The Internet of Things, Legal Aspects
What Will Change (Everything)…

Eric BARBRY
Attorney-at-law, Alain Bensoussan law firm

Abstract: After the birth of the Internet, the rise of Web 2.0, here comes the Internet of Things. Internet has led us to adopt special law, digital economy law…Web 2.0 has urged us to rethink core legal concepts such as liability and ownership and introduce notions such as sharing and availability. The Internet of Things – which no one doubts will be the next technological revolution – will be a legal tsunami, the intensity and magnitude of which are unknown to date.

Key words: Internet of Things, privacy, personal data, artificial intelligence, network, Web 3.0, IoT.

In the 1990s, only a few of us believed that the Internet was going to invade our life and those who thought so were considered at best as dreamers, at worse as weirdos. 10 years later, Internet was a pervasive part of daily life, both at work and at home.

At that time, rare were those who were convinced that the Internet was going to revolutionize law. But ten years later, virtually all states have a law dealing with the Internet or digital technologies.

In the 2010s, there was the advent of Web 2.0. Many called it at best a marketing stunt and at worse a legal bluff. Two years later, social networks are here, there and everywhere from large public networks to professional networks and corporate social networks.

Again, only a handful of us understood that Web 2.0 was to bring about new and complex legal issues and that with Web 2.0 nothing changed but everything was going to be different (BARBRY, 2007). With Web 2.0, the legal basics are still here but they are now implemented in multifaceted manners.

Now, here comes a new revolution: the Internet of Things, also known as "IoT".

Not surprisingly, just as for Web 1.0 and Web 2.0, the Internet of Things has already its opponents and other critics who consider it at best as a myth, and at worse as a technical mystification.

And yet, the Internet of Things already exists. It is part of our everyday life – at least for some of us – without us really knowing it.

The Internet of Things is still in its infancy. It has started with "augmented reality", "geolocation" or "QR code", but these are nothing compared to what the future has in store for us.

Basically, the Internet of Things purports to achieve two things: (i) make things intelligent and (ii) serve as a true decision-making tool, going as far as replacing human decision.

With IoT, the most ordinary, simplest (not to say stupid) objects, would become "intelligent". To put it simply, the most insignificant object would be able to communicate with its surrounding environment.

It is often caricatured as an empty fridge that would itself call the local supermarket to order food…but it is much more than that. What about connecting the white stick of a blind person to a network to allow him to move almost "normally"! An attractive project? No… a reality!

The "intelligent car" is also a telling example. An intelligent car is a vehicle that reacts to its environment, i.e. the driver, the traffic, the road environment. Many manufacturers have been investing significant amounts of R&D money in smart cars for a long time and it is today one of the top investment targets after the electric car.

The motor industry is not the only one to put money on IoT. Many other industries have adopted IoT. For example, the building sector is working on developing "smart homes" or "smart cities", where buildings and household appliances will interact with their own environment (to improve energy consumption, environmental aspects, life quality, …). Smart cities already exist: New SongDo City in South Korea, PlantIT Valley in Portugal, Masdar in the United Arab Emirates, T-City in Germany, … They have taken their cue from the energy sector, which has developed a "smart grid" (smart energy network) where a series of sensors dialog with one another to interpret the endogenous (real-time consumption) and exogenous (environment/climate/price) data of such and such energy source to create and operate efficient and reliable energy infrastructures.

Some projects are directly funded by the European Union, as demonstrated by the green cars, energy-efficient buildings or factories of the future initiatives. In the UK, the Technology Strategy Board is investing £500,000 in preparatory studies to develop strategies for moving towards a converged and open application and services marketplace in the Internet of Things, as "a widespread Internet of Things could transform how we live in our cities, how we travel, how we manage our lives sustainably, how we age". China is also placing a national priority on IoT. In 2009 Chinese Premier Wen Jiabao called for the rapid development of Internet of Things technologies, declaring "Internet + Internet of Things = Wisdom of the Earth" and early 2012 the Chinese Ministry of Industry and Information Technology (MIIT) released an Internet-of-things plan for the 12th Five-year period (2011-2015), which predicts that China will form up an industrial Internet-of-Things chain in 2015 that enjoys the presence of 100 backbone enterprises in 10 major industrial areas. While public authorities first adopted a wait and see attitude for Internet and Web 2.0, this time law makers have rapidly taken an interest in IoT, as if feeling the birth of a true revolution.

For example, the European ministerial meeting held on 6 and 7 October 2008 was focused on the Internet of the Future with emphasis on the Internet of Things and the European Commission drafted in 2009 an important Communication on the Internet of Things.

This Communication of 18 June 2009 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, entitled "Internet of Things: an action plan for Europe", lays down 14 lines of action, including:

- the implementation of a governance at least at the European level,
- the security of IoT, entrusted mainly to ENISA,
- the status of IoT as an infrastructure of vital importance,
- the necessary standardization of IoT technologies,
- the importance of R&D and the launch of pilot projects,
- the cooperation of public and private sectors in the form of partnerships,
- the institutional awareness within the EU,
- the international dialog,
- the management of waste and recycling,
- the acceptance level, including exposure to electromagnetic waves,
- the future developments of IoT, which is in constant evolution.

Two lines of action are more particularly interesting from a legal perspective:

- Line of action 2: It raises the necessity for a "continuous monitoring of the privacy and the protection of personal data questions"; and
- Line of action 3: It underlines the need to be able to disconnect from the networked environment, i.e. achieve the "silence of the chips".

While the two above questions are essential, this is just a beginning and one should expect IoT to raise many more legal questions.

This is why, as a follow-up to its 2009 Communication, the European Commission recently launched, from 12 April 12 to 10 July 2012, a consultation to solicit the views of a wide range of stakeholders and the public at large and "know what framework is needed to unleash the potential economic and societal benefits of the IoT, whilst ensuring an adequate level of control of the devices gathering, processing and storing information". Through the consultation, the Commission is seeking views on privacy, safety and security, security of critical IoT supported infrastructure, ethics, interoperability, governance and standards. The results of the consultation will feed into the Commission's Recommendation on the IoT, which will be presented by summer 2013.

But first things first: What is IoT exactly? Well, that's the 64 Million Dollar Question. Finding a common definition of IoT is indeed not so easy.

The French Wikipedia page on the subject rightly underlined that "there is not standard shared definition of IoT. Some definitions insist on the technical aspects of IoT […], others focus on uses and functionalities".

ITU-T Study Group 13, which leads the work of the International Telecommunications Union (ITU) on standards for next generation networks (NGN) and future networks, approved in July 2012 a Recommendation ITU-T Y.2060, Overview of the Internet of Things, which defines IoT as "a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies".

The Internet of Things has also been defined as:

> "[…] a network of networks that enables to identify digital entities and physical objects, directly and without ambiguously, via standardized and unified electronic identification systems and wireless mobile devices, and thus makes it possible to retrieve, store, transfer and process data relating to them, without discontinuity between the physical and virtual worlds". (MASSIT-FOLLÉA, BENGHOZI & BUREAU, 2009)

The advantage of the above definition is to contain most of the keywords symbolizing the legal issues surrounding IoT:

- "network of networks" implies topics such as ownership and standards;
- "identification system" implies topics such as traceability and monitoring;
- "physical objects" implies topics such as quality and related matters;
- "data" implies topics such as quality and ownership;
- "processing of data" implies topics such as relevance and liability.

But the heralded revolution of IoT lies above all in bringing together the "real/physical" world and the "digital/virtual" world, or more accurately in the merger of the molecular world (the things) and the octet world (the Internet). (BENSOUSSAN & BARBRY, 2012)

Today, from a legal perspective, these two worlds are hermetically sealed off from each other. The physical world is built on longstanding rules with key concepts such as "ownership" and "fault". The digital world has changed those concepts. Admittedly, they still exist in the digital world, but they have been revamped: ownership has been replaced in particular by the "right to share" and "fault" has made way for other systems such as "notification".

This paper will now discuss those different elements and attempts to enrich the debate on the various legal issues raised by IoT.

■ "Connected" objects

The Internet of things requires that objects be connected, but how? That's the core question!

The current form of "connection", whether wired or wireless is not sufficient for the Internet of things. As objects are everywhere, they must be freed from technical constraints, such as sockets or Wi-Fi hotspots.

R&D is committed to finding an easy, fluid and permanent connection between the thing and the network. To this end, it is considering a new networking pattern made of sensors capable of reading RFID chips. Concretely, each thing will have a tag and could sent/receive – i.e. exchange – information when passing in front of a sensor.

RFID chips seem to be an ideal solution to ensure a massive and permanent connection of things but other solutions exist; they might be less user-friendly but are equally reliable and above all cheaper, such as graphic tags. What solution will be chosen? The war is on!

Setting up a network of sensors and generalizing radiofrequency chips will certainly raise a variety of issues.

Firstly, it will raise public health issues. This is likely to be a heated discussion, fueled by the current debates around mobile phone masts. The public will be concerned about the installation of sensors "just next door". On that point of view, the Communication of the European Commission is interesting as it states that "most of today's foreseeable IoT devices are expected to be in the 'radiofrequency' group (i.e. >100 kHz) and operate with very low power, unlikely to produce significant levels of exposure to EMF. The existing regulatory framework on EMF is under periodic review and will keep ensuring that all devices and systems will respect the safety and health needs of the population in the future".

Secondly, to what is the thing connected? The connections can be established in restricted areas or made publicly accessible. A sub-question will thus be to make distinction between the *Internet* of things and the *intranet* of things …but this is yet another question!

Thirdly, what would be the impact on the neutrality of the Web and the right of access for everybody? Today, everybody (at least in the countries where the Web is not under surveillance) may freely and easily connect to the Internet. But will this still be the case when the connection will depend on the owner(s) of the sensor network?

Lastly, it should be pointed out that today things do not have a legal status. Legally, they are nothing; they do not exist.

This does not mean that things are not dealt with by law. Admittedly, things can be legal or illegal. Its use can be permitted or forbidden, it can be someone's property or free of use. However, things alone do not exist. Its legal existence depends on an element which is intrinsic to it. With reference to liability law, numerous legislations recognize "liability for things", in other words, damages granted to compensate harm suffered because of things. However, the liability at stake is not the liability of the thing, but the liability of the owner. What is dramatically new with IoT is that harm does not depend on things per se, but on its communication with the rest of the world, and

more specifically the way that things will interpret, process and return the data received. The problem is that all these functions depend on the way things are set, settings on which the thing owner has no control.

Without going as far as recognizing a legal personhood to a thing (i.e. acknowledge that a thing can have rights and duties and that it can exercise them on its own), there will certainly come a time when a thing will be seen as a "legal actor" (BOURCIER, 2001; SOLUM, 1992).

■ Identity of the thing

The question of the legal recognition of the identity of the thing will also arise. At present, the very concept of "identity" is inextricably linked to the human being; but what will it be like tomorrow when each thing will have an identity? (FIDIS, 2008).

The principles underlying the Internet of things require that each object is uniquely and certainly identified and identifiable inside the network.

Today, the elements connected to the network have most of the time three identifiers: (i) a machine identifier (e.g. MAC address), (ii) a product identifier (e.g. a bar code) or (iii) a digital identifier (e.g. IP address).

With the Internet of Things, identity will be a key issue, both qualitatively and quantitatively. It is established that the current addressing system based on IP V4 is very limited and will not be able to bear the connection of billions of things. In its Communication, the European Commission states that the Internet of Things "potentially concerns 50-70 billion ‘machines', of which only 1 % are connected today".

At this stage, there are two options: (a) change over to IP V6 or (b) start over with another technological solution, a solution currently explored by researchers, notably at the MIT.

In both cases, the impacts will be significant. Changing from IP V4 to IP V6 is already quite a challenge: although IP V6 is now controlled, it has not been actually implemented and it has been announced to occur "next year" for many years now. And using another technology can only be a big bang. In comparison, the Y2K changeover was only an appetizer... Are you ready for the main course?

Let's now take a closer look at another essential question, namely the ownership of the future new addressing system.

There will be a cut-throat competition between countries to avoid that one single person has a stranglehold on the object identification technology. This is why, for example, the French Commission for the Liberalization of Growth initiated by former French President Nicolas Sarkozy urged the French government to "ensure the independence and confidentiality of the operator managing the identities of the Internet of Things (radio frequency identification – RFID) as it will offer the possibility to trace identities and flows of transactions".

For all that, the big winner might be a…start-up, right under the nose of the most powerful states of the world. An efficient technology, imposed upon everyone … and patented! This is surely a more disturbing thought than the control of the Object Naming Service by the USA or Europe. The one who will hold the technical keys of the Internet of Things will definitely have an unequalled power. On this subject, the opinion of the European Commission, which cannot be taxed with interventionism, is crystal clear: "Simply leaving the development of IoT to the private sector, and possibly to other world regions is not a sensible option in view of the deep societal changes that IoT will bring about". This leads to a crucial question: Should IoT be excluded from patentability, as for software? The question is still open as nobody wants to take the plunge, believing that the future "winner" will be one of their own…but an answer is urgent in the light of the number of patents already filed in relation to "thing-to-thing communication".

Lastly, who will run the system? The current system, which enables to access web pages and browse from IP to IP is the Domain Name System (DNS). But who will control the Object Naming Service (ONS)?

Bernard Benhamou points out, with good reason, that:

> "If it becomes possible, thanks to the technologies of the Internet of Things, to know the movements of any objects and individuals around the globe, the government that would control such system would have a power that no other government had ever dreamed to possess" (BENHAMOU, 2009).

For now, TCP IP V4 is shared by everybody, but it cannot be denied that the DNS is totally controlled and decided in the USA, as recently demonstrated by the creation of new gTLDS by the ICANN. What about the IoT and the ONS?

■ "Smart" objects: when the object is in charge…

Being connected is good…but being smart is better. The IoT offers not only to connect any thing but also to make it I-N-T-E-L-L-I-G-E-N-T!

A smart object would have two new functions: help the decision-making process (the easier part) and take decision for the human (welcome to a world of Terminators).

This will change everything, especially in terms of liability.

Self-driving cars epitomize the liability issues raised by smart objects. In the USA, the state of Nevada legalized self-driving cars in 2011 and in May 2012 granted America's first self-driven car license to a Google car. In the event of an accident, law-enforcement authorities and insurers will have to decide who will be held liable: the driver, the car manufacturer, the "smart" car…? And this is just the beginning as other U.S. states are also considering the legalization of self-driving cars (California, Arizona, Hawaii and Oklahoma).

Today, the Internet is packed with information; this information may be good or bad, true or false, raw or detailed, accurate or misleading, but it only has one goal: inform! It is the responsibility of the Internet user to use this information correctly and take the right call.

The information at the heart of the traditional Internet is passive. But the primary objective of the IoT is precisely to make information active, so that it can help the humans in the decision-making process by offering analyses, solutions and alternatives not only based on their tastes, centers of interest and wishes, but also on real-time exogenous elements. Eventually, it will even take the decision on behalf of the human.

Let's take an example: today I receive static information telling me where I CAN eat in my neighborhood or where I am; in the future, it will tell me where I WILL eat, in the light of what I have eaten lately, my diet, my tastes, the number of my guests, their tastes, the number of available seats in the nearby restaurants and my budget! This changes everything, especially if the restaurant does not live up to my expectations!

Our legal environment mainly lies on a distinction between the right to information and the obligation to advise. Our law is not very familiar with – but will soon have to learn – the right to alert, warn, suggest, recommend…

With the Internet of Things, we will certainly need to reconsider all of these rights to know who is liable for what. And answering that question will be even harder when the machine will choose for the Human!

■ Big brother objects are watching you!

Privacy is of paramount importance for IoT because even if citizens of the world now disclose their private life on blogs and Facebook walls they are nonetheless at the same time fearing for their privacy.

The IoT will make it possible to record a range of data such as health parameters, reading habits, location data, energy use, driving style, eating habits...giving a detailed view of a user's life (OECD, 2012).

For example, a Pay As You Drive (PAYD) insurance monitoring device may log data on the location, time, distance, speed and other parameters that can influence an insurance premium. This can provide a detailed look into the use of the vehicle and the lives of its drivers. Moreover, mobile telecommunication companies in the European Union will have to keep a record of the start of every communication under European Union data retention law, every time the car is turned on, a record is made and the start and finish of a trip is known.

In the Netherlands, the Dutch privacy authorities objected to a project for introduction of smart metering due to the potential intrusion into people's lives.

A recent talk of CIA Head David Petraeus caused quite an outcry among privacy advocates. Discussing the emergence of an Internet of Things at In-Q-Tel CEO Summit, Petraeus explained that, because of the increasing development of technologies driving the Internet of Things, the intelligence community will have to rethink the notions of identity and secrecy: "these technologies could lead to rapid integration of data from closed societies and provide near-continuous, persistent monitoring of virtually anywhere we choose". Petraeus further said that "'Transformational' is an overused word, but I do believe it properly applies to these technologies, particularly to their effect on clandestine tradecraft. Taken together, these developments change our notions of secrecy and create innumerable challenges – as well as opportunities".

Several initiatives have been taken to protect the privacy of individuals. For example, in March 2011 Pachube (a company now called Cosm) proposed an "Internet of Things Bill of Right", i.e. a set of rights that it hopes to become an industry standard. It is intended to give people access to and control over their data created and gathered via IoT devices. Such rights include for instance "People own the data they (or their "things") create" and "People have the right to keep their data private".

Traditionally, being connected is a voluntary act and emphasis is placed on "prior consent" and "right to be forgotten" as well as a strict regulation of cross-border flows of data and interconnections. Will this still be the case with the IoT where objects will be by default connected to the network and where interconnection and cross-border flows will be permanent?

There is no doubt that this subject will also lead to a major legal evolution. Most authors who have already worked on the subject stressed the necessity to recognize a new right: "the right to disable chips". This extremely interesting concept is not new as it was first initiated at the birth of RFID chips when some "experiments" led to analyze the behavior of consumers without their knowledge.

The right to de-activate takes on particular significance with the Internet of Things, as the latter relies on a network of sensors and the generalization of RFID chips.

The right to de-activate chips, also known as "the right to silence of the chips" is based on an opt-out mode: in clear, the chips are by default active and I decide to disable chips. Others would favor the "opt in" approach, i.e. not recognizing a right to silence but a rather right to speak: the chips are by default inactive and I decide whether or not to activate them.

Be that as it may, both approaches have their limit: once activated or deactivated, the other way round is often impossible.

But instead of adopting a Manichaean, black-and white attitude, with on the one hand the right to speak and on the other hand the right to silence, it would seem more appropriate to strike a balance and establish a right to "manage chips". With one, major constraint: it will transform us all into chip managers… i.e. in other words into system administrators!

Lastly, it would certainly not be sufficient to penalize illegal access to personally-identifiable data as it is the case today (various personal data legislations punish unfair collection of personal data); it would be required to

punish the fact of placing connectors and other chips without giving prior information about and the capacity to disable such connectors. Similarly, even if the "right to be forgotten" is a necessity in an environment where information is the rule, the concept should change towards a right to erase tracks to adjust to IoT. Other evolutions will also probably be necessary, such as the one pointed out by David Forest in his article "Who is afraid of IoT", according to which "the management of these multiple identities required a change from a law focused on the protection of individuals to a law focused on data control" (FOREST, 2009).

■ "Augmented" information

With IoT, both reality and information are "augmented" – or more accurately "enriched".

Information may be owned or free. To date, ownership is the rule. Information belongs to somebody, who may use it as he wants, especially if it is protected by intellectual property. Information may also be "given" in the form of a free license, as has been the case for a long time now in IT as well as more recently for all types of content (e.g. Creative Commons).

The enrichment of information is to the Internet of Things what the hypertext link is to the traditional Internet: a building-block!

Therefore, it will certainly be indispensable to review our old legal theories on ownership and free profit and pave the way for new concepts such as sharing or enrichment.

■ A network of responsible objects?

The liability of the technical actors of the Internet is a tricky subject. For the moment, it is limited both legally and contractually.

Legally speaking, most countries that have adopted regulations on the Internet have created a specific regime that limits the liability of Internet actors, such as infrastructures, ISPs or hosting providers. They are typically liable for nothing or very few things in relation to the contents they display or otherwise use.

Contractually speaking, this is the same situation. To be convinced of this, one merely has to look at the liability (or more accurately, non-liability) clauses used by ISPs and hosting providers, who consider that the Internet is by nature uncontrollable and that they cannot as a result be held liable in terms of quality of service and performance.

This situation cannot work with the Internet of Things. Those actors will therefore have to be, to a certain extent, the guardians of the technical performance of the IoT.

Technical providers are already facing a significant increase of their liability. Web 2.0 has already required them to be more involved in the Web. For example, they are actively cooperating in the fight against counterfeit products (ACTA); they are subject to the legal obligation to handle security breach (various national security breach rules); and to have to accept the change from the "notice and take down procedure" (obligation to suppress) towards the "notice and stay down" (obligation to prevent reoccurrence).

Authors are also debating on whether the IoT will have profound consequences on contract and consumer law and more particularly on the contours of freedom of contract [1].

In addition, the Big Data phenomenon related to IoT is also raising a number of legal issues. According to an IBM official "The emergence of the Internet of Things has created such a flood of data that only state-of-the-art information technology can gather, filter, order and interrogate the resulting, massive data set, generically called Big Data". The legal questions of Big Data include in particular the ownership of the data, the limits of such data, the legality of their processing and the contracts needed between suppliers and clients (FORGERON, 2012).

With the Internet of Things, the liability of IoT actors, whether statutory or contractual, should be reviewed. Lobbies have already started to fight tooth and nail to defend their respective interests.

[1] PEPPET (2012): "Freedom of Contract in an Augmented Reality: The case of Consumer Contracts", *compared with* "Contract Law in the Age of Smartphones: Do Smartphones make for Smarter Consumers?", *Cornell Journal of Law and Public Policy* Blog.

■ A new interface

The Internet of Things will dramatically modify relationships, not only for machine to machine (M2M) but also for Human to Machine (H2M), and mainly the user interface.

Today, the interface is generally organized around three components: (i) a graphic interface, (ii) the omnipresence of keyboard and (ii) the organization in desktop mode. The interface is indeed mainly visual, activated from click to click and ordered via filing and databases.

With the Internet of Things, there is a threefold mutation. It is no longer "simply" sufficient to access and process information, as the filing and classification of information are meaningless without a new, more intuitive interface. Similarly, the Internet of things is closely interlinked with the "click" – an object interface, which will be replaced by a "behavioral" interface based on movement, voice or touch.

Today, the interface and navigation are decided by graphic designers and computer specialists, but with the Internet of Things, this will change and a war will be waged between the IT world and behavior specialists.

■ Security of things

Security of information systems and the fight against cybercrime are already high on the agenda of the Internet community. The Internet is plagued with virus, bootnet, spamming and identity theft.

The victims of these constant attacks are the connected information systems. They are protected by traditional IT anti-crime rules (intrusion/alteration of functioning/alteration of data), which are constantly enriched as new offences appear, such as identity theft and security breach.

With the Internet of Things the nature and consequences offenses will change: identity theft will no longer target the identity of a connected individual but the identity of the machine, with the objective to retrieve information by misleading one or more machines. Similarly, the security breaches that are today creating concerns for personal data will in the future not necessarily involve personally-identifiable data but other data that will nonetheless have crucial importance for businesses.

As underlined by the European Commission "in the business sphere, information security translates into the availability, reliability and confidentiality of business data. For a company, questions arise as to who has access to their data or how they can grant partial access to their data to a third party. These questions, while in appearance simple, are profoundly affected by the complexity of today's business processes".

As a result, the Internet of Things will necessarily lead to review IT criminal law around two concepts: (i) the protection of identity, as generalized and extended to objects and (ii) the protection of information, which is currently the poor cousin of law. The theft of data and the protection of the sensitive information capital (business secret) will also need to be recognized.

■ War of the machines

Lastly, to end on an optimistic note… let's talk about war!

Defense and military security should not be forgotten. Without necessarily shivering at the idea of a Terminator or Robopocalypse "for real", a war with things or by things is totally conceivable. The ability to mix mind and machine with the IoT, which will dramatically change the structure and function of the armed forces, has been described as a kind of "cloud combat" concept (HIPPLE, 2012).

In the last years, many countries have placed the Internet and information systems at the core of their military preoccupations, just after terrorism and well before "traditional" war.

In 2008, a U.S. report dealt with the law and responsibility aspects of military robotics (Office of Naval Research, 2008). In 2007, South Korea even thought of introducing a robot Ethics Charter (LOVGREN, 2007) to prevent human abuse of robots – and *vice versa*.

The IoT is also going to space. NASA plans to use over five hundred sensors on jet engines to gather information on almost every aspect of their flights. Project engineers say it will show how the engines work in real conditions and will be used to create individualized models that will prevent failures in the future (Accenture & Bankinter Foundation of Innovation, 2011).

France has already addressed the subject of Internet and war in a white paper on defense and national security.

A new step is about to be taken; it is not limited to the information warfare, made possible with Web 2.0 as recently evidenced, with varying degrees of success, by the Arab Spring; but a new form of war: the Thing Wars.

France is to update its white paper in 2012. It will be interesting to see if it will take on board IoT or threat it as a non-event.

■ Prologue (!)

A prologue and not an epilogue? Yes! Because this is just the beginning! As repeatedly underlined in this paper, the questions raised by the Internet of things are numerous and we are far from coming up with answers; there is still a long way to go before identifying (let alone managing) all legal aspects of IoT and it would have been difficult, and even contradictory, to “conclude” on this ever-evolving subject.

This is why this last section is rather more a call to open the debate.

The Internet of Things is not a new technological gadget. It is not the flavor of the month.

"The IoT is not yet a tangible reality, but rather a prospective vision of a number of technologies that, combined together, could in the coming 5 to 15 years drastically modify the way our societies function", as said by the European Commission.

All specialists agree that IoT is more than a network of information and might be one of the keys for a brighter future for next generations.

The Internet of Things might be pivotal in managing old-age dependency. The increase of life expectancy will raise old-age dependency, and will be a bottomless pit. The IoT will help meet the challenges of an ageing society and we can imagine that IoT allows the elderly to be autonomous longer. The financial impacts will be tremendous.

The Internet of Things might play a vital role for greater efficiency in the management of energy, waste treatment and other environmental

constraints. Humans will no longer be alone to cope with these problems, as things will proactively prepare, work out or even impose on us solutions.

No need to monitor the speed of your car according to the pollution index or gas price, the car will take the right call for you!

For these fundamental questions, it is clear that while policy makers have sized up what is at sake, they have still not gotten to grips with them.

In its 2009 Communication, the European Commission mentioned the possibility to propose "if necessary, additional regulatory instruments" (line of action 2)…It further invited ENISA to "take further action as appropriate, including regulatory and non-regulatory measures, to provide a policy framework that enables IoT to meet the challenges related to trust, acceptance and security" (line of action 4 on emerging risks).

The Commission seems to have understood the seriousness of the topic when warning that failing to adopt a proactive approach on IoT would mean "missing an important opportunity and could place Europe in a position where it is forced to adopt technologies that have not been designed with its core values in mind, such as the protection of privacy and personal data.

Yet one only needs to count the number of publications and political interventions about that subject since 2009 to note that Europe is maybe going to miss the boat. Unless….it has decided to act discreetly. But the consequence will be the same as it might be too little too late. There should be no hesitation to preempt every aspect of the Internet of Things, whether technical, economic or legal.

It is a pity that, to date, no major program, tackling all of the above mentioned tricky legal issues, has been launched to anticipate and regulate the development of the IoT in order to master it and not suffer it…

References

Accenture & Bankinter Foundation of Innovation (2011): *The Internet of Things. In a Connected World of Smart Objects*.

BARBRY E. (2007): "Web 2.0: nothing changes… but everything is different", *Communications & Strategies*, no. 68, 1st Q. 2007, special issue "Web 2.0: the internet as a digital common", www.comstrat.org

BENHAMOU B. (2009): "Internet des objets, Défi technologiques, économiques et politiques", *Revue Esprit*, mars avril.

BENSOUSSAN A. & BARBRY E. (2012): "Un tsunami juridique pour proclamer les droits de l'homme numérique", *Revue La Jaune et la Rouge*, avril.

BOURCIER D. (2001): "De l'intelligence artificielle à la personne virtuelle : émergence d'une entité juridique ?", *Droit et Société* 49-2001 (pp. 847-871).

Cornell Journal of Law and Public Policy Blog (2011): "Contract Law in the Age of Smartphones: Do Smartphones make for Smarter Consumers?". http://www.jlpp.org/2011/10/04/contract-law-in-the-age-of-smartphones-do-smartphones-make-for-smarter-consumers/

FIDIS - Future of Identity in the Information Society (2008): "D2.13 Virtual Persons and Identities", 24 March.

FOREST D. (2009): "Qui a peur de l'internet des objets", *Revue Lamy Droit de l'immatériel*, no. 54, pp.45-46.

FORGERON J. F. (2012): "Vous avez dit Big data", www.alain-bensoussan.com, 3 May.

HIPPLE Lieutenant (j.g.) M. R. (2012): "Cloud Combat: Thinking Machines in Future Wars", *U.S. Navvy Proceedings Magazine*, July, Vil 138/7, 313.

LOVGREN S. (2007): "Robot Code of Ethics to Prevent Android Abuse, Protect Humans", *National Geographic News*, March 16.

MASSIT-FOLLÉA F., BENGHOZI P.-J. & BUREAU S. (2009: *L'Internet des objets. Quels enjeux pour l'Europe ?*, Ed. Maison des sciences de l'Homme, Paris.

OECD (2012): "Machine to Machine Communications, Connecting Billions of Devices", Digital Economy Paper no. 192, 30 January.

Office of Naval Research (2008): "Autonomous Military Robotics: Risk, Ethics, and Design", a report prepared for the US Department of Navy, December 20.

PEPPET S. R. (2012): "Freedom of Contract in an Augmented Reality: The case of Consumer Contracts", 59 *UCLA Law Review* 676. http://www.uclalawreview.org/pdf/59-3-5.pdf

SOLUM L. B. (1992): "Legal Personhood for Artificial Intelligences", *North Carolina Law Review*, Vol. 70, p. 1231.