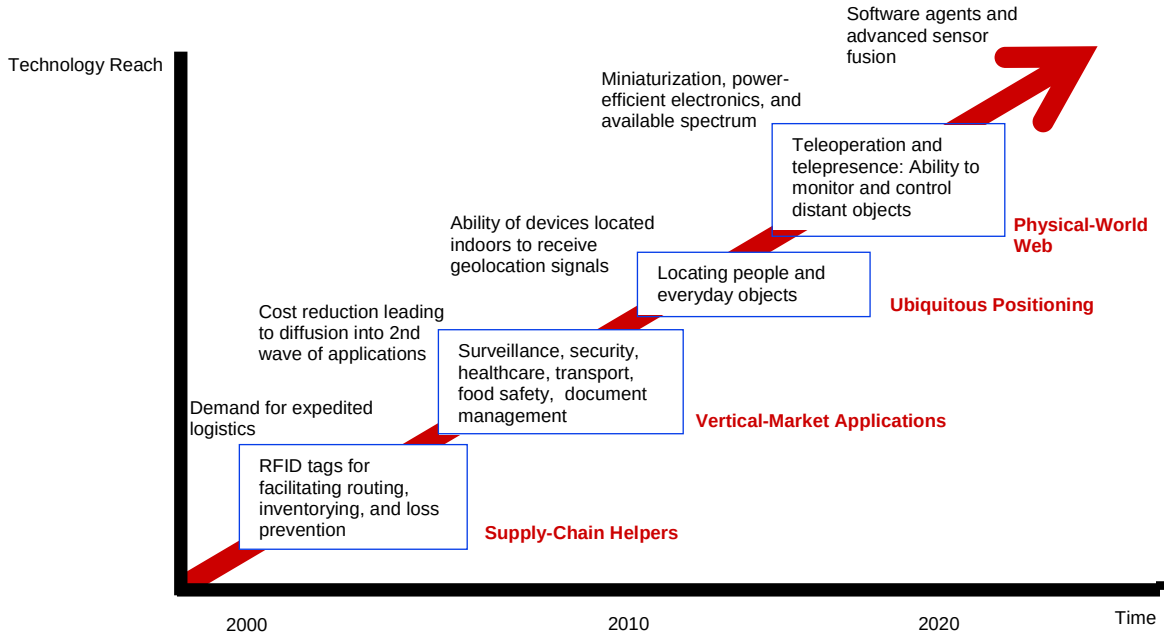
APPENDIX F: THE INTERNET OF THINGS (BACKGROUND)

The Technology

Figure 15[1]
TECHNOLOGY ROADMAP: THE INTERNET OF THINGS



Source: SRI Consulting Business Intelligence

The Internet of Things

The term Internet of Things appears to have been coined by a member of the RFID development community circa 2000, who referred to the possibility of discovering information about a tagged object by browsing an Internet address or database entry that corresponds to a particular RFID. Since that time, visionaries have seized on the phrase "Internet of Things" to refer to the general idea of things, especially everyday objects, that are readable, recognizable, locatable, addressable, and/or controllable via the Internet—whether via RFID, wireless LAN, wide-area network, or other means. Everyday objects includes not only the electronic devices we encounter everyday, and not only the products of higher technological development such as vehicles and equipment, but things that we do not ordinarily think of as electronic at all—such as food, clothing,

[1] The Technology Roadmap highlights the timing, features, and applications of significant technology milestones that would be necessary for developers of this technology to achieve if successful (equivalent to commercial) application—and possible disruption—is to occur by 2025.

and shelter; materials, parts, and subassemblies; commodities and luxury items; landmarks, boundaries, and monuments; and all the miscellany of commerce and culture.

Although analysts define the IoT in terms of connected everyday objects, the nature of the connection remains to be determined. A two-way connection by means of the Internet Protocol constitutes the ideal case, but the originators of the IoT concept appear to have emphasized a simpler model of RFID query and response. The IoT will be inextricable from sensor networks that monitor things but do not control things. Both connected everyday objects and sensor networks both leverage a common set of technological advances toward miniature, power-efficient sensing, processing, and wireless communication. Analysts commonly describe two distinct modes of communication in the Internet of Things: thing to person and thing-to-thing communication.

- Thing-to-person (and person-to-thing) communications encompasses a number of technologies and applications wherein people interact with things and vice versa, including remote access to objects by humans, and objects (sometimes called "blogjects") that continuously report their status, whereabouts, and sensor data.
- *Thing-to-thing communications* encompasses technologies and applications wherein everyday objects and infrastructure interact with no human originator, recipient, or intermediary. Objects can monitor other objects, take corrective actions, and notify or prompt humans as required. Machine-to-machine communication is a subset of thing-to-thing communication; but machine-to-machine communication often exists within large-scale IT systems and so encompasses things that may not qualify as "everyday objects".

Many everyday objects already incorporate embedded microcontrollers and will increasingly include wireless interfaces. Typical microcontrollers incorporate a microcomputer, storage, software, and interfaces for sensors and actuators that can reside aboard everyday objects. With addition of a network interface, people and machines can monitor and control such objects from a distance, via the Internet. Objects containing sensors can interconnect with one another and can be monitored by distant servers or people. Software that resides in servers and/or Internet-connected objects can initiate a sequence of events, with or without human intervention. The combination of embedded microcontrollers, sensors, actuators, network interfaces, and the greater Internet makes it possible for the Internet to evolve from an network of interconnected computers to a network of interconnected objects. Such objects may or may not have their own Internet Protocol addresses.

Developers and visionaries have described a number of concepts that are distinct yet closely related to the IoT.

- *Sensor networks* need not be connected to the Internet and indeed often reside in remote sites, vehicles, and buildings having no Internet connection. Smart dust is a term that some have used to express a vision of tiny, wireless-connected sensors; more recently, others use the term to describe any of several technologies that range from the size of a pack of gum to a pack of cigarettes, and that are widely available to system developers. One may think of the vision of tiny instances of smart dust as a

development that will arise after a long period of IoT evolution, during which a number of disruptions are foreseeable well before usable wireless sensors shrink to the size of gravel.

- *Ubiquitous positioning* describes technologies for locating objects that may reside anywhere, including indoors and underground locations where satellite signals may be unavailable or otherwise inadequate.
- *Biometrics* enables technology to recognize people and other living things, rather than inanimate objects. Connected everyday objects could recognize authorized users by means of fingerprint, voiceprint, iris scan, or other biometric technology.
- *Machine vision* is an approach to the IoT that can monitor objects having no onboard sensors, controllers, or wireless interfaces. For example, some developers propose that cameras on typical cell phones can capture images of objects; using image-processing algorithms, distant servers can identify such objects and report information about them. In other words, machine vision could be a channel for delivering the same type of information that RFIDs enable.

These and other developments are further described below under Synergistic Technologies. In fact, connected objects can have a range of capabilities--ranging from an object that merely contains a machine-readable identification, through objects that can determine their own location, through objects having a high degree of autonomy, such as the unpiloted military vehicles that DARPA has challenged the technology community to build. Generally, no sharp dividing line exist between IoT and many other Internet-related developments. Just as the Internet itself blurs boundaries among devices, people, organizations, and national boundaries, the IoT blurs boundaries between IT and objects that we do not ordinarily think of as IT.

The Enabling Building Blocks

Progress in the following technologies will contribute to the development of the IoT:

- *Machine-to-machine interfaces and protocols of electronic communication* set the rules of engagement for two or more nodes on a network.
- *Microcontrollers* are computer chips that are designed to be embedded into objects other than computers.
- *Wireless communication* is familiar to most people in the developed world. Many different wireless technologies have the potential to play important roles in the IoT including short-range and long-range channels; as well as bidirectional and unidirectional channels. Wireless devices identify themselves; in practice virtually all wireless Internet devices contain unique identifiers, including all cell phones and Wi-Fi clients. However, see the next bullet.
- *RFID technology* resembles an electronic barcode that a reader device can detect even without line of sight. Some RFID readers can identify multiple objects concurrently. And some RFID tag-reader architectures support security features such as requiring a human operator to input a challenge code before decoding an ID. RFID have varying sizes, power requirements, operating frequencies, amounts of rewriteable and nonvolatile storage, and software intelligence; ranges vary from a few cm to hundreds

of meters. However, larger devices having an internal power source tend to operate at longer ranges; conversely, smaller devices having no internal power source (RF engineers say they are illuminated by the reader device, much as a radar illuminates a target) tend to operate at shorter ranges. Also, architectures that support more storage, rewriteability, and processing tend to cost more than simpler architectures.

- *Energy harvesting technologies* capture small but usable amounts of electrical energy from the environment. Current energy-harvesting R&D concentrates on adventitious temperature variations, ambient sound and vibration, and ambient RF. Unlike passive RFIDs, which simply resonate when illuminated, an energy-harvesting transducer produces electrical power that runs a microcontroller, sensor, and/or network interface in whole or part. Technically, energy harvesting transducers respond not only to adventitious sources but also to intentional transmissions of power, say, via RF and acoustic channels. A dramatic example of intentional transmission of power via RF channel: MIT's recent "Witricity" demonstration of closely-coupled resonators, enabling relatively efficient wireless power transfers over a distance of a few feet.
- *Sensors* detect changing attributes in the environment and report them to a system; sensor networks aim to exploit the benefits of sensing at more than one location. Sensors are a type of transducer that must produce the miniscule amount of power required to convey information at a usable error rate. Sound, light, atmospheric conditions, vibrations, and other environmental signals are all fair game for sensor designers.
- *Actuators* detect an incoming signal and respond by changing something in the environment. For example, a relay is an actuator that toggles a mechanical switch, and can thus cause a good number of responses to occur such as enabling illumination, heating system, audible alarm, and so on. Actuators such as motors, pneumatics, and hydraulics can move objects and pump fluids.
- *Location technology* helps people and machines find things and determines their physical whereabouts. Sensors play a role in dead reckoning, but that approach does not satisfy practical needs for geolocation, resulting in the rise of wireless approaches including GPS (which is often augmented by other signals) and cellular towers. Fixed or orbiting transmitters have known locations. They broadcast timing signals, and receiving devices triangulate by calculating the amount of delay from each transmitter. Radar, lidar, and sonar can detect relative locations of things, depending on their electromagnetic, optical, and acoustic properties. And some things transmit their own radio, light, and/or sound in order to disclose their whereabouts to people and machines.
- *Software* comprises a broad domain of development. Development of the IoT will rely on many dimensions of software capabilities including distributed execution, self-describing data structures, and more. No theoretical framework exists to circumscribe the limits of software development, leading to speculation about software that emulates human reasoning and performs tasks on behalf of people. Regardless of the merit of long-awaited artificial intelligence, software will no doubt help future users make sense of complex data sets collected from networks of everyday objects and sensors.

Implications of Advancement in Various Technological Capabilities

Ideally, the following use cases could be common in ten to fifteen years. To complete shopping in bricks-and-mortar retail stores, customers could simply walk through doorways to check out, debit accounts, and receive e-receipts that they can inspect via the displays on their cell phones. A soldier could rapidly learn how to perform a maintenance procedure by scanning an item of equipment using a handheld device and reading the device's display. Handheld devices could become not only information sources but universal remote controls for the environment—user interfaces for engaging lights and appliances, locating misplaced and loosely-organized objects, diagnosing problems with systems, and controlling tele-operated objects from greater or lesser distances.

Using machine-to-machine communication, objects could collaborate with one another to perform actions on behalf of people and reduce or eliminate need for human labor. Vehicles that communicate wirelessly with each other can collaborate by "refusing to crash". Entertainment systems can sense and respond as users walk through a house, transferring the baseball game from living room to kitchen to garage. A medicine cabinet fitted with RFID reader and an array of weight sensors could detect when someone does not remove a pill as prescribed and respond by alerting the patient; alternatively, the cabinet could detect when the supply of a particular pill runs low, automatically renew a prescription, or make a medical appointment. Buildings can optimize energy savings, indoor air quality, and comfort by adjusting climate-control systems to account for the number of people passing through entranceways, readings of oxygen sensors in walls, data from rooftop weather stations, and national weather services.

Ever smaller, cheaper, and smarter systems have the potential to augment evermore everyday objects. Note that typical microcontrollers (although not all of them) can be reprogrammed, and this reprogrammability accelerates the ability of systems to evolve. Once an object has a network interface, its abilities can improve at the speed of software development: Progress is not limited to the speed of hardware and infrastructure deployment. Capabilities of software updates promise to evolve toward processes that resemble reasoning. For example, researchers aim to develop systems that adapt messages to the present network, device, user, and context. Some users may perceive such adaptation to be "intelligent"; but researchers hope to implement algorithms that come ever closer to emulating human reasoning to make sense of complex data sets. One promising approach to the latter goal relies on computational semantic algorithms that operate on self-describing data structures.

Significantly, synergies among Internet-connected objects will arise, yielding capabilities that designers will not have anticipated. Smart buildings could prove to become a network for collecting fine-grained weather data. Home- and office-security systems could double as ad hoc wireless network infrastructure. Many everyday objects could serve as nodes for collecting data that's useful to businesses; an open market in usage data could support the launching of advertising messages; such an open market in information could equally enable surveillance by law enforcement agencies and exploitation by enemies of the United States.

Synergistic Technologies

The following are some of the technologies that may not be essential to the development of the IoT, but could extend the scope of the IoT. These technologies may be synergistic in the sense of adding value to the IoT; but they may also be antergistic or counterproductive in the sense of aggravating risks attendant to the IoT.

- G*eotagging/geocaching.* Geographic information systems play roles in locating things. But they play other roles, too, and thus comprise an independent domain of technology development. An Internet of Places can arise as evermore systems recognize where they are and can access GISs. Such GISs can include ad hoc contributions, control physical access according to different privilege levels, calculate social-networking metrics described above, and more.
- *Biometrics*. Systems can identify individuals for security and other purposes. Identification combined with databases of information about persons could itself have synergies with personal geolocation, enabling an Internet of People.
- *Machine vision.* Image recognition could evolve toward characterizing things' behaviors, not just their identities. In some cases, machine vision may be perfectly adequate for identifying things in the IoT, obviating need for RFID tags.
- *Robotics.* Connected everyday objects and sensor networks are key enabler for robots. Onboard wireless communications may be critical for interconnecting robot subsystems. And robots may need to monitor and control the IoT just as people do.
- *Augmented reality.* Researchers aim to enable systems to report context-sensitive information when people come into proximity with other people, places and things. Such information could appear on cell phone displays, wearable near-eye displays, head-up displays in vehicles, or using other convenient means.
- *Mirror worlds.* Electronic media—whether a simple display or a complex virtual-reality platform—can help people visualize distant events and situations. Software can use icons and other abstractions to help people visualize the locations of real-world objects. Military commanders and first responders may find value in such situation displays. Objects including vehicles, personnel, and equipment can self-report their location to a database. Various types of sensors, machine vision, and other technologies can detect objects that don't self-report.
- *Telepresence and adjustable autonomy.* Persons at a distance can access information gathered by an object and can control the actions of distant objects. From one moment to the next, distant objects can vary which functions are under control of a distant human user, and which are under local machine control as required.
- *Life recorders and personal black boxes.* Some wearable devices continuously capture and store lifesigns, sounds and images, routes traveled, and other user experiences. Current applications include health-care research, but personal black boxes could have value in fitness training, encouraging workplace safety, storing personal memories for productivity purposes, and social networking ("life blogging"). A common set of technologies may apply to monitoring people and things.

- *Tangible user interfaces.* People can control technology by manipulating everyday objects rather than being limited to using keyboards, mice, displays, and dedicated control surfaces. E.g., DGT Projects' RFID chessboard tracks the motion of chesspieces; as a player moves, displays automatically update to communicate with a distant user or nearby audience. Another example: The IO Brush, (the result of a research project conducted at MIT) resembles a normal paintbrush but contains a digital camera and network interface. The user can points the brush at any object to capture a desired color; when the user applies normal brushing gestures at a suitable display, a computer simulates the appearance of a brushstroke. TUIs use natural behaviors to control systems. In theory, machine vision and other sensor systems could detect gestures involving unprepared objects, enabling people to use any object to control any other: An electric shaver could activate a coffee maker; a key in a lock could deactivate an alarm and activate a thermostat; removal of a gun from a safe could initiate a call to the police or a security service.
- Clean technologies. Embedding electronics in everyday things will be associated with increased e-waste, as in the case of an RFID tag embedded in an aluminum can. Even renewable technology could be associated with e-waste, as in the case of a solar cell that powers the connection for a pet collar. Society may bring to bear the technologies of reuse, recycling, and remediation to address an e-waste problem that will emerge with an IoT.

Applications

Key Uses and Instantiations of the Internet of Things

Commercialization and adoption by government organizations is key to enabling progress in development of the IoT.

- *Retail and logistics.* Emergence of RFID applications depends strongly on adoption by retailers, logistics organizations, and package-delivery companies. In particular, retailers may tag individual objects in order to solve a number of problems at once: Accurate inventorying, loss control, and ability to support unattended walk-through point of sale terminals (which promise to speed checkout while reducing both shoplifting and labor costs). Cold-chain auditing and assurance could require tagging food and medicine with temperature-sensitive materials and/or electronics; assuring or monitoring whether perishable materials are intact and/or need attention may entail communications among things, refrigeration systems, automated data logging systems, and human technicians.
- *Product management.* Product managers are concerned with the marketing of products and the maintenance of brands. They strongly influence product attributes and responses to ad hoc market problems ("issues management"). An IoT promises to a be a key tool for product managers who want to accomplish several goals: Differentiate from competitors (or keep up with competitors that have used the IoT to innovate); create new channels for marketing messages and new ways to engage customers; track usage of products; and use software to add updated capabilities to products, monitor performance against warranties, and fix bugs.

- *Surveillance.* Emergence of applications of sensor networks depends on adoption by law enforcement, military, border patrol, customs, private security, and other security-minded organizations. Analysts often cite the potential for vibration sensors distributed along national borders to form an effective "virtual fence" that replaces the need for a costly yet still breech-able physical fence.
- *Smart buildings and green buildings.* The IoT could arise in part due to efforts to enhance comfort, convenience, and security, and to reduce energy costs and environmental impacts. Initially, IT is migrating into other technological features of residential, commercial, industrial, and government buildings including alarm systems, access controls, indoor climate controls, elevators, and so forth. These developments set the stage for diffusion of IT into illumination, appliances, and furniture; and for distant PCs and cell phones to offer remote access to sensors and actuators in buildings
- *Telematics.* Efforts to improve transportation promise to drive progress toward an IoT. Onboard diagnostics, safety systems, communications systems, comfort controls, entertainment electronics, driving assistance, and systems that enhance fuel efficiency have already driven progress in sensors, sensor networks, embedded microcontrollers, geolocation, and other technologies that support the IoT. Notably, wireless tire-pressure monitoring systems which NHTSA and a U.S. court has mandated for light vehicles sold after 1 September 2007) appear to be the first instance of a wireless sensor network that will be connected to pervasive everyday objects (tires); and significantly, emerging and future batteryless tire-pressure monitoring may commercialize energy-harvesting technologies for mass markets, thereby reducing cost of such technologies and enabling their use in other automotive and nonautomotive applications.

Current Affected Products and Services

Today, the population of Internet nodes is dominated by personal computers, cell phones, rack-mounted servers, and switches that reside in communications infrastructure. Beyond devices that exist specifically for information and communications purposes, a few other categories of network-connected objects exist—notably, a great many point-of-sale terminals in retail stores. However, a number of niche markets exist for other Internet-addressable (and otherwise networked) devices including entertainment systems, navigation devices, vending machines, security systems, industrial equipment, medical imagers, and more. And precursors exist for network-connected everyday objects including golf balls, dog collars, appliances, furniture, shopping carts, TV remote controls, and more.

- *Dot codes and other two-dimensional printed identifiers* on real-world objects and places can stimulate cellphones to automatically perform actions such as displaying an informational message, connecting to a Web page, completing a contest entry form, playing back a music sample, or responding in another way.
- *iPot* consists of a teapot appliance with a bundled Web service. iPot is available commercially in Japan. A caregiver receives messages regarding use or nonuse of the pot and can check a Web site to monitor use over time. A caregiver can be assured that a person under care is keeping to their regular tea-drinking habits; alternatively, if a

person under care fails to prepare their routine tea, the caregiver receives notification and may check up on the person under care.

- *Onstar Remote Diagnostics* is a feature of the subscription-based Onstar telematics service. Onstar relies on a cellular radio embedded in a vehicle dashboard. Onstar subscribers who own a late-model GM vehicle receive email notification when a car needs attention. Such a subscriber can also visit a Web page that presents the most recent information that GM downloaded from the vehicle. Also, some reports indicate that GM can update the Onstar software via the cellular channel. On a related note, audiences can view the status of racing vehicle dashboard instruments by browsing the NASCAR Web site during a race.
- *Electronic signs and indicators* increasingly connect to networks so that distant parties can modify messages. In addition to networked advertising signs, so-called ambient displays (such as the multicolored orbs sold by Ambient Information) indicate many kinds of information including weather, traffic, stock-market conditions, and more. And emerging indicators for homes and businesses present energy use and energy price information that they gather from utility meters and the Internet.
- *Security sensors* in some cases convert everyday objects into instruments for information gathering. Specifically, wireless sensors report when doors and windows open and close and when pipes freeze or leak. Not only organizations but some households use door sensors, for example so that parents can automatically receive a message indicating that children have returned from school. In addition, antitheft systems such as Lojack help police locate stolen cars. When a stolen notebook PC containing software from CyberAngel connects to the Internet via a Wi-Fi hotspot, the PC notifies the company of its whereabouts, based on a GIS compiled by another startup, Skyhook Wireless. Certain police, military, and hunting dogs wear GPS receivers and RF transmitters that allow handlers to monitor animals' locations. (Of course, various ordinary-appearing objects also contain surreptitious surveillance capabilities, such as a pair of eyeglasses with built-in wireless camera, and a pen with built in wireless audio transmitter.)
- *Object-location capability* for misplaced and loosely-organized items exists in various forms. Organizations that provide good Wi-Fi coverage—across the area of, say, an industrial park—can track locations of notebook PCs and other property, materials, and persons that have a Wi-Fi tag such as those provided by AeroScout, Ekahau, PanGo, and WhereNet. Radar Golf sells a golf ball locating system that reportedly works over a range of some 10 to 30 meters. And various devices help people find keys, remote controls, pets, and so on. Typical key-finder devices cause a key fob to emit an audible alarm when paged. Better solutions indicate direction, such as left or right, upstairs or downstairs. An available approach to increasing location range, reporting absolute position, and supporting many tag devices relies on UWB (ultrawideband) wireless technology. Ubisense targets its UWB platform to industrial users such as warehouses. Users install a pair of reader devices, e.g. on opposite walls of a storage area. When a user wants to locate an object, the readers transmit a 2.4 GHz telemetry signal to tag, which responds with a unique UWB code. The two readers collaborate to estimate the location of the UWB tag after detecting the geometric angle of arrival of the UWB signal, as well the delays between sending and

receiving a signal. Ubisense claims that the system supports thousands of tags that have a 5-year battery life, and can locate tags to within 15 cm of true position at a range of 160 m.

- *Car probes* currently provide traffic reports. Although cars contain much information and communication technology, they differ from computers and telecommunications equipment because cars remain first and formost objects for transporting people. Efforts to relieve congestion and its annoyances have led to the emergence of cars that report traffic conditions to other cars. Fleets of car probes now exist in several nations including France, Japan, and the United States. In some cases, especially in the United States, cars used as probes have Internet addresses. Also, in some cases, roadside sensors detect the flow of cars that have RFID-based toll-collection tags, and this data contributes to traffic reports; often, drivers download such reports from the Internet.
- *Automated metering.* Increasingly, utility meters rely on machine-to-machine communication, eliminating need for a human meter reader and allowing fully automated billing, billing according to time of use, and billing according to network status (e.g., with prices rising and falling according to peak and trough usage).
- *Evapotranspirative irrigation.* Weather-forecasting infrastructure collaborates with in-ground sensors and irrigation-control software. The irrigation system engages based on intelligent decisions involving the level of moisture in soil and likelihood of precipitation. While evapotranspiration technology is probably most common in agriculture, systems are available for commercial and residential landscaping.

New Capabilities Created by the Technology

Here are some of the more prominent application areas for the IoT:

- *Cell phones as "windows on everyday things".* Handheld devices can display information about objects tagged with barcodes and RFID tags, and camera phones can collaborate with distant servers to identify untagged people, places, and things by means of machine vision. A phone could give details about the product including its attributes, origin, price, warranty, reviews, and user manual, as well as where to buy it and how to recycle it; the identify of a person; and foreign-language details about a place such as a restaurant or historical site. Users might come to feel that such information is as vital as today's World Wide Web.
- *Cell phones as "remote controls for the environment".* Cell phones already find common use in Japan as payment channels for checking out or retail stores, and occasional use worldwide as remote controls for audiovisual equipment. Handsets can further evolve into a means for controlling nearby and distant things such as door locks, security systems, lights, appliances, and office equipment.
- *Continuous monitoring and measuring.* Commoditization of sensors and networks will enable everyday objects to be channels for surveillance, consumer surveys, measuring environmental-quality benchmarks, and any other continuously changing dimension of the world that people find valuable to track.
- *Locating things.* Miniaturization, ability to work in indoor locations, and other technological advances promise to increase the variety of things that can report their locations to owners, including keys, wallets, eyeglasses, jewelry, and tools. As an

intermediate step between today's location capabilities and these future applications, animal-locating technology promises to become practical and affordable for typical farmers and pet owners

- *Loosely-organized things.* Ability to locate objects as required could lead to changes in paradigms for warehousing, filing, and household storage, away from the tradition of "a place for everything and everything in its place". When a cell phone RFID reader is the ultimate arbiter of where something resides, business, government, military, and individual approaches to storage will change.
- *Prognostics and just-in-time maintenance for vehicles and machines.* Continuous monitoring promises to enable a new paradigm in vehicle and machine maintenance. Rather than conducting maintenance at specified intervals, organizations may be able to conduct maintenance as needed. Fluid-level and contamination sensors can tell technicians when fluids need to be replenished; and microphones embedded near rotating parts can detect sounds that indicate excessive wear. Sensor readings combined with service records enable creation of predictive-maintenance databases; algorithms could trigger custom schedules that concurrently improve reliability and reduce the cost of regularly-recurring maintenance. Such algorithms would aim to provide not only after-the-fact diagnoses but "fixing problems before they occur". During an emergency, responsible parties could use algorithmic prognoses to select only that mothballed or marginally-maintained equipment that is most likely to accomplish a desired task. Thus, vehicles, electric generators, factory equipment, and other devices containing rotating machinery could be early candidates to join the IoT.
- *Health care and caretaking.* Sensors and actuators in beds, floors, and plumbing promise to be "helping the helpers". The University of Virginia's AlarmNet research project has interconnected networks with some everyday things such as beds and floors. A pressure sensor in a bed detects heart rate, breathing, and movement; sensors in the floor nearby can detect when a person falls. The AlarmNet project team has also embedded accelerometers and a GPS receiver into clothing, in order to detect location and classify activities. Pressure sensors in beds or furniture may also be able to detect sudden weight gains associated with certain heart conditions and the side effects of beta blockers. Various R&D projects have experimented with connected smart medicine dispensers that facilitate compliance with complex, multi-prescription regimens.
- *Loosely-coupled relationships among connected things.* Just as physical objects have ad hoc temporary synergies (as when a brick serves as a door stop), ad hoc interconnections among everyday things can have opportunistic benefits. A single Web-services interface for a vehicle could couple with a dealer's diagnostic tool for maintenance purposes; a law-enforcement server for recovery after theft; a colleague's cell phone for inputting the physical address of a destination into an onboard navigation system; and any number of surprising and unplanned-for applications .

Timeline

Use of RFID in supply chains has begun, and use at the item level could begin as early as 2010. Incorporation of compatible RFID readers in common cell phones could begin shortly thereafter and be common by 2015, enabling everyday people to interact

electronically with everyday objects. Ubiquitous positioning technology, including accurate indoor positioning, could be available by 2017. Synergies between positioning and Internet connectivity could enable a number of must-have applications, especially theft-resistant personal items that can be located, controlled, and monitored from a distance. After 2020, intelligent software may emerge that accepts large sets of data from connected everyday objects, and analyzes such data using processes that resemble human reason. After 2025, perhaps, such software can be deputized to make unsupervised decisions and act on behalf of people.

Issues Determining the Development of The Internet of Things

Key decisions affect outcomes of how quickly the IoT will develop and what capabilities it will have. The factors that determine outcomes fall into two categories, depending on whether businesses or governments play the deciding role.

Business Issues

- *Logistics and supply-chain support.* Large businesses are driving adoption of RFID tags and readers for the purpose of streamlining supply chains. The speed and scope of such developments is important to creating economies of scale for RFID technologies as well as for related database infrastructures. Stakeholders take for granted that the Internet will be the primary platform for such infrastructures.
- *Deterring knockoffs.* Companies' interest in deterring counterfeit products could drive adoption of RFID-tagged containers, pallets, and perhaps individual items. Pharmaceutical companies' interest in deterring unauthorized and/or unlicensed production of drugs—whether generic or counterfeit-labeled—could be key to driving the trend toward item-level RFIDs (see below).
- *Deterring theft.* Individuals and organizations who seek to deter and remedy shoplifting and theft could drive adoption of both RFID-tagged items and devices having self-locating features (such as embedded GPS and wide-area wireless capability).
- *Food safety and competitiveness.* People's interest in the food they eat, especially its safety, could drive adoption of RFID-tagged food packaging.
- *Item-level RFIDs.* On balance, business has the greatest influence over when and whether to deploy RFIDs on individual items and therefore on resulting development of mass markets for reader devices. Government decisions to tag file folders, library books, and identification cards will play a significant role is far from certain to drive adoption of RFID readers by the general public. Conversely, if individual prescription bottles, say, contain RFID tags, members of the public have reason to adopt RFID readers to support medication reminders and smart medicine cabinets that help people manage complex, multi-prescription regimens. If food packages contain RFID tags, the public has reason to adopt RFID readers, e.g. to check ingredients, preparation instructions, price and availability for repurchase, nutritional content, use or nonuse of pesticides, farm of origin, information about package recycling, promotional offers, and more. Outcomes rest on businesses' views of whether investments in RFID are mainly for logistics reasons or to enhance the value proposition in other ways; the

payback period needed to justify the investment; whether individual items receive unique, serialized RFIDs, and so on.

- *Automotive-industry competitiveness.* An "Internet of cars" could arise because users (owners, service personnel, and factories) have reason to make inquiries about a car's condition and location; because internetworking could enhance onboard safety, information, and entertainment applications; and because carmakers continuously seek to stimulate demand by updating features annually and differentiating their wares from one another. Some analysts also expect that government mandates to enhance safety could drive the emergence of connected cars.
- *Energy cost and environmental concerns.* Adoption of network-addressable energy appliances could be a key driver for IoT development. Network-addressable utility meters, indoor climate controls, hot water heaters, and pool pumps could provide ways to control costs and reduce energy use while preserving the creature comforts that people are accustomed to. Adoption of renewable energy sources could drive toward increasingly distributed energy storage and distribution, such that many household-scale and small-business systems each possess Internet addresses for the purpose of monitoring, metering, and crediting electricity generation.
- *Intellectual property rights.* A patent assigned to NeoMedia asserts that the company has exclusive rights to establish a correspondence between barcodes and Internet addresses; other patents the company owns could apply to systems that identify objects and respond by looking up information and executing other actions. While at least one organization acceded to NeoMedia's demands for licensing fees, others have resisted; as a result, the USPTO may or may not invalidate NeoMedia's patent. Because NeoMedia arguably has a "paper patent" and lacks a useful technology to contribute to a licensee's development efforts, some companies that want to develop the IoT see the patent as an unrecoverable cost of doing business and a barrier to entry. While the uncertainty about NeoMedia's IPR may be resolved within a few years, this example remains pertinent because other IPRs could dampen investors' enthusiasm and thereby impede progress of the IoT.
- *Standards.* Today's networks comprise complex ecosystems of vendors, whose wares are interoperable—to a remarkable degree, even if not perfectly so. Smooth functioning of the IoT will require development of and consensus about standards for physical interconnection, protocols, data structures, and distributed-execution architectures.
- *Business collaboration.* A key gatekeeping item for the IoT will be ability of businesses, including competitors, to cooperate with one another. While the competitive spirit is key to innovation and cost reduction, there are many cases where competitive forces impede interoperability, as one company seeks to dominate a market by means of a proprietary technological approach. (Apple's iPod is a key example.) Such proprietary technologies may yield innovations but they also tend to discourage some of the conditions that a robust IoT requires such as ad hoc thing-to-thing communications and unmetered connectivity. Unresolved issues regarding standards and IPR licensing are in a sense subsidiary to the larger question of whether rival suppliers will collaborate sufficiently to enable a robust IoT.

- *Personal and business security.* Risks associated with an IoT span from annoyances to threats of large financial losses. Mischief-makers could exploit one's ability to control lights and appliances, while criminals could exploit one's ability to control security and payment systems.

Government Issues

- *Spectrum policy.* License holders occupy a great deal of usable spectrum by means of inefficient, 50- to 75-year-old technologies, yielding a premium on assignable spectrum. Current FCC spectrum-allocation doctrine revolves around a combination of spectrum auctions (mandated by the Balanced Budget Act of 1997) and "facilities-based competition". These doctrines have led to a "razors and blades" business model for auction winners, where subsidized handsets ("razor handles") are bundled with contracted minutes ("blades") in exchange for monthly charges. The result favors devices that generate large amounts of monthly "minutes". Facilities-based competition works against the promise of self-organizing meshes of wireless nodes that obviate need for dedicated infrastructure. As a result, users typically cannot justify a typical operating costs of, say, $60/month per object for handling Internet Protocol data. Significantly, TV broadcasters also have incentive to oppose allocation of adjacent channels, in order to protect reception of free, over-the-air TV in locations where reception is marginal. Incumbent licensees also tend to oppose allocation of unlicensed bands, considering that such bands could introduce unwanted competition. Incumbents also tend to exercise best-of-breed expertise in regulatory advocacy to sway government decisions in their favor. In short, the means of allocating spectrum does not encourage the most rapid innovations. This is one of the reasons why an IoT, though in many respects technically feasible today, will require 10 or more years to develop. However, emerging technology uses spectrum more efficiently and enables spectrum sharing, as telecom industries mature they may make room for lower-margin opportunities; and as high-tech businesses learn to wend their way around Washington D.C., they may learn to exercise regulatory clout to rival that of broadcasting and telecom industries.
- *E-waste.* Efforts to reduce waste going to landfills and seeping of toxic materials used in electronics into water sources could moderate the spread of the IoT, as could consumer and business preferences for reduced waste and sustainable practices. Some proposed approaches to solving the technical problems of power distribution for smart objects—specifically, microbatteries—may entail more toxic materials and thus may be more threatening to landfill and ground-water content than other approaches—such as energy harvesting. But even the miniature power sources most attractive to environmentalists—including photovoltaics—may impose significant burdens on the environment owing to their manufacture. Policy makers will be wise to carefully study cradle-to-grave and cradle-to-cradle impacts, costs, and externalities. Policy makers may also need to consider steps that could encourage development of clean technologies, e.g. those that facilitate reuse, recycling, and remediation of environmental harms.
- *Geolocation.* A key benefit of the IoT may be ubiquitous ability to locate stolen, misplaced, and loosely-organized things. The U.S. government greatly helped increase availability of geolocation signals by means of the Navstar GPS program. But nobody

knows whether or when positioning technology will become ubiquitous, especially for indoor use. Worldwide, including in the US, policy doctrines are internally inconsistent and await rationalization: Deployments are underway for several redundant satellite geolocation infrastructures, yet solutions for indoor location remain elusive. Challenges exist in balancing policy mandates for helping first responders locate persons in trouble versus maintaining ability to deny location signals to enemies of the US. For example, investment in the effort to help first responders by means of opportunistic signals (such as radio and TV broadcasts) could make it difficult for the military to disable or jam location signals during a crisis; yet first responders' lack of pinpoint indoor navigation could aggravate such a crisis or be a direct cause of one (say, if they cannot locate a briefcase-size WMD in a timely fashion). IoT development would be accelerated if such pinpoint navigation emerges.

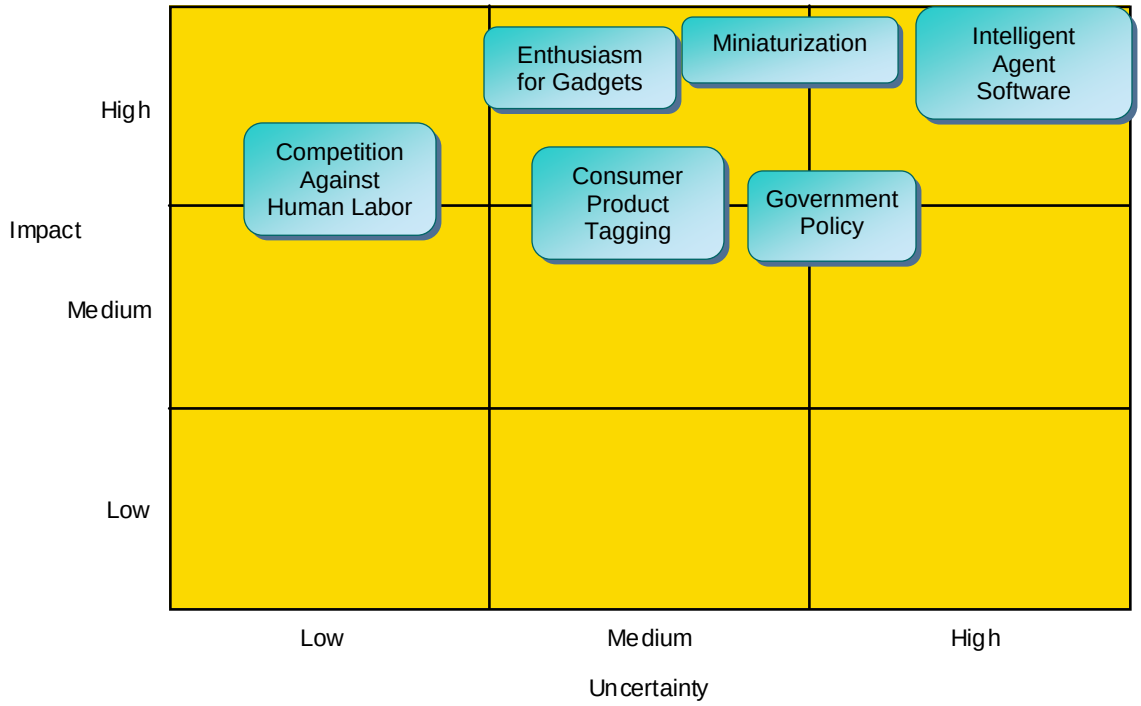
- *Cyber-warfare.* This issue potentially cuts several ways. U.S. law enforcement and military organizations could seek to monitor and control the assets of opponents, while opponents could seek to exploit the United States. Conversely, all parties will seek to deny access to one another's systems. As in the case of all high-stakes security issues, escalation pathways are long and perhaps stakeholders will find no decisive end to such pathways.

Items to Watch

A number of issues have uncertain outcomes and significant impacts, depending on how (or if) they resolve.

- *Consumer product tagging.* The timing and capabilities of the IoT depend strongly on the timing of commercial market development for RFID, the application of RFID tags to containers, pallets, and individual packaged items, the categories of materials and products that receive tags, and how those categories evolve over time.
- *Miniaturization.* The timing and capabilities of the IoT also depend strongly on the miniaturization of processors, wireless interfaces, sensors, actuators, and power supplies. Generally, reduced power requirements comprise a key aspect of miniaturization, enabling use of small batteries, unattended operation without charging/replacing batteries, use of energy-harvesting transducers, and/or use of wireless power transfers.
- *Government policies.* Policy enablers and obstacles abound. Policies that encourage interconnection and automation include efforts to keep soldiers out of harm's way, maintain an all-volunteer armed force, support the Navstar GPS constellation, develop national GPS augmentation signals (such as NDGPS), assist emergency responders by mandating accurate location information, encourage smart metering of energy, permit unlicensed communication in the UHF band, and waive export controls on encryption in certain cases. Policies that may tend to discourage interconnection and automation include restrictions on accuracy and availability of GPS, pseudolites, and other location technologies; spectrum-allocation policies that favor deep pockets and exclusive licensing; free-trade agreements that enable access to very low-cost labor; and restrictions on hazardous substances aimed at keeping such substances out of landfills and groundwater. Outcomes will be a complex multi-dimensional resultant of the sum of these forces.

Figure 16[2]
THE INTERNET OF THINGS: ISSUES AND UNCERTAINTIES



Source: SRI Consulting Business Intelligence

- *Enthusiasm for gadgets.* The timing and intensity of demand are uncertain. Consumer demand will be a key driver for the adoption of the IoT, assuming technology makes it affordable and attractive for people to appreciate innovative convenience features of cars and homes; allow possessions to remain only loosely organized while remaining safe in the knowledge that location technology will help them find desired things as required; gain a sense of command over appliances such as lights and thermostats; and express their social status commensurate with like-minded members of their community.
- *Intelligent-agent software.* The timing and sophistication of advanced software solutions are uncertain. Capabilities of connected objects may depend on technical approaches to address the desire for software to interpret the environment, detect human intentions, make human-like inferences and decisions, and act on behalf of people. One current approach to delivering such intelligence insists that the most

[2] Figure 16 illustrates major issues and events that will have an impact on the rate or direction of a technology's development and thereby application. The impact of these issues and events is plotted against a measure of uncertainty, where uncertainty implies insufficient knowledge of how (and usually just when) the issue or event will be resolved or be sufficient to drive or hold back development of the technologies. An organization that is able to accurately predict or (better) influence or dictate the outcome (thereby moving the issue/event to the left of the figure), will have a distinct advantage over organizations that are still in the dark or just passively following developments.

fruitful pathway toward systems having human-like reasoning processes may be for inference engines to operate on structured metadata, and that people must construct such metadata. Another approach insists that pattern-recognition and feature-extraction technologies can be effective in automatically constructing metadata, and furthermore that feature extraction is a necessary step in market development because people will not take the trouble to produce structured metadata to describe objects and digital content. A further approach is for software engineers to construct relatively simple application-specific agents and enable many such agents to interact. And yet another approach is for software engineers to try to teach an agent so much about the details of the world that the agent begins to display common sense and ability to teach itself as required. The timing, scope, and applications of the IoT depends to a significant extent on the timing of software developments, and which agent-software approaches take the lead over rival approaches.

- *Competition against human labor.* Unattended checkout, automated inventorying, and antitheft features appeal to retailers and packaged-goods distributors only to the extent that RFID technology pays for itself; reduced labor costs is one of the key financial justifications. Similarly, robotic heavy equipment at ports can use thing-to-thing connections to coordinate routing of containers with minimal human intervention; but again, shippers and port authorities are attracted to solutions largely if machine-to-machine communications pays for itself; and again, the cost of human labor strongly influences the financial justification for deployment of IoT technologies. Companies will have motivation to cut costs but uncertainty remains about to what extent they will do so by investing in the IoT versus by expanding their use of low-cost sources of human labor.

Directional Signposts

Identifying the major issues that will determine how the Internet of Things will develop and understanding the uncertainty of items important to watch help us to understand better the potential dynamics of development and application that we might see in the future. That heightened sense of awareness is necessary because the United States will want to formulate a policy and act before unambiguous evidence on the drivers and barriers to, and direction of advancement of the necessary technologies is available. Preparation for a watch-and-respond system is essential to identify correctly the signposts that would indicate whether the advancement of the Internet of Things is proceeding rapidly or not. Plausibly, the following events and developments could occur near the suggested years, and their occurrence would indicate that the above issues and uncertainties were being resolved in the direction of positive development and application of the Internet of Things.

- 2007-2009—Large retail chains in the United States adopt RFID-tagged pallets and packaging for expediting supply chains
- 2010—Large retail chains in the United States begin to deploy RFIDs on individual items to support unattended, walk-through checkout; healthcare providers, large organizations, and government agencies adopt RFID tags for keeping track of individual documents

- 2011-2013—End users adopt cell phones containing RFID readers that scan everyday things and provide information about price, availability, origin, ingredients, how to use, where to receive warranty service, and other attributes
- 2011-2016—Vehicles gradually incorporate wireless diagnostics and prognostics, concurrently improving reliability, eliminating cost and weight of wiring harnesses, reducing cost of maintenance, and enabling delivery of new features via software updates
- 2017—Effectively, ubiquitous positioning technology arrives in the United States—initially, to help first responders locate people carrying cell phones, even indoors.
- 2018-2019—Manufacturers increasingly deliver everyday things with a guarantee against loss and theft, equipping such things with receivers for ubiquitous positioning technology as well as low-duty-cycle wireless Internet capability.
- 2020—The past ten years of spectrum auctions and reallocations has gradually yielded a transformed spectrum plan. Everyday mobile communications is now broadband. The legacy mobile frequencies used for narrowband communications (the type that revolutionized person-to-person communications during 2000-2005) have largely been repurposed for supporting person-to-thing and thing-to-thing communications.
- 2020-2025—A period of innovation, growth, opportunity, and disruption follows whereby users and suppliers find and implement synergies among connected everyday things—and counterproductive uses also emerge. For example, organizations may create ad hoc sensor networks by fusing data gathered from disparate devices. Such networks may on balance do more good than harm, notwithstanding the substantial harms that do arise when unauthorized persons exploit connected everyday things for crime and espionage purposes.

Within the timeline that these developments are likely to occur, it will be important to watch for and monitor various signposts that will indicate the direction and pace with which the field is advancing and to assess any resultant potential threats to and opportunities for U.S. interests. Key signposts, which, if positive, would indicate progress toward realization of the Internet of Things, include:

- The size and nature of demand for expedited logistics in commerce and military organizations
- The effectiveness of initial waves of IoT technology in reducing costs, thereby creating conditions for diffusion into vertical application areas including civilian government operations, law enforcement, healthcare, and document management.
- The ability of devices located indoors to receive geolocation signals—possibly, distributing such signals by leveraging available infrastructures (cell towers, broadcasters, and so on)
- Closely related technological advances in miniaturization and energy-efficient electronics, including reduced-power microcomputers and communications methods, energy-harvesting transducers, and improved microbatteries.

- Efficient use of spectrum, including cost-effective solutions for wide-area communications at duty cycles that are much smaller (e.g., the equivalent of a few minutes per month) than those of cell phones (averaging many minutes per day).
- Advances in software that acts on behalf of people, and software that effectively fuses ("makes sense of") sensor information from disparate sources.

Abbreviations

The following abbreviations are used in this Internet of Things disruptive technology profile:

DARPA	Defense Advanced Research Projects Agency
cm	centimeter
FCC	Federal Communications Commission (United States)
GHz	gigahertz
GIS	geographic-information system
GPS	global-positioning system
ID	identification
IOT	Internet of things
IPR	intellectual property rights
IT	information technology
LAN	local-area network
m	meter
MIT	Massachusetts Institute of Technology
NASCAR	National Association for Stock Car Auto Racing
NDGPS	Nationwide Differential Global Positioning System
NHTSA	National Highway Traffic Safety Administration (United States)
PC	personal computer
R&D	research and development
RF	radio frequency
RFID	radio-frequency identification
TUI	tangible user interface
UHF	ultra-high frequency
USPTO	United States Patent and Trademark Office
UWB	ultrawideband