WHITE PAPER

Capitalizing on the Internet of Things (IoT):

Challenges and Opportunities for Insurers and Automakers

Executive Summary 1

Introduction: The Nature Of The Internet Of Things 2

The Five Keystones Of Iot Continuity 2

Technical And Policy Challenges 5

- Standards And Interoperability 5
- Harnessing Data Effectively 5
- Agnostic Approach To Standards 6
- Portability Of Data 6

The Working Ecosystem 7

Case Study For Iot: Insurance Opportunities – 7

- Expanding The Book Of Business Example: Life Insurance Discounts Based On Fitness Tracking 8

Case Study: OEM – The Promise Of The Connected Car 9

- Example: Road Usage Charging 9

Additional Examples 11

About IMS 12

About IMS Iot Marketplace 12

Executive Summary

Advances in Big Data technologies and the increasing use of sophisticated analytics to solve business challenges have established a foundation for the Internet of Things (IoT). IoT solutions expand on the Big Data concept, harvesting massive volumes of data through sensors and edge devices and then applying analytics to this data for practical applications. IoT provides ways to improve home security and convenience, influence our health and well-being, make automotive travel safer and more efficient, and add to everyday activities in a way that informs, guides, and—in the best examples—delights.

Applied to insurance, the Internet of Things can become a mechanism to open up new opportunities and develop new programs. Applied to vehicles and transportation, particularly in the case of the connected car, it combines personalized entertainment, intelligent route planning, emergency assistance, multiple channels of communication, improved maintenance and operational efficiency, and—through specialized apps and embedded hardware and software, or added by means of smartphone connectivity—a wide range of services that can be shaped to the individual needs and preferences.

Many of the pieces needed to realize the IoT vision are already in place. Others are being readied for use and prepared for mainstream application. At this point—in the early stages of IoT maturity—the possibilities are substantial and expansive. As a differentiator in the market, IoT capabilities offer numerous chances to draw on innovation and invention, making it possible to develop products and services that can provide a strong competitive advantage to organizations that move quickly. As with any new technology, the direction will be shaped and controlled by the pioneers who gain the expertise and enter the market early, before it becomes saturated.

This whitepaper provides an introduction to IoT and showcases some of the opportunities that it affords, giving insurers a means to expand their book of business and OEMs a glimpse of how IoT will re-energize and reshape personal travel. We also provide examples of how IoT is already being used, as well as blue-sky imaginings of how it can be used as the supporting technologies are refined. A fair measure of knowledge and expertise is required to participate in the IoT ecosystem and this paper outlines the factors that are leading to the formation of a marketplace around IoT that will open numerous opportunities.

Introduction: The Nature of the Internet of Things

In simplest terms, IoT provides a means to connect devices (e.g., smartphones, tablets, or wearables) and everyday objects (e.g., thermostats, vehicle telematics systems, or home security systems) to the Internet. Connected devices and objects are able to communicate with other "things." Data derived from these devices can be run through analytics applications to inform, predict, project, and carry out intelligent actions based on algorithms.

Prior technologies have allowed devices to communicate with the Internet and exchange information of value, such as a home security system that alerts security firm professionals when there is a breach of the home perimeter. The IoT amplifies this value by exchanging data across systems, analyzing this data, and then interacting with other devices, sensors, and data canters. For example, the home security system might detect the family automobile turning into the driveway, unlock and open the garage door, let the security firm know that the owners are home, provide the insurer issuing the home policy with the occupancy data of the residents to help set premium levels, and communicate with other home systems to turn on the lights, or turn on the heater or air conditioner—depending on current weather conditions. As the homeowners or other occupants enter the house, control units might turn on the entertainment system and play relaxing music to end the workday (or turn on the sports channel featuring a game being played by the homeowner's favorite team). This cross communication among different systems and sensors opens up tremendous possibilities for OEM automakers and insurers looking to extend and strengthen product and service offerings.

The Internet of Things advanced within the Gartner Hype Cycle for Emerging Technologies, moving from simply being a promising speculative idea to becoming a worthwhile, proven technology that is beginning to generate useful implementations in commerce, transportation, healthcare, and more. In a press release in November 2015, Gartner projected that 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015. The research firm estimated the IoT spending across services will reach $235 billion in 2016.[1] In respect to the current state of IoT, Gartner commented: "The Internet of Things is becoming a vibrant part of our customers' and our partners' business and IT landscape."[2]

Different organizations are approaching IoT from a variety of directions, depending on individual interests in various types of data and how that data can be captured and applied to solving practical problems. As momentum builds around the business potential of IoT, some fundamental challenges are being addressed that will set the course for business implementations over the next few years.

The Five Keystones of IoT Continuity

To make IoT technology useful for OEMs and insurers, a number of barriers must be overcome. A foremost consideration is that the rights of participants providing data—from vehicle, home, person, or other source—must be managed according to prescribed usage terms. Throughout the full range of IoT activities and processes, rights to data use and sharing must be explicitly granted by an authority, and tracked to respond to any changes in consent (such as a subscription ending or a participant canceling consent). The complexities of managing rights and related activities across a large-scale IoT ecosystem require considerable expertise and a keen understanding of the supporting technologies. Only when these issues are

1 http://www.gartner.com/newsroom/id/3165317
2 http://www.forbes.com/sites/gilpress/2014/08/18/its-official-the-internet-of-things-takes-over-big-data-as-the-most-hyped-technology/#7ba98b2e1aaa

resolved can solutions for OEM automakers, insurance providers, and others be introduced into the marketplace.

This principle extends beyond simply accessing a service. It includes verifying any data brought into the ecosystem in a timely way and then ensuring that if this data is moved into different areas and domains, it is only being used for purposes that have been expressly stated. The recognized authority in each case bears responsibility for ensuring permissions are current and that the type of usage employed for an instance of data is consistent with assigned rights. For example, if a participant has consented to personal information only being used anonymously to detect trends and patterns, any data that identifies an individual, their home or their vehicle, must be decoupled and removed from distribution.

To create a workable and healthy ecosystem around IoT and to build useful services based on shared data, five key issues must be addressed, as shown in Figure 1:

Figure 1: Five primary considerations for building an IoT marketplace.

Data Anonymization: To protect personal privacy and business interests, aggregate data used for specific purposes within IoT solutions must be stored and used in way that it can't be linked to an individual or company unless expressly permitted. An example of anonymized data might be the collection of vehicle-travel information to help improve traffic control on city streets. (For example, how many vehicles use one particular on ramp at 7am in the morning?) Or, as another example, how many individuals are at home after dark in a particular neighborhood, which might have bearing on incidences of burglaries or theft in the vicinity.

Consent Management: IoT ecosystem participants offer consent for the use and application of data they provide in exchange for receiving a variety of services. For example, a driver may grant access to personal vehicle-operation data in exchange for receiving scoring that may lower insurance premiums or grant certain privileges. A participant may also consent to the use of anonymized data associated with a particular application or for a narrow application of data sharing; such as basic telematics data about the vehicle operation—speed, braking, travel times, lateral movement, and so on—but excluding any geolocation details for the vehicle or other commercial uses.

Usage Rights Management: The application and control of rights that have been granted through participant consent must be carried across the connected IoT ecosystem so that individual components and systems abide by the usage rights that are in force. In a complex system with multiple data sources and a variety of services involved, this can be a substantial effort. Usage rights must be maintained in an agile, accurate form using open standards available in near real-time to all authorities responsible for controlling data distribution and use. Whether through real-time push or a batch feed, data should be converted into a universal

format—consistent across all platforms—to effectively enable the range of services being offered.

Subscription Management: Data pooled and aggregated across the IoT represents a potential revenue source for organizations with the rights to grant access to that data. Whether personalized or anonymized, data acquired by an OEM automaker through a connected car has value to other organizations, such as an insurer building a program around safe vehicle operation. Subscription management provides the basis for creating subscription services around different types of data and managing all aspects of the interchange—including rights, permissions, revenue streams, and so on. Also, organizations or participants using a service that is part of an IoT ecosystem sometimes do so on a subscriber basis (for example, an insurer offering home security services based on data captured and delivered through the subscription on an annual basis). Managing the subscription information across a complex system in which a stream of data may be used as input to more than one service constitutes a key challenge within an IoT ecosystem.

Analytics: Raw data gets filtered, distilled, and interpreted as the basis of the intelligence behind the IoT. Analytics performed using the data can be used to extract trends, make projections, create scoring, detect patterns, and perform machine learning—essentially producing useful information that can be applied to whatever services are being delivered using those analytics or whatever issue is under consideration. As a part of the analytics, data collected from individual things (telematics data from cars, monitors embedded in homes, or wearable health scanners) can be combined with contextual information, such as weather, traffic, geolocation information, medical conditions, accident alerts, road construction detours, and so on, to provide deeper insights into applications of the IoT technology. All of this—use of specific data for use in the analytics programs—is dependent on the data management and rights issues being satisfactorily resolved, as described in the previous four areas.

Beyond these definitions, a number of different interpretations within each category exist. For example, anonymization often means different things to different people and different organizations. The challenge is to create a single, clear definition that functions effectively for the contributors sharing the data, as well as the agencies moving the data throughout the ecosystem. The administrators and operators of an IoT ecosystem should clearly spell out the parameters for each management concern and communicate these details to all parties and stakeholders involved within the ecosystem.

Information security is a prime consideration as well, particularly for financial institutions, security firms, and government agencies. Full security to protect user privacy and data integrity includes:

Secure Hosting Facilities: The facility in which the host servers reside should meet appropriate certifications for security and comply with all local, regional, and federal regulations that apply.

Strict Access Controls: Access to the systems and databases should be limited to assigned personnel who have undergone necessary background checks and have been authenticated for specific tasks within the secure premises.

Rigorous Protection of User Privacy: Sensitive data must be handled in a prescribed manner, isolating high-risk personally identifiable information (PII) from datasets when necessary. Encryption should be applied to data across its entire lifecycle—from acquisition to transport, and at rest—to ensure privacy protection. Compliance with global standards that apply to the privacy of personal information is also a key consideration.

Technical and Policy Challenges

A number of technical challenges exist that must be resolved to fully gain the benefits and extend the opportunities available to insurers, OEMs, and others in the Internet of Things space.

Standards and Interoperability

Vast numbers of standards complicate the means by which data get sourced, exchanged, and shared across the IoT. At this stage of development, many individual data sources have their own unique standards, making interfacing and exchange a serious challenge.

Among the leading IoT standards bodies and consortia are:

> 3GPP – Working toward mobile broadband standards and IoT interoperability.

> AllSeen Alliance – Enabling communication and interoperability among the billions of IoT devices, apps, and services.

> IEC Smart Grid Standards – Developing a standards roadmap for building a smart grid for efficient delivery of electricity.

> IEEE Standards Association on Innovation and IoT – Devising IEEE standards for building IoT-based products.

> Industrial Internet Consortium – Helping to shape and grow the industrial Internet.

> Internet of Things Consortium – Driving adoption of IoT products and services through strategic partnerships, market education, consumer research, and business development initiatives.

> IoTivity – Enabling seamless device-to-device connectivity to address the emerging needs of the IoT.

> ISO/TC 204 Intelligent Transport Systems – Standardizing information, communication, and control systems in the field of transportation.

> ITU Internet of Things Global Standards Initiative – Promoting a unified approach for development of technical standards enabling the IoT on a global scale.

> Open Connectivity Foundation – Providing the software to link the IoT devices and services (formerly the Open Interconnect Consortium).

> Thread – Creating the best way to connect and control products in the home.

Harnessing Data Effectively

The nature of the devices connected to the IoT presents numerous challenges in terms of capturing and integrating data originating from them. In some cases, data can be acquired with real-time and near real-time efficiency. In other situations, there is uncontrollable latency that impedes the effective collection and integration of data.

Users and participants of IoT ecosystems commonly expect that data will be readily available all the time and that devices will be perpetually online so that all services will be immediately accessible. Syncing and data collection, however, can be dependent on the actual device. For example, the Fitbit tracker, a useful device for monitoring personal fitness, does not communicate directly with the IoT, but attempts to sync with Fitbit.com through available connectivity links, such as a smartphone or desktop computer, at regular intervals (usually every 15 minutes). Syncing can be delayed for hours or days if no method of connecting to the base station is available. Any services that rely on this data—for example, a health insurance program rewarding positive fitness practices—must be adapted to the sporadic and unpredictable acquisition of data from the Fitbit.

Certain types of services can provide data with near-continuous access, such as connected cars that are equipped to deliver vehicle and driver data frequently, on a periodic schedule. The challenge, however, is adjusting for those data sources that introduce information at unpredictable intervals. Services based on IoT can also be affected by large bursts of data that arrive simultaneously from diverse sources in an unsolicited manner.

Agnostic Approach to Standards

In the interest of ensuring the highest levels of interoperability and broadest opportunities for data acquisition, firms engaging with an IoT ecosystem should adopt an agnostic perspective during the ongoing evolution of standards, providing support for as many prevailing standards as is feasible to support the goals of customers and subscribers.

To meet the emerging market demands, companies must stay informed of developments, including promising transport level standards, and to be prepared to adapt to changes as the market matures.

Portability of Data

The portability of device-specific data sets presents an interesting and somewhat difficult challenge. This represents more of a policy challenge than a technical challenge. Achieving portability of data from one IoT system to another can be problematic if not proactively addressed through policies. This challenge becomes less of an issue if the type of data involved shares a common backend at the server level and no porting of different kinds of data sets is necessary. Otherwise, the obstacles to using the full range of data can be significant.

For example, if a customer is using a Fitbit to provide fitness tracking data and then begins using a Sony watch, maintaining any reasonable historical record can be difficult or impossible at the moment. Similarly, a user moving from an iOS-based device to an Android device introduces problems in the continuity of data records. Porting data is an option, but many organizations working with IoT services haven't set up to ensure portability of data for these kinds of issues. This ongoing challenge needs to be met to support the very real possibility that customers will purchase and use a variety of different devices over the span of a service subscription.

The Working Ecosystem

Ultimately, when a complete, well-functioning ecosystem is built around IoT technologies, the data derived from the individual sensors and components can be combined, aggregated, repackaged, and used as the basis of an expanding continuum of new services and novel business opportunities. The beginning framework is in place and applications are already arising from this framework. OEMs are competing to find the best ways to use the built-in connectivity features in modern vehicles to draw increased consumer interest and revenue shares through subscriptions and other services. Insurance organizations are building on the successes from UBI programs to venture into programs that include data-driven home and life policies where the risk can be accurately assessed and IoT can provide additional benefits. Government agencies are leveraging advances in brought-in, plugged in and embedded vehicle technology for road-usage charging as a viable and effective means to gain revenue for equitable road taxes based on actual road usage.

The acquired data distributed and shared throughout the IoT ecosystem can also be combined with a vast array of contextual information obtained from readily available sources: weather information, road conditions and closures, airline schedules, market trends, government services, points of interest, restaurant menus, available parking slots in monitored lots, maps, construction zones, and so on. This contextual information can help provide innovative new services and enhancements to existing services. Anonymized data sources shared among participating partners can also lead to richer and more intelligent applications and specialized knowledge bases that lead to informed decision-making and guided actions.

The business value of IoT escalates as data is merged, recombined in productive ways, run through sophisticated analytics, and processed by machine-learning algorithms. Road usage charging, for example, balances the costs of maintaining a particular stretch of road against the actual use of that road by commercial and private drivers. Fees can be assessed based on real-world data and fairly distributed costs, even factoring in information such as the fuel efficiency and CO2 values levels generated by a particular vehicle type and model. Similarly, a Fitbit tracker can be combined with the telematics and route-mapping intelligence in a car, communicating to the driver, who only received 4 hours sleep the night before and who is looking at driving a 150-mile route at night, that it might be wise to find lodging and get rest at some point.

Case Study for IoT: Insurance Opportunities – Expanding the Book of Business

IoT provides opportunities to expand an insurers' book of business beyond the boundaries of UBI to include:

Auto Insurance: Capitalize on a variety of data from the connected car to offer consumers new benefits, scope risk more accurately, and tie in with other co-marketed services. Anonymized vehicle and driver data—whether delivered by an OEM or aftermarket device—can also serve as a source of revenue when fed into an analytics engine to deliver valuable information about traffic use patterns, driver behavior, factors that cause accidents, time spent driving, road usage indications, and so on. Wireless data from automobiles—managed properly—represents both

a means of risk mitigation and a prospective source of revenue. Usage-based insurance can be made richer and more intelligent with a deeper level of driver and vehicle information through IoT interconnections. The end result is greater safety for drivers and a potential discount to those whose driving behavior merits it.

Home Insurance: Provide opt-in home insurance programs that include discounts for homeowners who demonstrate—through a variety of shared data—that they are responsibly handling maintenance and care, and showing regular occupancy of the home. Home monitoring helps provide peace of mind, as well as being a means through which insurers can reward responsible practices with discounted premiums. As with the connected car opportunities, insurers can use a number of connected home devices to better assess risk and introduce new products based on information that was previously not available to them. Much of the surge of interest in the connected home has been triggered by advances in IoT technologies, making it easier for devices in the home to communicate, as well as smartphone popularity, which makes it possible for homeowners to remotely monitor and control the basic systems within the home, such as heating and cooling systems, sensors to detect water leakage, video monitors, smart appliances, security systems, and so on. Fitness tracking devices offer a means to determine the occupancy of the home at a given hour as does a geofence that determines if the homeowner's vehicle is in the garage at a certain time. With deeper insights into homeowner habits and needs, insurers can improve claims handling and perform ongoing risk assessment to improve operational efficiency and spur top-line growth.

Life/Health Insurance Solutions: Grant users who can demonstrate a positive approach to wellness and health practices—through data delivered by wearables or fitness equipment—a discount in their premiums. Participants gain encouragement in following healthy lifestyle practices and insurers can provide rewards commensurate with these behaviors. IoT technologies make it possible for an insurer to refine their business model and become a trusted advisor to customers, offering coaching and guidance to help improve their level of health and life expectancy. Technological advances are already moving beyond wearable devices for monitoring health signs to ingestible and implantable technologies, all of which can be combined and coordinated through an IoT infrastructure. To circumvent the existing stagnation within the current insurance industry, insurers need to transform and adapt to technologies that enable them to deliver highly personalized services to customers and create products that take advantage of the rich data and invaluable insights that can be gained through an IoT ecosystem.

One of the keys to effective risk mitigation and innovative product introductions for insurers is the capability of collecting and correlating data from numerous sources, including vehicles, homes, and individuals. For example, in the connected car sector IoT technology can link and connect a wide range of data sources to generate feedback to the driver, as well as assess the state of the vehicle, as shown in Figure 2.

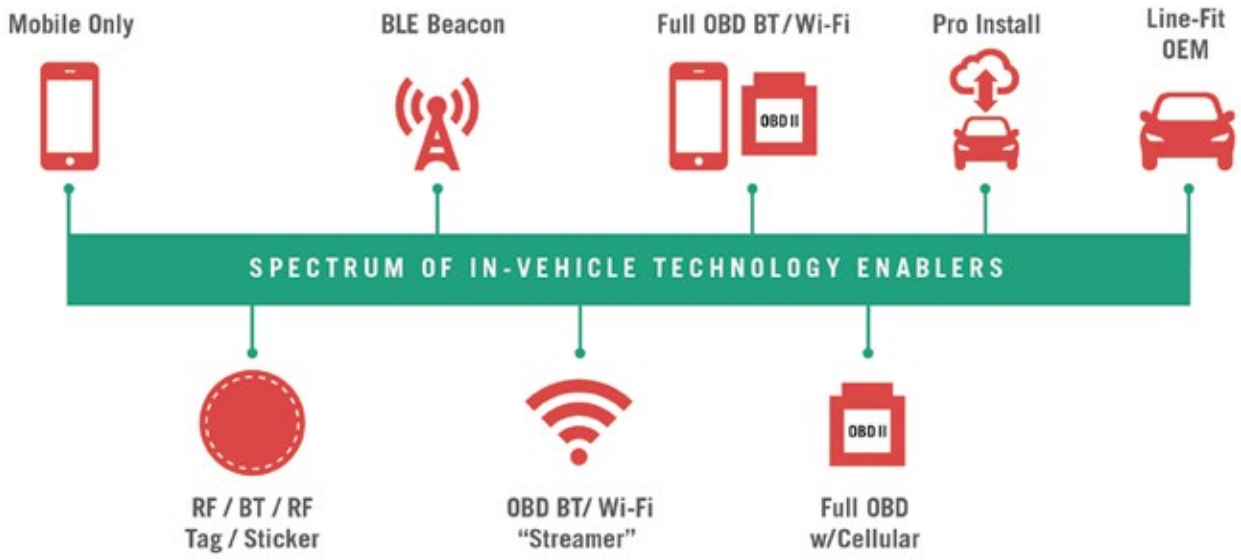

Figure 2: Access to multiple device types to derive intelligence.

Example: Life Insurance Discounts Based on Fitness Tracking

As part of a special program designed to re-energize life-insurance sales, John Hancock (a division of Canadian-based Manulife Financial) offers discounts to participants who agree to provide personal fitness information in exchange for access to medical information and data collected by a Fitbit tracker, which is provided free to users. The Fitbit is configured to deliver data about activities directly to the insurer. Discounts up to 15 percent of insurance policy costs can be obtained for those who demonstrate healthy practices and stay within certain ranges of health indicators, including blood pressure readings and cholesterol levels.

With the Internet of Things presenting enormous opportunities for insurers, these organizations are advised to seek a partner with the skills and expertise to help identify the best areas for profitable growth, avoid the potential pitfalls associated with newer IoT technologies, and provide a stable platform for data exchange and use across multiple data sources and a multitude of data providers. A well-managed IoT ecosystem must be in place to make all of this happen—to bring together the necessary data sources, rights managements, and interoperability across diverse systems to make IoT work. Achieving success in this dynamic market sector will require careful examination of the benefits and challenges, as well as an experienced guide and knowledgeable partner to identify the paths that offer the best value and least risk.

Case Study: OEM – The Promise of the Connected Car

Automakers are in the midst of a tremendous competitive race to take advantage of digital services as a differentiator in the market. The connected car—linked to the Internet continuously and wirelessly—provides access to a number of automated links to other connected objects and devices, increasingly available as the IoT technologies proliferate across industry sectors. Communication through a connected car can encompass traffic lights, other vehicles, emergency responders, smartphones, geolocation systems, entertainment

providers, and many other "things." According to Analsys Mason, by 2024, 89 percent of the automobiles sold globally will include embedded connectivity. Features will include built-in Internet connectivity and mechanisms for monitoring vehicle operation, detecting faults, and providing value-added services, from entertainment to accident avoidance and mapping.[3]

In the Connected Car Study 2015[4], published in September of the same year, the authors stated: "Both premium and volume automakers clearly see connected car technologies as essential to their futures. They also realize that overall vehicle prices aren't rising as rapidly as the prices charged for digital capabilities. This means returns on investments in traditional car components are shrinking. Over the next five years, the connected car could disrupt the entire automotive ecosystem."

One way for automakers to derive revenue from the data associated with built-in telematics and Internet connectivity is to commercialize the data itself. By sharing information about the driver and the vehicle operation, a range of services and enhancements becomes available. Possibilities for extended services are not just limited to the OEM, but are available to other industries inside and outside the automotive ecosystem.

Given that OEMs have been losing revenue from digital subscriptions recently, third-party applications based on commercialized data could offset these losses. To contend with the potential risks around this approach, these considerations should be addressed:

Ensure Transparency: Make drivers aware of the program and be sure that they understand they are receiving connectivity in exchange for providing certain kinds of data.

Provide a Process for Consent Management: Once the driver is aware of the program boundaries, implement a process to verify driver consent to the ongoing use of the data. Include descriptions of the types of information being accessed and the purposes for which this access is being granted.

Protect Privacy: All data derived from the driver and vehicle operation must be protected based on prevailing local, regional, and federal privacy regulations.

Architect Built-in Security: Emphasize end-to-end security for all devices and systems connected to the IoT as part of a program, with adherence to current industry practices. OEMs considering commercializing data in this manner will need to know how much of the effort to implement this will be their responsibility and whether hardware or software changes will be required. Some assurance of the scale and scope of revenue opportunities is also a key consideration. Many companies struggle today to obtain reasonable business value from transactional data that they have generated and acquired. The challenge is to link and exchange this data across multiple platforms, a substantial effort that requires partners and a supporting ecosystem.

The Boston Consulting Group[5] in a report titled "Insurance and Technology: Evolution and Revolution in a Digital World" noted that a rise in digital ecosystems is occurring as companies seek ways to extract value from data. They define such an ecosystem in these words:

3 2014. "Connected cars: worldwide trends, forecasts, and strategies: 2014 – 2024." Analsys Mason. http://www.analysysmason.com/Research/Content/Reports/connected-cars-forecast-Jun2014-RDME0/

4 Vierecki, Richard, et al. 2015. "Connected Car Study 2015: Racing ahead with autonomous cars and digital innovation." Strategy&. http://www.strategyand.pwc.com/reports/connected-car-2015-study

5 Hocking, Jon, et al. 2014. "Insurance and Technology: Evolution and Revolution in a Digital Word." The Boston Consulting Group. http://www.the-digital-insurer.com/wp-content/uploads/2014/10/372-evolution-revolution-how-insurers-stay-relevant-digital-world.pdf

"A digital ecosystem is a network of companies, individual contributors, institutions, and consumers that interact to create combined services. In consumer-oriented digital markets, ecosystems are enabled by a standard technical platform (say, an operating system or an app store) that connects devices, applications, data, products and services across the value chain. The platform allows components in the ecosystem to work together more easily than if the individual products operated alone—this can create a new market for products and services that do not exist yet."

IoT provides the mechanism and foundation for such an ecosystem, making it possible to construct a data exchange hub fueled by intelligence and analytics.

Example: Road Usage Charging

Road Usage Charging (RUC) offers a balanced way for governments to meter vehicular use and collect revenue based on actual metrics, vehicle by vehicle. This service, deployed by IMS in a number of regions, is expected to increase dramatically in the near future. One deployment in Oregon has proven successful and IMS is working with a number of state governments and federal agencies to expand the service into new areas. A new pilot project is being initiated in California to further advance this approach. The same in-vehicle technologies and sensors used for road-usage charging can also be leveraged by insurers to offer UBI programs, and by automakers to offer connected car and dealer-based services.

Additional Examples

IoT technologies and an ecosystem that unites companies that share data across a managed infrastructure provide a means to deliver personalized services to clients and customers, tailored to their needs and preferences. With more extensive data-sharing across an IoT ecosystem, these are some of the possibilities of combining different sources of data to create insightful actions:

Supplementing health and fitness data: The prior example of Manulife collecting fitness data primarily through a Fitbit tracker could be enhanced. For example, if a geofence was created around the user's local gym and relayed information from his or her vehicle as to how many times the individual visited the gym each week. Or, if an individual is dealing with a chronic illness, such as diabetes or high blood pressure, a wearable could provide guidance and tips over the course of a day to help improve vital health signs, and suggest meals, encourage exercise, or deliver other informed advice.

Enhancing Safety and Convenience in the Home: As more and more systems are connected together with IoT technology, opportunities arise for convergence and intelligent enhancement of daily routines, leading to improved safety, healthier habits, and informed travel. For example, an intelligent clock connected with your entertainment system could assess current road conditions and weather, wake you up at a time that allows you to comfortably get ready for work, and then give you a morning report during breakfast that warns of icing conditions during the commute or accidents that may impede your travel or cautions based on the current weather forecast. This kind of information could lower accident risk and reduce stress levels during the morning commute.

Early Warnings of Home Issues: An interconnected array of monitoring devices communicating with a personal wearable device or smartphone could help deal efficiently and intelligently with problems that occur in the home during the day. For example, water sensors could indicate that flooding is occurring in a particular room, check the location of family members against trackers or appointment calendars, notify the closest person to respond or, if no one is nearby, select a registered service with access permission to the home through a security token, and simultaneously contact the insurer's response team of the problem.

Preventing Theft: A combination of intrusion sensors, video monitors, and home occupancy information could be connected over the IoT to provide alerts, safety warnings, and other notifications—assessed intelligently using analytics—to dramatically reduce the incidence of theft. Homeowners could be alerted automatically by smartphone if they're getting in bed at their normal time to retire and the garage door or a downstairs window has been left open.

Moving from Connected Cars to Intelligent Cars: A steady trend toward automated driving has resulted in self-parking vehicles, self-braking, cruise control speeds linked to current road conditions, and automatic accident avoidance systems. We're on the verge of seeing car-to-car communications that can adjust speed and position for maximum safety, and autonomous vehicles that let drivers completely relinquish control of the vehicle. These types of systems can be connected in imaginative ways, cutting accident risk, reducing driver stress and tiredness during lengthy travel, adjusting travel routes based on personal calendars and current traffic conditions, automatically reserving parking at destinations before arriving, and, generally, making travel a better experience. Beyond the insurance discounts possible from using proven safety systems, insurers can use IoT connectivity to offer value-added services—competitive differentiators—that make travel more pleasurable and rewarding for drivers and their passengers.

Personalization of services, real-time risk assessment, and innovative business models are the keys to profitability for insurers struggling with current industry conditions. IoT technology offers abundant opportunities to provide significant support in each of these areas.

About IMS

Intelligent Mechatronic Systems Inc. (IMS) is a leader in connected car technology that enables drivers to be safer, smarter, and greener. IMS is well positioned with the requisite knowledge and insight to work closely with insurers and automakers around the world and also has the direct experience and deep expertise to help craft strategies in support of IoT and connected car programs. IMS is prepared to assist insurers and automakers with the necessary facts and figures to guide them through all stages of a successful program deployment. For more information about IMS, visit www.intellimec.com/about

About IMS IoT Marketplace

By establishing an open platform for the kinds of data exchanges that underlie home operations, automotive travel, and personal lifestyle choices, IMS is enabling an IoT marketplace (Figure 3) and collaboratively engaging with industry leaders, partners, and participants to help shape the advances in IoT. The creation of programs and initiatives around IoT will generate revenue opportunities that can bring value and business growth to all those involved with this exciting technology.

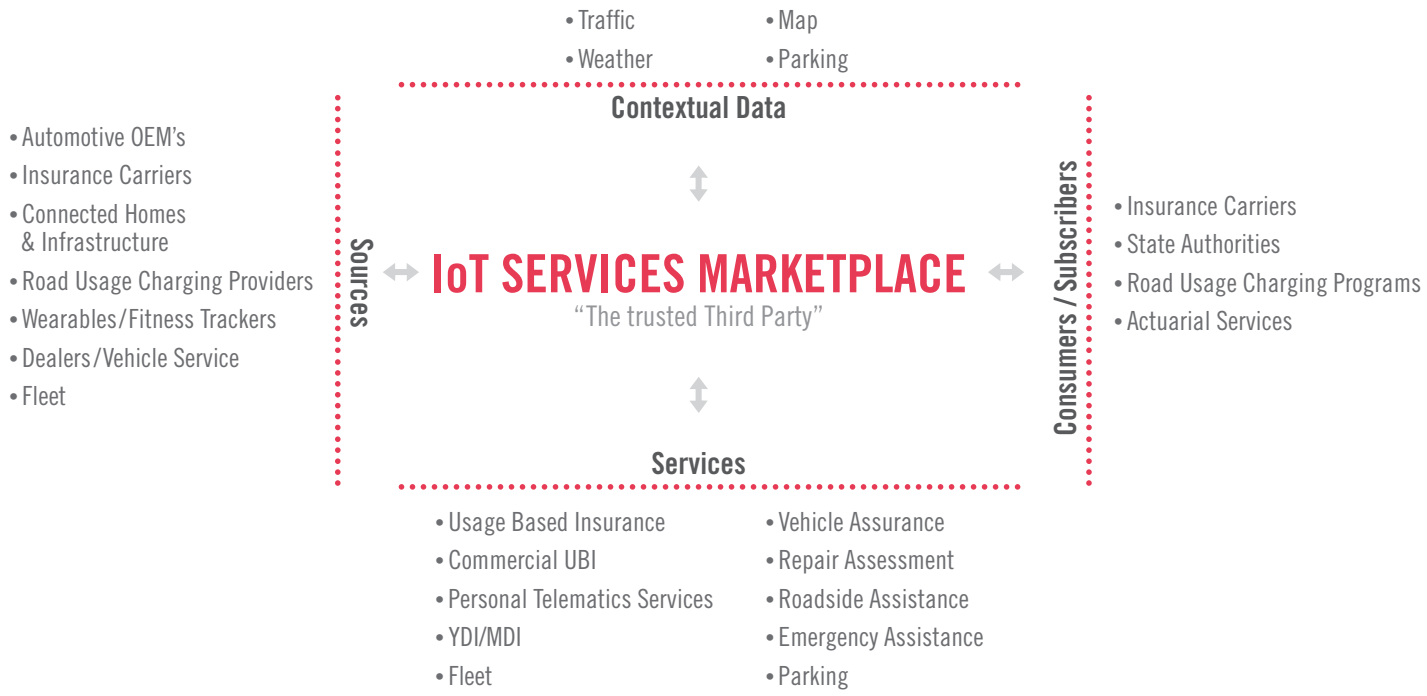

Figure 3: The IoT Marketplace serves as an ecosystem builder.

The IoT Marketplace provides a centralized hub supporting the licensing of data sources. For example, data sources from a road usage charging program could be licensed to an insurer offering commercial or personal lines UBI programs. This provides greater value to the end user, using data captured from a single source. Companies partnering with IMS can harness and exchange a vast array of data without dealing with the complexities of creating or maintaining the vast infrastructure that makes this possible.

To learn more or to become a partner in the IoT Marketplace, visit: www.intellimec.com/iot