
Inspection Committee

RADIO-FREQUENCY IDENTIFICATION (RFID) TECHNOLOGIES: INDUSTRIAL ISSUES AND SOCIETAL QUESTIONS

Report presented by

**Françoise ROURE, General Inspector
Jean-Claude GORICHON, General Inspector
Emmanuel SARTORIUS, General Engineer**

REPORT No. II-B.9 - 2004 - January 2005

Inspection Committee

RADIO-FREQUENCY IDENTIFICATION (RFID) TECHNOLOGIES: INDUSTRIAL ISSUES AND SOCIETAL QUESTIONS

Report presented by

**Françoise ROURE, General Inspector
Jean-Claude GORICHON, General Inspector
Emmanuel SARTORIUS, General Engineer**

**REPORT No. II-B.9 - 2004
January 2005**

Report no. II-B.9 - 2004
January 2005

Rapporteurs:
Françoise ROURE, General Inspector
Jean-Claude GORICHON, General Inspector,
Emmanuel SARTORIUS, General Engineer

**Radio-frequency identification (RFID) technologies:
Industrial issues and societal questions**

S U M M A R Y

Digital identification is a problem found at the heart of industrial, society and sovereignty issues. It covers physical objects or groups of objects as stocks or flows, digital objects and finally living entities, both animal and human.

RFID technologies cause profound changes in the informational balance of international exchanges based on labelling and managing material assets under a bar code system, for the benefit of widespread traceability and constant control of asset flows, access media to services and the moving of people. **Controlling the network information systems which underly digital identification is now becoming a powerful sovereignty issue in the context of economic war.**

This situation is likely to give a considerable, sustainable competitive advantage to the first to master the technological and industrial supply of digital identification, particularly via RFID technologies, given their *dissymmetrical* access to economic and commercial information that counts in an open, globalised economy.

Marking and traceability technologies have made huge steps forward in recent years thanks to a combination of paperless monitoring processes, reduced costs for information processing media and storage capacities (tags, readers, electronic communication networks, software intelligence) and contactless reading via radio frequency identification.

Substituting RFID chips for barcodes has already started in the professional and general public mass markets. Associated with technological options taken up by influential buyers, including the American Department of Defense, it indicates widespread use worldwide at the service of a rapidly-expanding international trade.

The technological standards and information system architectures which combine the data and produce added-value services at the same rate as the RFID tag memory capacity expands, lead to a **significant concentration of knowledge in the hands of a very reduced number of industrialists, who turn out to be the same chosen for the "technical" world governance of the Internet.** Thus, the company VeriSign has been chosen to manage the root server of the globally integrated EPC Global information network, which distributes the electronic product codes that are taking over from barcodes.

The requirement for traceability will certainly be made easier by radio frequency identification technologies, particularly under the new legal obligations on food and health safety. It also supports anti-pirating and anti-fraud initiatives and productivity gains the length of the logistics chain. Applied to people, their moving, even their purchasing or other conduct, it raises formidable questions on the protection of sensitive personal data, meaning that institutional balances are undermined by the widespread use of RFID. The protection of sensitive personal data may be widely compromised, as may the ability of the public authorities to ensure that the related legislation is respected.

Making traceability widespread is in itself a major economic and societal issue through the quality and diversity of the solutions offered by the RFID technologies for the rapidity and security of the logistics chains overall as well as the upheaval to traditional supply structures in this field.

French and European industry are clearly not involved enough in the dynamics of applied research, standardisation and development of new markets with respect to the considerable industrial and societal issues of radio frequency identification technologies. **The size of the markets, the solutions offered to businesses, individuals (particularly in health and aid for persons with reduced mobility) and the authorities in their quest for a fair balance between greater security and maintained freedom at acceptable cost, productivity gains and measures against pirating made more accessible by RFID technologies are all reasons for defining and implementing a new, clearly-understood public promotion policy for RFIDs that stimulate supply and contribute to innovation.**

The report recommends that the public authorities make every effort to raise the awareness of all stakeholders concerned to the opportunities from radio frequency identification technologies, whilst evaluating their negative impacts to control them better, **starting with the supply stakeholders:**

- raise the awareness of RFID supply and demand stakeholders to the major productivity, innovation and value-creation opportunities from this technology:
- analyse in depth the threats from the RFID technologies, be they targeting people-traceability aspects, the control of economically strategic information for businesses or national sovereignty, particularly with respect to their ease of use, and make the results known to all interested parties to raise their awareness;
- educate accordingly (symposiums, forums, articles), to create confidence amongst the general public and provide public authorities with a weapon in their initiatives to maintain national sovereignty;
- adapt the RFID services offered in the light of feedback received, even introduce incentives to strengthen the French and European offering in this field;
- encourage France to participate in standardisation bodies and international forums on RFID technology, alternative naming and routing;
- encourage professional initiatives, by both manufacturers and end-users, to develop RFID applications likely to generate trust understood clearly by consumers and citizens;
- invest in research on the economic and social effects of the RFID technologies and information systems that underlie applications with a societal focus;
- assess the applicability of the law providing for the protection of personal data from the viewpoint of radio frequency digital identification technology.

CONTENTS

Introduction	1
Part I - Digital object identification and industrial issues.....	2
1.1. RFID technologies and the supply stakeholders.....	2
1.1.1 Definition, technological roadmap, industrial applications	2
1.1.2. The EPC standardisation process	3
1.1.3. The supply stakeholders in the RFID object identification technologies	3
1.2. Strategic relationship between ONS and DNS and the main demand stakeholders	4
1.2.1. Strategic relationship between ONS and DNS.....	5
1.2.2. Demand stakeholders, their requirements and their influence on market development	9
Part II - Digital identification of people and institutional balances	11
2.1. Reminder of French legal provisions; scope and limits.....	12
2.1.1. New resources for CNIL, standing back with regard to new threats	13
2.1.2. Automatic processing, merging of filing systems and the reality of prior consent	14
2.1.3. New technological risks for applicability of the law.....	14
2.1.4. On exercising the right of rectification	16
2.2. The authorities are responsible for the framework set for the digital tracing of individuals, at all subsidiarity levels	17
2.2.1. Protecting digital health identity: context and scope.....	18
2.2.2. The European Data Protection Supervisor	20
2.2.3. European Network and Information Security Agency (ENISA)	21
2.2.4. Specific risks inherent in the centralisation of personal digital data.....	23
Conclusion.....	24
Recommendations	26

INTRODUCTION

The digital identity issues that we are proposing to analyse in this report are restricted to the entire range of technological as well as societal questions raised by the collection, archiving and processing of information using contactless technologies (electronic chips, printable antennas in particular), information systems carrying communicating objectives and especially tracing software programmes.

An institutional approach will therefore focus on items of information whose collection, storage and use taken as a whole may serve to identify a person, regardless of whether or not this identification and/or its use is lawful, by putting the technological choices and changes in the national, European and international regulatory framework into perspective.

An industrial approach will then direct attention towards information that identifies an object, by putting into perspective the global information systems required to develop relevant applications on a worldwide basis.

Our mission has elected to limit its approach to the contactless identification technologies, with their greater development prospects over the next decade, given the very low prices expected from their rapid widespread use, and where the recent positioning of stakeholders around a standard likely to replace barcodes by adding intelligent functionalities opens the way in the short term to mass applications, in response to both civil and military, public and private markets.

The tags, readers and software programmes based on RFID technology together form a radio frequency identification system, with vital contributions from stakeholders well established in the worldwide digital economy (IBM, Philips, VeriSign and Gemplus especially). Other businesses in the supply sector are developing rapidly, particularly, but not exclusively, around the Sophia-Antipolis technological centre in France. RFID technology plays its part in developing unprecedented international commercial flows. It provides a material counterpart for financial flows in terms of international trade digital data flows and therefore in principle sees no halt to its future development. It creates savings by preventing human logistics errors and by limiting "fraud" opportunities regardless of origin.

PART 1 - DIGITAL OBJECT IDENTIFICATION AND INDUSTRIAL ISSUES

1.1. RFID technologies and the supply stakeholders

1.1.1 Definition, technological roadmap, industrial applications

RFID technology (Radio Frequency Identification) - sometimes referred to as smart tags - is at the crossroads of barcode and contactless chip technologies. It has modernised and retained the barcode principle of giving every object an identification code that may be read by a machine. From the contactless chip card it has retained the possibility of reading and even processing information remotely. RFID technology lends itself, therefore, to automating the entire logistics chain, all the more so as the object can be moving or in any position whatsoever, despite continued weaknesses¹. There is nothing innovative about the RFID principle - the *Navigo* pass on the Paris transport system (RATP) and the remote toll control booths on motorways all use it.

Replacing optical reading techniques by electromagnetic techniques gives RFID the upper edge over barcodes, which have to pass in front of a reader window or be scanned by a portable reader (the supermarket cash desk handset). The only difference between the RFID, which can be inserted into the thickness of the packaging or even be printed on it, and the contactless chip card is the lack of the "plastic card" itself. The physical principle remains the same: a microprocessor with an antenna "lit up" under suitable conditions by an electromagnetic field is capable of emitting information it holds or even of processing it.

Distinction is made between:

- read-only or passive tags: here, data (a single identification code that cannot be falsified) are inscribed on the label by the manufacturer and cannot be altered nor added to; end-users can only read the serial number inscribed on the chip;
- read/write or active tags: here, the tag has a storage capacity which may be written to, added to, read or even erased; there is an unlimited number of reading cycles.

RFID may also be classified into four categories based on the frequency bands it operates under:

- low frequency tags (frequency less than 135 kHz), with a few centimetres reading distance;
- high frequency tags (13.56 MHz frequency), with a reading distance of several tens of centimetres; most passive tags use this frequency band;
- UHF tags (868-960 MHz), with a reading distance in the order of one metre;

¹ RFID functions particularly badly in the presence of masses that reflect electromagnetic waves (for example, packaging in metal or containing water).

- microwave tags at 2.45 GHz (same band as the Bluetooth and WiFi standards).

1.1.2. The EPC standardisation process

Standardisation issues are considerable inasmuch as they will ultimately guarantee interoperability between information tags, readers and processing systems and the correct functioning of the system overall under a globalised economy where restrictions on the circulation of goods no longer exist. Standardisation also plays a part through the effects of series and therefore of the cost reductions it creates. There are three basic levels:

- exchange protocols between RFID and its environment;
- radioelectric frequencies that allow the exchanges between RFID and its environment;
- encoding of objects themselves carrying RFID.

ISO has already developed standards for this first point (14443, 15693, 18000 standards family²) which are far from being recognised unanimously. Proprietary standards are still numerous, without mentioning those produced by other interest coalitions like the very recent *EPCglobal UHF generation 2 standard*³.

As for frequencies, a serious problem exists in the UHF band, in principle the most interesting in terms of the potential use of RFID. Frequencies used in the United States (915 MHz) are reserved exclusively for the second-generation mobile telephone networks in Europe and Japan, which restricts considerably the power at which they can be used and hence their range. Europe has adopted the frequency 868 MHz. As it is unlikely that these will disappear before several years, international negotiations will be necessary to ensure interoperability between the American systems and the rest of the world.

1.1.3. The supply stakeholders in the RFID object identification technologies

Industrialists found in the RFID field include:

- major manufacturers of electronic components: Hitachi, Infineon, NEC, Philips Semiconductors, STMicroelectronics, Texas Instruments, etc.;
- major systems manufacturers, able to design, develop, install and even operate systems using RFID, widely based on information technologies

² ISO 18000-2 in the 125-135 kHz band, future standard ISO 18000-3 which should replace standards ISO 14443 (A/B) and 15693 in the 13.56 MHz band, future standard ISO 18000-6 in the 860-9340 MHz band and future standard ISO 18000-4 in the 2.45 GHz band.

³ On EPCglobal Inc., see § 1.2.1.

(database management, networks, etc.); IBM clearly heads this field, but Accenture, Bearing Point, CSC, Unisys and VeriSign are also found here;

- software programme suppliers like Microsoft, Oracle and SAP;
- mobile telephone manufacturers such as Nokia;
- and last but not least, allottees or managers of codes allotted to objects that allow them to be identified, like EPCglobal Inc.

In terms of actual RFID manufacture, note simply that the current major issue is to reduce its current cost dramatically (to around €0.05 compared with today's €0.30), that potential users are comparing unfavourably with the virtually nil cost of a barcode. Given the difficulty of acting on the cost of microprocessors beyond the effects of series, industrialists are focusing their efforts on the cost of antennas and *packaging*. Thus small, innovative companies like IER, Tagsis and ASK at Sophia-Antipolis are filling the niche by developing processes to print the antenna using a simple ink jet on any medium. Even so, the market prospects are just tremendous: word has it that 10 to 20 billion objects will be RFIDed by 2008.

Managing the codes becomes infinitely more important due to its potential consequences and the power issues involved. The non-profit making American body EPCglobal Inc.⁴, a joint venture between EAN International⁵ and the American Uniform Code Council (UCC⁶), has clearly positioned itself in this extensive niche of tagging pallets and cartons; it is offering to manage the Electronic Product Codes (EPC) worldwide and supply a combination service to servers containing information on *EPC*-identified objects. EPCglobal Inc. states that it wishes to link all objects to the Internet and supply a basic transaction service through its EPCglobal Network; this includes localisation of information on a given object, localisation of a given object in the logistics chain and added-value tracing and other services. EPCglobal Inc. confirms that it is only targeting the B to B (business to business) market, not the B to C (business to consumer) market. The potential power it would gain from this central role in worldwide circulation of goods is clear to see in any event. Note also that EPCglobal has entrusted the management of its network (EPCglobal Network) to the American company VeriSign, which manages the Internet domain name system (DNS) amongst other things.

1.2. Strategic relationship between ONS and DNS and the main demand stakeholders

Known for many years for its role in operating the critical infrastructure underlying the DNS and the Internet, VeriSign is developing its infrastructure and expertise to support

⁴ <http://www.epcglobalinc.org/>. Firms such as Carrefour, Cisco Systems, Coca-Cola, Gillette, HP, Metro, Nestlé, Procter & Gamble and Wal-Mart are represented on its Governing Council.

⁵ International organisation representing 101 organisations in 103 countries (Gencode EAN France for France), based in Brussels and with the status of non-profit making association; created in 1977 to develop standards to manage global and multi-business logistics chains. EAN International sets the barcode structure outside the United States (EAN = European Article Number) (<http://www.ean-int.org/>).

⁶ Technical body founded thirty or so years ago in the United States; the Uniform Code Council develops standards and solutions to improve overall logistics chain management. UCC sets the barcode structure in the United States (<http://www.uc-council.org/>).

the root server for the EPCglobal Network object naming service (ONS Object Naming Service).

ONS is one of the services contributing to "higher value commercial processes in the EPCglobal Network". VeriSign is offering the EPC Starter Service (SM) technology, which identifies and quantifies the value of information for monitoring and locating RFID-tagged products created at each step in the object production, transmission and distribution chain for its entire service life, unless deliberately or accidentally deactivated.

1.2.1. Strategic relationship between ONS and DNS

Symbiosis between the Internet and the identification of physical objects was not compulsory. But this merger has simply become logical very quickly in the current context, where the Internet is the all-encompassing bond creating complementarity between those activities that have up until now been related yet distinct.

RFID tags are direct descendants of the barcode. As such, their use could have remained enclosed in a logistics-specific sphere, just like the barcodes over the past thirty years.

But their partisans⁷ immediately saw the fantastic gearing down possible with on-line databases, particularly the Internet IP technologies, to render the process "seamless", thereby making exchange architecture impressively efficient for a derisory extra sum for the infrastructure.

And very rapidly the similarity of the situations led to a copy-paste of solutions invented for Internet routing, the DNS (Domain Name System).

⁷ Basically the MIT laboratories.

- Routing: an irreversible and pressing phenomenon?

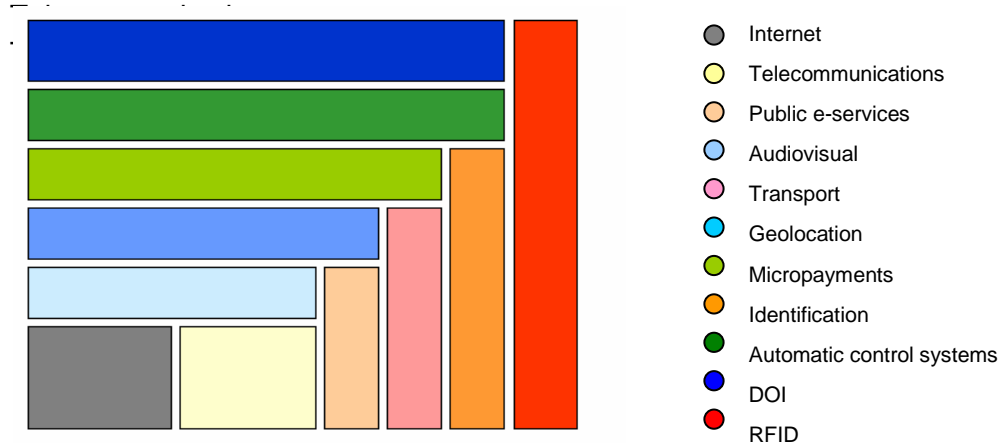
For several years the world has entered into a frenzy of giving a preferably-permanent address not just to physical objects, individuals, road vehicles and animals, all in the name of traceability, but also to all virtual objects, be it e-mail or SMS messages, administrative documents, pieces of digitised music or software micro-slaves (applets, servlets and other so-called "intelligent" agents), which rush tirelessly through the networks swapping bits of micro-information to serve us better, and indeed spy on us better.

The battle is of course not yet won between technologies, standards and industrialists who have entered this war of influence between the various networked worlds.

- Fratricide in the networked worlds

For already these multiple networked worlds⁸, from telecommunications to automatic control systems via people identification, that are repeatedly perceived to be converging willingly on an idyllic merger for the well-being of the end-user, are in fact embarked on insidious fratricide, having all decided to take over the IP world - **and** they are all distorting it and fashioning it to their own specific constraints.

To simplify, these networked worlds could be mapped temporarily as follows.



It may well be possible that these former frontiers between worlds working towards phagocytising the others constantly will not remain intact. Competition promises to be particularly fierce between DNS, ONS and DOI (Digital Object Identifier).

⁸ See presentation in Appendix 4.7.
Centre de traduction Minéfi – Dossier 2388-05-EN – 28/12/2005

- Advanced similarities between ONS and DNS

It is not surprising to find similarities between the first routing method dreamt up for the Internet - DNS - and the routing system in every other world, once the needs are similar.

But thanks to a combination of several factors, the ONS world was definitely the fastest in remaining close to the DNS architecture.

Firstly, the stakeholders capable of applying sufficient weight in decisions are basically the same: the American government with the DoD and the DoC, major industrialists like IBM and the stakeholder rapidly becoming the force to be reckoned with on the Internet planet - VeriSign.

In both the DNS and ONS schemes, the root server has been entrusted by the American government very discreetly to VeriSign, without apparently giving other stakeholders the chance to say their piece. It has to be said that since the American Executive Order of 16 October 2001 classifying the basic Internet architectures as "Defence Confidential", there is little chance that light will ever be shed on this designation.

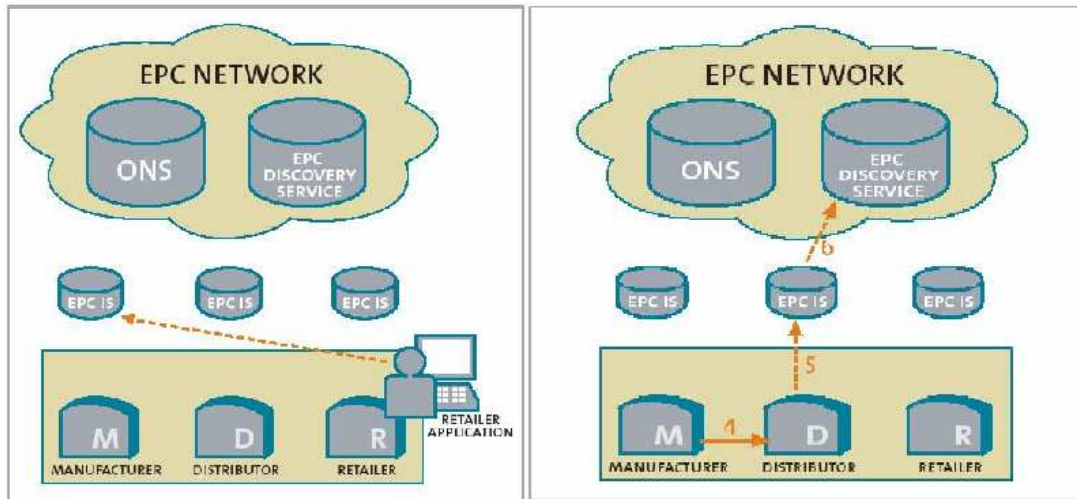
In our view, the difference in size relates to the second-level servers. Geographical breakdown has been kept in DNS, whereby each State maintains control over the operator for the addresses relating to its geographical territory.

For the EPCglobal and ONS standards, this geographical breakdown has disappeared completely. The secondary servers belong to major industrialists, multinational corporations which are known to resist all attempts by States to control them. Here, at least, it can be deduced that the UN debates over what place States should hold in efficient governance of the Internet will no longer apply.

Like the flows, the number of objects to be identified, the number of sub-contractors and distribution warehouses are several times more than the number of internet sites; the odds are that the ONS (or at least its incontrovertible stakeholders) could rapidly phagocytise the Internet we know, thus turning the modest attempts by the Government Advisory Committee (GAC) and the World Summit on the Information Society (WSIS) into wishful thinking.

The diagrams below illustrate the three architecture levels:

- first level: a root server (ONS), accompanied by its whois (called Discovery Service here)
- second level: servers specific to professionals (manufacturers, wholesalers, etc.)
- third and last level: access to end-users, including in particular major retail outlets (VeriSign graphics and captions).



Retailers and other parties have real-time view through the EPC Network

Distribution information is available to all parties

What does appear open to question and which could put a brake on the increasing popularity of a model such as this is the risk of economic intelligence that encourages such architecture. Nothing says that the industrialists are going to leave every stakeholder in the various spheres free to interrogate their own bases and compile economic and behavioural data that the model gives a glimpse of.

It is amazing to note that, apparently won over by the unquestioned advantages glimpsed in the "seamless" management of their physical flows, European manufacturers on EAN or EPCglobal steering or monitoring councils are very discreet on the undoubted risks that such centralised architectures put on information vital for their competitiveness, progress and know-how.

Similarly, the various forums, be they professional like ETF or more institutional like WSIS, focus insistently on the turning of certain wheels (like the Internet Corporation for Assigned Names and Numbers - ICANN), but omit systematically to invoke the increasing, even inappropriate place taken by some private stakeholders in the Internet sphere.

In our view it is time that the European authorities, who are scrutinising carefully the computing world (cf. the Microsoft case), extend their watch to neighbouring "worlds", including the Internet, and assess the conditions in which VeriSign spreads its net over the most sensitive sections in managing networked worlds.

In any case, it seems important to us at this stage to warn the government on these drifts potentially very damaging to the economic integrity of entire sectors of the economy.

Why, for example, should all exchange data in French industry (luxury goods, aviation, pharmaceuticals and so on) be made available centrally *in real time* to a single company with as yet unproven ethics on the subject?

Indeed, when it comes to the Internet, this same company is already clearly judge in its own cause, as it maintains root servers under contract to the American government whilst elsewhere managing several tens of millions .com (and .net) addresses commercially, as well as certifying encrypted links and ensuring their confidentiality (including for some essential French government departments!).

1.2.2. Demand stakeholders, their requirements and their influence on market development

Given the appeal of its low cost and high added value in the roadmap generally accepted by RFID tagging and reading professionals, RFID and the currently-forming EPCglobal Network have between them the potential to make this technology totally part of everyday life in all areas of the objects logistics chain, plus movements and conduct in living units in the animal and plant kingdoms: living animals under compulsory health monitoring, humans for their conduct as (cyber) travellers, consumers (including health and safety systems) and citizens.

In Korea, a country that has invested €100M over four years in an Ubiquitous Sensor Network plan in an attempt to become an RFID leader by 2010, a major retail store chain invites the consumer to follow the itinerary of the beef he is eating on its Internet site...

The reasons for adopting RFID are economic. It reduces inventory and supply manpower costs, plus losses from shoplifting and forgery. Economies in the major retail logistics chain would be in the order of 6 to 7% (AT Kearney study quoted in the DREE report, see bibliography).

The usage cost for a standard EPC should be increased by the cost of paying the RFID technology patents held by the American company Intermec; the extra cost from payment of royalties would be some 5 to 10% of the price of the electronic chip according to EPCglobal. All other manufacturers have donated their patents, so that the EPC standard is free of intellectual property royalties.

At this stage an RFID tag costs more than a barcode, but direct comparison is impossible if the added possibilities of collection, storage and use of additional data are taken into account. Significant cost reductions are expected from both mass production and technological innovations such as printing.

The first demand stakeholders will certainly influence the worldwide normative approach. Are concerned: major retail outlets with Wal-Mart and Marks & Spencer; the terms and conditions for accessing procurement contracts by the American Department of Defense (DoD) and its agencies for tagging objects; the specifications of the DoD's Wireless Global Information Grid (WGIG) in its contactless dimension, not forgetting the major consumer industries (Coca Cola, Gillette, Nestlé and Whirlpool Europe in particular), petroleum product distribution (Exxon Mobil) and transport companies (RATP, motorway toll companies, etc.).

RFID tags are used on loyalty cards distributed by Metro in Germany or for express freight services (DHL) or to measure the quality of the international postal services (Posteurop).

An influential stakeholder given the number of its suppliers and the quantity and diversity of its procured products in logistics, the DoD has opted for an integrated digital object identification strategy. It has approved the 860-960 Mhz frequency band for the passive RFID tags. According to its internal regulations, which may be consulted on its Internet site www.dodrfid.org, these tags will match the specifications of the EPCglobal consortium class 0 and 1 passive tags. They should be applied to all despatches and every pallet unit. From 1 January 2007 will be added a far more detailed object tagging system under the Universal Identity registry concept, illustrated graphically in Appendix 4.1.

The policy of radio frequency identification based on active tags was explained by the American Under-Secretary for Defense on 30 July 2004, the idea being to provide global visibility of mobile entities. This service should be propped up by an Internet network infrastructure functioning under the following diagram: data provided by RFID tags will be transported to so-called regional visibility servers, then routed towards the global information transport network. A centralised structure will maintain relations with the regional servers, including the secret Internet protocol routing network (ITV server on the Secret Internet Protocol Router Network - SIPRNET). This server will be responsible for ensuring the interoperability of these data thus centralised with the armed forces global support system, the global control and command system and other classified information systems. (See Appendices 4.2 and 4.3).

Although an audit by the General Accounting Office (GAO), the American agency in charge of auditing the Federal accounts, has its doubts over the ability or indeed the willingness of the various units in the American armed forces to adopt such a centralised and global system, the budgetary resources have been made available, by forced marches.

Another major factor influencing the market will be the position taken by the Chinese standardisation bodies on RFID. The development of the internal Chinese market must be taken into account in addition to the export markets and the resultant delocalisation of international stakeholders to this country. Although RFID technology is itself neutral, within the limits of the toxicological and ecotoxicological impact from the materials used (nanotechnologies according to the roadmap timetable), it raises tremendous societal questions in addition to the technical (frequency availability and harmonisation) and economic (speed at which costs fall) brakes to its widespread use in the short term.

The example of the debate over paying for anonymity for the weekly and monthly RATP tickets under the widespread application of the Navigo system illustrates **the uncertainty as to societal acceptance** with respect to the ergonomics in use provided by the technology. Should one pay to remain anonymous in daily transport is a question provoking a negative response from the *Commission Nationale de l'Informatique et des Libertés* (CNIL - data protection authority). The emergence of this type of debate is caused by contactless technologies becoming commonplace. Should strict economic necessity prevail and if yes, with what effect? **Here, the fragile distinction between the identification of people and of objects is particularly tangible.**

PART II - DIGITAL IDENTIFICATION OF PEOPLE AND INSTITUTIONAL BALANCES

When referring to individuals, we shall only use the term **identification**; although the recent law on bioethics authorises human genome sequencing phases to be patented in some cases as an innovative process, there is no question at this stage of a genuine digital human identity.

Nevertheless, the question of digital human identity is beginning to rear its head globally, over and above now conventional elements such as digitisation of name, first name, date of birth, home address and signature and registering people with a number in the national identification register of individuals or in an international register (for example, in the so-called Schengen II information system - SIS II).

In August 2004, the Japanese authorities allowed cloning of human embryos for medical research purposes, where genetic digital databases could represent a digital identity component. Human biometric databanks will undoubtedly flourish, including commercially, thus raising the question of anonymity and consent.

Other factors making up digital human identity are being developed under pressure of requirements for safety, public order and counter-terrorism: digital imaging of the face, iris and fingerprints, medical digital imagery of all or part of the human body, including brain fingerprinting (already used in the USA courts of justice in criminal trials). The single medical file created by law should speed up the move in France towards the definition and public and private use of digital human identity.

By accessory we mean the digital identities relating to communicating objects and digital services, insofar as the purpose with the most pressing issues focuses on the gathering, by all lawful or illegal means, of personal and non-personal digital data, which may be used to identify an individual - and his conduct.

For all that, this information and its processing, mainly a product of transactional economics (free or market-based), itself represents a significant accumulation of value, directly and indirectly, and therefore clearly justifies that the public authorities in charge of industry and the information society be in a position to understand and anticipate the changes, to carry out their mission properly. They are therefore fundamental from an industrial viewpoint.

French law provides for the processing of personal data but seems behind in the possibilities of merging digital information. When correctly organised, this allows the use of a set of data, which taken in isolation do not fall under the scope of the law and which together result not just in identification but also in the establishment of a status and conduct profile, depending on the purpose actually being pursued.

The existence of this combined information, along with its actual purpose and use, is not yet under the control of the members and officials of the CNIL.

The result is that the spirit of the law may easily be circumvented in fact, particularly when the obligations of the controllers cannot be applied, let alone controlled, given the extraterritoriality of the contravening actions.

2.1. Reminder of French legal provisions; scope and limits

Act no. 2004-801 of 6 August 2004 on the protection of individuals with regard to the processing of personal data, amending Act no. 78-17 of 6 January 1978 on data processing, files and liberties, transposed in particular the provisions of the European "privacy and electronic communications" directive of 12 July 2002.

In Article 1 it defines precisely personal data and how to decide on the identifiable character or not of a person.

Thus "personal data shall mean any information relating to an identified natural person or a person who can be identified directly or indirectly, by reference to an identification number or to one or more factors specific to him or her".

"To determine whether a person is identifiable, account should be taken of all the means available to or accessible by the controller or any other person to identify him".

The legal definition of processing is neutral with regard to the technologies used, as "processing of personal data shall mean any operation or set of operations which is performed upon personal data, *regardless of the process used*, in particular the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".

Combining random factors to identify and ultimately establish a profile or other is taken into account here, particularly by the terms alignment and combination.

Note that community law is more specific than French law in the list of data potentially assisting in identifying an individual. In accordance with Regulation (EC) no. 45/2001 of 18 December 2000, "an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number **or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity**".

The applicability of French law to controllers is of necessity limited to their establishment on French territory, or their recourse to processing methods located on this same territory, excluding processing used solely for transit purposes by one of the member States of the European Union.

One obligation imposed on controllers is the prior information of individuals where the intention is to transfer personal data to a State that is not a member of the European Union.

In particular, "any person using electronic communications networks should be so informed clearly and fully by the controller or his representative:

- of the purpose of any action attempting to access, via electronic transmission, information stored in his/her terminal connection equipment, or to place, by the same means, information on his terminal connection equipment;
- of the means available to him/her to object to this".

The Act also gives any individual the right to:

- object, for legitimate reasons, to personal data relating to him/her being processed:
- to object, without charge, to data relating to him/her being used for commercial canvassing by the current or subsequent controller.

Identification without the knowledge of the data subjects is therefore clearly illegal and duly punished, and contravening individuals or corporate bodies are liable to criminal proceedings for violations of the legal provisions listed in and penalised under Articles 226-16 to 226-24 of the French Penal Code.

2.1.1. New resources for CNIL, standing back with regard to new threats

The Chairman of CNIL, Mr. Alex Turck, when presenting the body's annual report on 22 June 2004, underlined three possibilities for capacity building for this authority - inspecting individual items on site despite opposition from the inspected bodies, announcing pecuniary sanctions up to €300,000 and lastly playing to the full its new advisory role in international negotiations by the government or in the granting of approval for operating codes or software programmes designed to protect personal data.

Note that the processing of biometric data to authenticate or control the identity of individuals has to be authorised by decree approved by the *Conseil d'Etat* based on a reasoned opinion published by CNIL.

The full and complete application of the law nevertheless seems subject to a dramatic change in behaviour by the responsible stakeholders, in the sense of increased awareness and responsibility. CNIL estimates that the declaration rate for SMEs is only 30%. As for the 700,000 associations listed, only 7,000 member files have been declared since 1994. This involves individuals duly identified by the Register of Trade or an administrative declaration, but are all the stakeholders in digital file processing definitely identifiable from French territory and allowed sufficient time to assert their right of rectification?

Among the four focal points for the new CNIL as defined by its Chairman - communication, correspondent, control and coercion - the area of verifications still needs to be boosted both initially and afterwards; qualitatively, through major investment in the

understanding of techniques, particularly extraterritorial, and by combining multiple data, and quantitatively, to remain in proportion with the potentially exponential developments towards which the expansion of the information society has already led us.

2.1.2. Automatic processing, merging of filing systems and the reality of prior consent

Although prior consent is supposedly given for all types of data, how can individuals be guaranteed that their private lives are respected faced with processing operations to merge filing systems? The law clearly considers alignment or combination as processing personal data, but the applicability of the law with regard to the many people potentially involved (current and future controllers, sub-contracting via communication to third parties), much less subject to the risk of sanction or penalty under actual delocalisation, is up against significant difficulties that should not be underestimated.

Some personal data are collected, stored and processed via automated identification, which on the face of it is supposedly known by the end-user and accepted by him; for example, data may be collected automatically via an electronic gate or by using a GPRS or GSM or RFID antenna. For all that, nothing leads to the assumption that prior consent is given on the *purpose* of a filing system combining data making up the identity and, beyond that, individual conduct, and which is being collected on behalf of a third party.

The risks incurred by people over the respect of their private lives simply through automatic data processing are taken into account in Article 19 of the Regulation (EC) mentioned above. They are so well-known that only special circumstances may authorise this type of processing for decisions with legal consequences.

Thus: "the data subject shall have the right not to be subject to a decision which produces legal effects concerning him or her or significantly affects him or her and which is **based solely on automated processing of data intended to evaluate certain personal aspects relating to him or her, such as his or her performance at work, reliability or conduct**, unless the decision is expressly authorised pursuant to national or Community legislation or, if necessary, by the European Data Protection Supervisor".

For information, the single denunciation prosecuted out of the nine cases put forward by CNIL in 2003 relates to an illegal and underhand collection of personal data from directories without the data subjects having been able to exercise the right to object, a "technologically" simple case, if such a thing exists. The mesh of the net therefore seems very wide as far as practices are concerned.

2.1.3. New technological risks as regards the applicability of the law

When Cisco Systems, a major world player in routers used in the Internet network, acquired from the Californian company P-Cube the technology whereby IP telephone operators (VoIP) can identify their "subscribers" - i.e. free end-users like for the Skype service, or paying customers -, it announced its intention of offering to its own operator

customers ***new capabilities for controlling and managing services such as VoIP, interactive games, on-demand videos and peer-to-peer, or creating specific offers.***

This means that with the expansion of uses for the Internet thanks to the progressive widespread use of high and even very high bandwidth, personal practices, both private and transactional, will actually be subjected to an exponential increase in automatic recordings of personal data and therefore a surge in the number of combinations materially achievable of corresponding digital filing systems, over time and space.

Faced with the current issue of worldwide Internet governance for general interest purposes, how can the obligations on erasing and making anonymous traffic data required for establishing communications and for billing be applied in the European Union and in France? (see Article 37 of the EC Regulation quoted).

In particular, the ever-increasing swing away from voice traffic, the traditional telecommunications networks, towards the all-IP, coupled with the growth of communication IP operators through the lowering of technological and financial barriers means that the application of the law will require not just major investment in the effectiveness of control methods but also in their financing to an adequate level. Failing this, the entire architecture of trust, patiently shored up, will be weakened for a long time.

In addition, the "free-of-charge" downloading of software programmes and sometimes also of IP communications now negates any chance of referring to traditional criteria of operator liability in a conventional, contract-based transactional economy (subscription), making the signs even more tenuous when seeking liability for violation of the law, i.e. collection for unlawful purposes, transfer in real time for processing by "third parties" towards countries with insufficient protection of personal data according to the European Commission, as the processing is not subject to obligations of disclosure or prior consent that protect the individual.

For information, the Luxembourg-based Skype, created by the founders of Kazaa, has recorded seven million people downloading its freeware since it started up, manages 1.2 million calls per day, owns no network, spends practically nothing on advertising its service and employs fifty people (*Wall Street Journal Europe 25 August 2004*), which characterises economically and technologically the very low, virtually nonexistent threshold for entry onto the market.

The speed at which the IP voice model is taking over from traditional telecommunications networks is already conveyed in the forecasts by financial analysts, who note the falling profits of the giant telecommunication industrialists. Thus AT&T has seen its profits fall by 18% over three years; the share value is assessed downwards, sometimes as low as the junk bond.

Beyond the problems raised by freeware in terms of responsibility for collecting and processing information for identity or identification, the question of prior consent is raised even more acutely for on-board processors, where no opt-out option exists by definition. Built-in digital handcuffs is the nickname given to this type of chip the other side of the Atlantic. To our knowledge no "free" processor exists following the example of the freeware.

Electronic chips scheduled for the data processor manufacturing lines at the end of 2004 must include specifications adopted by the TCPA (Trusted Computing Platform
Centre de traduction Minéfi – Dossier 2388-05-EN – 28/12/2005

Alliance); Microsoft and Intel are both members of this group. They put forward excellent arguments for the safety and protection of intellectual property rights. The downside of the innovation is that it can sometimes be impossible to choose to exercise the right to refuse automatic data collection.

In September 2002, the computing department of the Academy of Sciences in China announced the manufacture of the "dragon chip" processor based on RISC (not CISC) architecture, which uses a Chinese version of Linux, officially for reasons of security of information systems in military applications.

In both cases, the technical specifications should be studied in the light of the applicability of the law.

2.1.4. On exercising the right of rectification

The global legal architecture of obligations, sanctions and penalties is based on the notion of a controller, defined as any organisational entity which, alone or in conjunction with others, determines the purposes and methods of processing personal data.

This definition can potentially apply to so many entities simultaneously that it becomes virtually impossible - already - to exercise the right of prior consent, retraction of this consent, even temporary, or rectification in the widest sense. How can controller(s) be definitely identified? Where are they located exactly? The time taken by each data subject to check that his/her digitised personal data are duly protected from illegal purposes or without prior consent is infinite, given the uncertainties weighing on the successful conclusion to his research or request.

The "freedom" of the right of rectification, vaunted as a principle in legislative practice, then becomes entirely theoretical.

How under these conditions can respect of the law on prior information be imposed and subsequently the new Article 43 of Act no. 78-17 amended cited above be applied, where "any individual justifying his identity may require the controller to rectify, complete, update, block or erase, depending on circumstances, personal data that is inaccurate, equivocal, out of date, or where its collection, use, communication or storage is prohibited"?

Even more so, how is it possible to check effectively that a controller has made **reasonable efforts** if data have been transmitted to a third party, to be able to notify operations undertaken in the context of exercising the right of rectification (paragraph 4)?

2.2. The authorities are responsible for the framework set for the digital tracing of individuals, at all subsidiarity levels

When carried out under the responsibility of the public authorities, merging personal digital data filing systems can raise questions as to the democratic control of the purpose for a processing operation that turns out to be abusing the legal provisions.

The same technologies giving governments free rein to broadcast programmes and services, whether interactive or otherwise, by multiple applications of national, regional or local electronic government may, "in unscrupulous hands", be diverted from their initial purposes to monitor and control citizens outside the control of a judiciary procedure or any applicable legal provisions.

For France, the lawyer Etienne Wery, in an Internet article published on 11 August 2004, points out in this respect that the Constitutional Council was not required to give its opinion on whether it was right, under the Constitution, that the creation of a police record containing sensitive data was no longer dependent on a decree approved by the *Conseil d'Etat* with the favourable opinion of the CNIL, for it was not asked the question; a fact that *seems* to imply consensus, at least in the short term, of the French political class on the subject.

Symmetrically, with the widespread application of electronic government models, the public authorities that use digital personal data to identify or assist in identifying and authenticating individuals, must be totally protected against any intrusion into their information systems.

They must ensure that their information networks are sheltered from so-called cognitive hacking, that attempts to introduce one or several sources of disinformation, especially on identification factors used in e-government applications, to modify the conduct of public officials and the data subjects without their knowledge.

Whether public or private bodies are involved, one of the threats hanging over the management and life cycle of tangible objects - visible or otherwise to the human eye - and intangible objects is usurpation of digital identity. This may be involved in the radio frequency tracing phase (intelligent radio frequency tags taking over from the passive and static barcodes) or through software (electronic "tattooing" for identification and recognition purposes).

These questions are yet to be resolved technically in international civil standards.

Thus, usurping the domain identity of an e-mail address, highly prevalent via spam, but not just there, was the subject of a call for comments that were to be sent by February 2005 within the framework of an IETF Working Group under the so-called "Marid" protocol entitled "Sender ID: authenticating e-mail". Binding standardisation seems impossible before some time (several years, if appropriate).

Faced with the extent of this worldwide phenomenon, internet surfers have adopted the English neologism of *phishing*, a contraction of *ishing* and *phreaking*, or computing

fraud, to describe the sending of an e-mail falsely claiming to be a company or other body with a reputation for trust, for the purposes of collecting sensitive information from the addressees.

What balance should we be striving for, between the "big brotherism" of the all-electronic and the model acknowledged as ideal, decentralised, respectful of the status of personal data on the privacy of citizens, their health, heritage, income and family? The self-regulation of private stakeholders has not inspired confidence, whilst State interventionism still incites paradoxical expectations of greater security as well as greater freedom - when this does not involve radical distrust of public action in countries that are gradually moving away from a planned economy.

But in any case there is no doubt that, as the authors of the report on the Hyper Republic submitted by Pierre de La Coste to the Minister of State for State reform in January 2003 state in their conclusions, failing the determination to exercise due diligence, "it is not impossible that the Orwellian nightmare comes to pass, but not in the form originally intended by its author".

"For the major groups holding the keys to the information technologies will not hold back from decompartmentalising and crossing personal information coming into their possession in place of States and will break down the derisory legal barriers that these attempt to put up against them, particularly in France. Big brother, far from being the Head of State, will be its worst enemy".

A new scope to the law under the health and sickness insurance reform has opened up in France and merits special attention.

2.2.1. Protecting digital health identity: context and scope

Information system security technologies are used by numerous private stakeholders as tools contributing to the protection of data for the controllers; stakeholders in monetary exchange head the field in this, shortly to be joined by the health professionals.

The implementation of the personal medical file, created by Article 3 of Act no. 2004-810 of 13 August 2004 on health insurance, will in this respect represent a special challenge in defining the factors making up the personal data and their digitisation, collection, processing and use. The entire population covered by health insurance in France is involved, in other words nearly 60 million people.

Created under an authorised system hosting personal health data, the personal medical file will have restricted access and, in particular, will not be accessible by occupational medicine nor under the signing of additional protection contracts covering health expenses. A decree approved by the *Conseil d'Etat* with the favourable opinion of the CNIL will set the conditions whereby an identifier could be used to open and maintain the personal medical file.

A GIP (public interest group) called *Institut des données de santé*, formed under Article 64 of the said Act, has the task of maintaining consistency and monitoring the quality of the information systems used for sickness risk management as well as assessing the

availability to its members, for the purposes of health risks or for public health concerns, of data produced by its members' information systems.

A new step towards digital human identity will be crossed with the creation of this digital medical file. This wonderful technical opportunity, with its promise of substantial savings for increased efficiency at the service of those insured, should be surrounded by precautions for use and sanctions against all violations that are commensurate with its potential risks of abuse. We will discuss this point further in the context of European regulations on digitised personal biometric data. The opinion of the CNIL will carry considerable societal responsibility in this field.

Community law is based on Article 286 of the Treaty establishing the European Community, under which "Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty."

The so-called safe harbour provisions on the level of protection of personal data exported towards countries that are not members of the European Union were bolstered by a Commission decision of 27 December 2001 on the standard contractual clauses for the transfer of these data to processors established in third countries by virtue of Directive 95/46/EC.

In particular, they recall the obligations of the exporter of data "who is the controller of the personal data transferred" and liable for compensation in the event of a remedy, with the right to exercise a remedy against the importer being the exception. Here also questions may be raised over the applicability of the principle of free recourse in long and complex international procedures, in addition to the difficulty in tracing and establishing technical proof.

Microsoft interprets these safe harbour provisions by including in its privacy statement (available at <http://privacy2.msn.com/en-us/fullnotice.aspx>) that it "abides by the safe harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use and retention of data from the European Union". It specifies that MSN does not "use or disclose sensitive personal information, such as race, religion, or political affiliations, without your explicit consent", which supposes nevertheless that it would be capable of doing so, if necessary.

Community law on personal data protection has recently been finalised. It responds to the contrasting requirements of the civil society, which demand both increased, guaranteed respect of privacy protection rights and trust in the institutions to maintain public order, particularly against terrorist actions.

The "privacy and electronic communications" directive quoted earlier is an attempt to update the directive of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. It takes into account the introduction of new digital technologies into the European Union and new electronic communication services brought about by the gradually widespread use of the Internet and

its procession of new data collection and processing opportunities relating to individuals and their privacy.

It has clearly grasped the measure of the risks when it states that **"so-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users" (recital 24)**. It estimates that "the use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned".

It also recognises that these devices, cookies for example, may turn out to be absolutely essential, for example to authenticate and control the identity of users carrying out on-line transactions, but subject to clear information and a "right to refuse".

It also admits that data giving the geographical position of the mobile terminal equipment may be produced more accurately than is strictly necessary to establish a communication and that they are used to offer personalised value added services such as traffic information and guidance. Here again the directive recommends that the provider obtains prior consent (Article 9), with the possibility, using simple means and free of charge, of temporarily refusing the processing of localisation data even when agreement has been obtained.

Three recent provisions under Community law deserve special mention - the European Data Protection Supervisor (appointed on 22 December 2003), the European Network and Information Security Agency (created by a Council and European Parliament decision on 22 November 2003) and the proposed visa information system following the conclusions of the Justice and Home Affairs Council of 5 and 6 June 2003, incorporating biometric data.

The intentions pursued by the European legislator in all three cases appear to be in line with the expectations of the civil society; for all that, in each case, we are forced to recognise the difficulty raised by the final decision and the occasionally considerable delays in its implementation, even the apparently minimum application of the community documents finally adopted.

2.2.2. The European Data Protection Supervisor

The European Data Protection Controller institution was created under Article 41 of the regulation adopted on 18 December 2000. The EC Treaty called for a tripartite decision to be taken before 1 January 1999, based on the procedure provided for under its Article 251, instituting an independent supervisory authority responsible for monitoring the application of the obligation of data protection by institutions covered by the Treaty.

The regulations and general conditions governing the performance of related duties were only decided by the European Parliament, the Council and the Commission on 1 July 2002. The decision of the European Parliament and the Council on the appointment of the independent supervisory authority provided for under Article of the EC Treaty was not published until 17 January 2004, opening the way for the appointment of Mr. Johan Hustinx (Netherlands) and his deputy Mr. Joaquin Bayo Delgado (Spain) for a five-year term.

Centre de traduction Minéfi – Dossier 2388-05-EN – 28/12/2005

All in all, the delay between the intention expressed by the European legislator and effective implementation amounted to five years, during which the Internet revolution had taken place in the European Union and the developed world.

For the future, Article I-51 under Title VI of the draft European Union constitution entitled "The democratic life in the Union" confirms the right of any individual to protection of personal data concerning him/her and places compliance with the rules relating to this right within the scope of Union law for Union institutions, bodies and agencies. Compliance with these rules shall be subject to control by an independent authority.

The European Supervisor made no mention of the evaluation of the impact of changes in information technologies on data protection among the five short-term missions presented to the Polish Diet on 26 May 2004. He simply mentioned that one of his major duties was to monitor relevant developments insofar as they have an impact on the protection of personal data. He omitted to quote the end of paragraph e) under Article 46 of the founding regulation, which says: "in particular the development of information and communication technologies".

He nevertheless fully acknowledged the impact of counter-terrorism, as waged by the United States and the European Union, on his institution's work load. He had taken the initiative to contact Mr. Gijs de Vries, the European Union Counter-Terrorism Coordinator. He could be called on to formulate opinions and advice, over and above the so-called safe harbour agreements for the security of cross-border data agreements, on the very sensitive issue of the transfer of data relating to airline passengers, given the diverging positions taken by the European Parliament and, subsequently, by the European Commission on its decision, which has not been accepted unanimously.

It is advisable to await the first activity reports from this new European institution to assess the results obtained from the missions entrusted to it.

With fifteen staff employed full-time and a double-network operation involving the delegates of each community institution and the representatives of the member States within the so-called Article 29 working group (for the implementation of the 1995 directive), this institution certainly has the potential to implement the technological watch it needs and which is expressly mentioned in its founding text. It nevertheless has to recognise the strategic importance of this, which does not really appear in the only public communication available on its Internet site.

2.2.3. European Network and Information Security Agency (ENISA)

Founded following the events of 11 September 2001, in the context of commonplace logic attacks via the Internet and in response to pressure from e-commerce stakeholders, the European Network and Information Security Agency could, originally, have wished to perform major missions of general community interest.

The decision of the European Council of 18 February 2003 found in favour of the Commission proposal to create a working group on cybersecurity. It invited the member States to develop training and awareness-raising programmes, particularly for young people, on the problem of information system security.

The Agency, which has been legally operational since January 2004 with a budget allocation of €24.3 million over five years, finally has a Management Board on which each member State is represented, in accordance with the agreement signed between the European Parliament and the Council on 20 November 2003. Henri Serres, Central Director of Information Systems' Security, is the French representative.

ENISA's vocation is to advise and assist the Commission and member States in understanding the threats hanging over the security of information systems and in their dialogue with industry, be it over infrastructures or digital data assumed to be sensitive, whether or not of a personal nature.

Its role is more accurately to identify the problems relating to hardware and software offered on the internal market; to collect and analyse data on security incidents in the European Union and explain the emerging risks; to promote appropriate methods to assess and manage risks to build up capacity against threats to information security; and lastly, to increase awareness and cooperation between the various stakeholders in the sector by developing, amongst other things, the public-private partnership.

At this stage, it is not explicitly mentioned that the new risks of breaches in legislation on the protection of personal data which are made possible by recent technological developments and are likely to come into play through the combination and use of networks and information systems come under the ENISA missions. Nothing in the texts for all that suggests that this should be excluded.

Here also, the first ENISA reports will show if this Agency intends to consider the complex subject of the potentials and threats in digital identification of individuals and identity of objects and services, and if so to what extent, under its dimension of compliance with the European legislation on personal data understood as one of the key factors of the trust placed by European citizens in the goods and services on offer in the European information society.

The current positioning, now in the start-up phase, seems to be of an observer, with measures for implementation being within the competence of each member State. The use of the community programme Modinis 2003-2005 to monitor the e-Europe action plan could be a way of taking the close relationship between trust and protection of personal data into consideration in the search for an efficient level of security for the information systems.

2.2.4. Specific risks inherent in the centralisation of personal digital data.

Regarding the centralisation of data, it should be noted that the so-called Article 29 working group on data protection made a statement on 1 August 2003 on the use of biometric data. Despite adopting a very balanced approach with regard to the potentials and risks, it nevertheless insisted on the special dangers of any centralised system of images and digital identifiers.

It recalled that several national authorities have found in favour of storing data by means belonging to the individual himself, such as a smart card, bank card or mobile phone, but recognised the impracticability of recognition without a system using a digital image to make the verification.

It underlined that, in some cases, biometrics could *increase* the respect of privacy when this type of data rendered superfluous the cross-checking with other identification data such as name, first name and address.

It nevertheless insisted on the illusion of total trust that could be associated with these digital identifiers, both by lowering vigilance on the protection of privacy due to common use from childhood (access to school catering, use for lending books in libraries especially) and also, more serious, through the near-impossibility of proving hardware failure which could potentially create major prejudices and considerable difficulties in defending it in court, if necessary.

How will European Union citizens be able to account for any error and exercise their right of rectification? What would be the real cost? What compensation for damages suffered, if appropriate? What will be the delay in obtaining the information and notice of rectification?

The Article 29 group concluded finally by expressing its decided preference for systems based on biometric data where the collection, digitisation and purpose of processing do not take place without the knowledge of individuals from traces they have given without paying attention (fingerprints, DNA, etc.), that are not centralised in a single system nor lead automatically to a combination with other systems and files by their very technical architecture, and which make it easier for data subjects to control processing based on personal digital data.

The European Parliament adopted a Parliamentary legislative resolution on 2 December 2004 on the proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports, along the lines of the Article 29 group's recommendations. It adopted an amendment to Article 1 of the regulation according to which **"no central database of European Union passports and travel documents containing all EU passport holders' biometric and other data shall be set up"**.

CONCLUSION

The report has shown the emergence of a digital entity identification technology, developing the most rapidly in the field of logistics, as an addition to the barcode technologies at this stage.

The technological roadmap of the RFID tags, the acceleration of stakeholders being equipped with information systems used to develop efficiently an understanding of stocks and flows as well as knowledge on movements and conducts, open up considerable market prospects that far exceed ultimately a fully-digitised, contactless system, with worldwide interoperability, taking over from the barcode system.

The alignment, even the identity of the most significant stakeholders in the Internet domain naming system (DNS) and object naming system (ONS) infrastructures, suggests uncontrollable drifts in capturing commercial, economic, financial, technological - in a word, strategic - information.

Awareness of a concentration of powers of intervention in the hands of just a few stakeholders, bolstering the American leadership in controlling the information systems, is still slight, not to say non-existent, both for the stakeholders in the marketplace and for the public authorities in France and the European Union.

For the protection of digitised personal data and unlawful use of identifying data relating to an individual or his conduct, France and the European Union continue to seek an institutional balance.

The increase in collection and processing opportunities through interoperability and exporting of data to "third parties", the introduction of relations with varying degrees of contractual formality between private and professional Internet stakeholders and the extensive expansion of electronic government are all creating a true dilemma for the civil society, with its occasionally contradictory expectations hardly helping the public authorities to choose the most appropriate policies easily.

Binding legal instruments henceforth exist to expose the limits and sanction punishable uses. Nevertheless, the inadequacy of the technological watch and delays in adopting appropriate coercive methods to make sure that the law is respected, over and above the exercise of due diligence by the stakeholders, create a context of free will and trust needed for the widespread use of the information society for the benefit of the greatest number of people.

A range of existing recommendations is to be explored to compensate for identified weaknesses, extending beyond simple advice and proposing to include in the CGTI action programme the preparation of a specification for the dynamic evaluation and control of technological changes in France in this field.

The report on digital identity scheduled in the 2004 programme could state the reasons for this specification. It will present the problem areas surrounding identification from three angles, namely the creation, processing and use of personal data; the traceability of

objects throughout the product's service life; and lastly, services. It will address the lawful applications and those that may be performed in a voluntarily obscure fashion, whether or not they fall within what is lawful.

RECOMMENDATIONS

1. Carry out an in-depth analysis of the threats from RFID technologies, whether they are targeting individuals, companies or national sovereignty, particularly with respect to their ease of use.
2. Make RFID supply and demand stakeholders aware of the opportunities and threats from this technology.
3. Set up an appropriate educational programme (symposiums, forums, articles, etc.), to create confidence amongst the general public and provide public authorities with a weapon to maintain national sovereignty.
4. Adapt the range of RFID services on offer to reflect feedback.
5. Encourage professional initiatives, by both manufacturers and end-users, to develop RFID applications likely to generate trust understood clearly by consumers and citizens.
6. Assess the applicability of the law providing for the protection of personal data from the viewpoint of radio frequency digital identification technology.
7. Encourage France to participate in standardisation bodies and international forums on RFID technology, alternative naming and routing.
8. Invest in research on the economic and social effects of the RFID technologies and information systems that underlie applications with a societal focus.

Inspection Committee

RADIO-FREQUENCY IDENTIFICATION (RFID) TECHNOLOGIES: INDUSTRIAL ISSUES AND SOCIETAL QUESTIONS

Report presented by

**Françoise ROURE, General Inspector
Jean-Claude GORICHON, General Inspector
Emmanuel SARTORIUS, General Engineer**

A P P E N D I C E S

**Report No. II-B.9 - 2004
January 2005**

SUMMARY of APPENDICES

Appendix 1 : Abbreviations and acronyms

Appendix 2 : Bibliography

Appendix 3 : Internet sites

Appendix 4 : Attached documents

APPENDIX 1

Abbreviations and acronyms

CISC	: Complex Instruction Set Computer
CNIL	: <i>Commission Nationale de l'Informatique et des Libertés</i> (French Data Protection Authority)
DNS	: Domain Name System
DoC	: Department of Commerce
DoD	: Department of Defense
DOI	: Digital Object Identifier
EAN	: European Article Number
ENISA	: European Network and Information Security Agency
GAC	: Government Advisory Committee
GAO	: General Accounting Office
GIP	: <i>Groupement d'Intérêt Public</i> (public interest group)
GPRS	: General Packet Radio Service
GSM	: Global System for Mobile Communications
IETF	: Internet Engineering Task Force
IP	: Internet Protocol
JHA	: Justice and Home Affairs Council
ONS	: Object Naming Service
RFID	: Radio Frequency Identification
RISC	: Reduced Instruction Set Computer
UID	: Universal Identity
WGIG	: Wireless Global Information Grid

APPENDIX 2

Bibliography

Legal provisions mentioned in the report:

French law

Act no. 2004-801 of 6 August 2004 on the protection of individuals with regard to the processing of personal data, amending Act no. 78-17 of 6 January 1978 on data processing, files and liberties.

Penal Code, Articles 226-16 to 226-24, Section V, "Violations of personal rights resulting from data files or processing".

Act no. 2004-810 of 13 August 2004 on health insurance, "personal medical file" Article 3 and "use of health data" Article 64.

European Union law

Regulation (EC) no. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJEC of 12 January 2001).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJEC of 23 November 1995).

Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJEC of 31 July 2002).

Commission Decision no. 2002/16/EC of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC.

Decision no. 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data Protection Supervisor's duties (OJEC of 12 July 2002).

Decision no. 2004/55/EC of the European Parliament and of the Council of 22 December 2003 appointing the independent supervisory body provided for in Article 286 of the European Community Treaty (European Data Protection Supervisor) (OJEC of 17 January 2004).

Council Resolution (2003/C 48/01) of 18 February 2003 on a European approach towards a culture of network and information security (OJEC C 048, 28 February 2003).

Parliamentary legislative resolution of 2 December 2004 on the proposal for a Council regulation on security features and biometrics in EU citizens' passports (P6_TA-PROV (2004) 0073 A6-0028/2004).

Proposal for a Council decision establishing the Visa Information System (VIS) (COM (2004) 99 final).

The Charter of Fundamental Rights of the European Union, Article 8 (future II-8 of the Draft Constitution), adopted by the European Summit in Nice, June 2002.

Article 29 - Data protection Working Party, "Working document on biometrics", 1268/02/EN WP 80, 01/08/2003, 11 p.

International law

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, known as Convention 108 of the Council of Europe, adopted in 1981 and ratified by 31 member States of the Council of Europe, specifically Article 8

Reports

La RFID dans la distribution : une technologie prometteuse mais limitée à la sphère logistique ? Synthèse Amérique du Nord, Asie, Europe occidentale (RFID in distribution: a promising technology but limited to the logistics sphere? North America, Asia and Western Europe synthesis report). Ministry of the Economy, Finance and Industry, DREE 5 C, April 2004, 21 p.

L'Hyper République. Bâtir l'administration en réseau autour du citoyen (The Hyper Republic. Building a networked administration around the citizen). Report submitted to Henri Plagnol, Minister of State for State reform, by Pierre de La Coste. Rapporteur Vincent Bénard. 8 January 2003.

Technical specifications

Department of Defense standard practice. Military marking for shipment and storage (Point 4.9 RFID), 29 October 2004.

Articles

Anne Debet, commission member of CNIL, *L'Europe de la sécurité* (The Europe of safety), 23 July 2004, Tribune in <http://www.cnil.fr>.

Brett Glass: "Microsoft's Palladium: security for whom?", 24 June 2004, in http://www.extremetech.com/print_article/0,3998,a=28481,00.asp.

Etienne Wery: *La France transpose enfin la directive vie privée de 1995 ! La loi du 6 août 2004 est publiée au JO* (France finally transposes the 1995 privacy directive! The Act of 6 August 2004 is published in the official journal), 11 August 2004, in http://www.droit-technologie.org/1_2.asp?actu_id=971.

APPENDIX 3

Internet sites

<http://www.dodrfid.org>

<http://www.EPCglobalUS.org>

<http://www.verisign.com>

<http://www.edps.eu.int> Site of the European Data Protection Supervisor.

http://europa.eu.int/comm/internal_market/privacy/links1_fr.htm European Commission site with useful links on the personal data protection policy.

<http://privacy2.msn.com> Microsoft site on the framework and undertakings to respect digital personal data collected by MSN sites and services (for example, MSN Hotmail, MSN Money and MSN Health).

<http://www.ietf.org/internet-drafts/draft-ietf-marid-core-03.txt> IETF site on the working document on authorising the use of domains in MAIL FROM. 2004, 10 p.

<http://english.peopledaily.com.cn>. Science-Education heading, 29 September 2002 in particular.

APPENDIX 4

Attached documents

- 4.1 **UID registry concept: DoD graphic representation and provisional timetable**
- 4.2 **Military marking for shipment and storage. MIL-STD6129P w/Change 3, DoD, October 29, 2004**
- 4.3 **Radio Frequency Identification (RFID) Policy, The Under Secretary of Defense, DoD, July 30, 2004**
- 4.4 **“VeriSign to run EPC Directory”, RFID Journal, January 13, 2004**
- 4.5 ***Demain, une autre gouvernance de l'INTERNET* (Tomorrow, another governance for the Internet), .ppt presentation, J-C. Gorichon, January 4, 2005**
- 4.6 **IEEE position statement against the use of universal identifiers (UIDs)**
- 4.7 **VeriSign: the EPC Network: Enhancing the Supply Chain (White Paper) 2004**

APPENDIX 4.1

UID *registry concept*: DoD graphic representation and provisional timetable

A P P E N D I X 4 . 2

Military marking for shipment and storage.
MIL-STD6129P w/Change 3, DoD
October 29, 2004

A P P E N D I X 4.3

***Radio Frequency Identification (RFID) Policy,
The Under Secretary of Defense, DoD
July 30, 2004***

APPENDIX 4.4

***“VeriSign to run EPC Directory”, RFID Journal
January 13, 2004***

A P P E N D I X 4.5

***Demain, une autre gouvernance de l'INTERNET,
.ppt presentation, J-C. Gorichon,
January 4, 2005***

A P P E N D I X 4.6

IEEE position statement against the use of universal identifiers (UIDs)

A P P E N D I X 4.7

VeriSign: the EPC Network: Enhancing the Supply Chain (White Paper) 2004