivering consumer electronics products and services. His projects involve mergers and acquisitions, complex commercial contracts, employment laws, intellectual property laws, legal advisory to business, and shared support functions, with an additional focus on IoT and healthcare specific issues in the industry.