Influence of the “Internet of Things” on Legislation Regarding the Protection of Individual Privacy

Jean-François Henrotte

Partner in the elegis law firm and Director of the “Revue du Droit des Technologies de l’Information”
www.elegis.eu – www.rdti.be
jf.henrotte@elegis.be

Abstract
The “Internet of Things”, considering its characteristics, calls for developing third-generation data protection with a new field of application and greater use of the technology itself for resolving the problems it poses.

Introduction
Network technology as we know it, with the Internet centre-stage, is on the dawn of another quantum leap. Progress on miniaturization and wireless communications presage the imminent interconnection of the things surrounding us, to form a vast network: “the Internet of Things”\(^1\).

In this scenario, seriously envisaged by several governments worldwide\(^2\), things used in daily life will communicate with each other or to other entities (people or machines) information they have collected on their environment, using their various sensors.

Although this permanent interconnection, this “ambient intelligence”\(^3\), is expected to “contribute to addressing today’s societal challenges”\(^4\), more and more authors are also pointing out that it calls into question our concept of private life and its protection.

The right to protect private life has evolved gradually over the years, mirroring technological progress\(^5\). First-generation laws on the protection of individual privacy were founded on Article 8 of the European Convention for the Protection of Human Rights\(^6\). This first-generation basically grants a “right to be left alone”\(^7\). Protection is understood as a prohibition on processing certain sensitive

\(^3\) Greenfield, A., "Everyware: the dawning age of ubiquitous computing", New York, New riders publishing,
\(^4\) See the Communication from the Commission to the European Parliament, the Council, the European Social and Economic Committee and the Committee of the Regions "The Internet of Things - an action plan for Europe" COM(2009) 278 Final, 2.
\(^6\) The European Convention for the Protection of Human Rights of 4 November 1950, conventions.coe.int/Treaty/EN/Treaties/Html/005.htm
\(^7\) The famous "Right to be left alone" defended by Warren, S., and Brandeis, L., in their article: "The right to privacy", 4, Harvard Law Rev., 193 (1890), groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.
data and protecting various spheres, both physical and communications-related.

In recent years, technological progress led to second-generation laws on the protection of individual privacy (Convention no. 108 of the Council of Europe\(^8\), Directive 95/46\(^9\) or Article 8 of the European Charter of Human Rights\(^10\)) which while remaining concerned with data and its nature, focus on data processing. The processing of personal data gives rise to a disparity of information between the party processing the data and the person to whom that data relates. The disparity results in an imbalance of power to the detriment of the person whose data is being processed. The emphasis is now on rules governing data processing and the need for transparency, in order to restore the balance and guarantee an informational right of self-determination for all\(^{11}\).

---

**Calling key concepts into question**

**Life-changing technology…**

The “Internet of Things” is based on technology with acronyms like RFID (for Radio Frequency Identification) chips, geo-location via GPS (for Global Positioning System) or NFC (Near Field Communication) etc.

This “ambient intelligence” technology creates a new type of data or even a new generation of data. The data is linked to possession of an object belonging to a person.

---


---

The data no longer directly concerns the actual person - but an object belonging to them.\(^{12}\) This allows monitoring indirectly but with certainty, the behavior of the object’s owner and even predicting future behavior through an analysis of the latter’s habits. The example of the RFID chip speaks volumes in this regard. The route taken by anyone carrying a card fitted with this type of chip can be tracked easily. All they need to do is walk in front of terminals fitted with the same technology. The technology records habits without any visible physical contact between the reader and the tag; the card-holder may remain blissfully unaware of this happening. Notably, this allows creating made-to-measure advertising and knowing where and when to display it. In fact, imagine the owner of an RFID card bought a large number of books of the same genre at a bookshop. On walking past an RFID terminal at a bookshop in the same chain the card-holder is struck by an advertising message recommending them to purchase a particular book in the same genre! Better still, a discount voucher could be displayed for an item not usually purchased by the card holder, in order to optimize the marketing budgets: why grant a reduction for an item the card-holder will to all intents and purposes, purchase? The technology can thus anticipate and create expectations in the consumer….

---

\(^12\) In fact, in the Internet of Things, the data collected are not personal except by a consequential effect. The data refers to an object, itself linked to the person possessing it.

---

\(^13\) Article 2, a) of Directive 95/46.
The European Commission’s action plan as a premise of additional protection for individual privacy

The European Commission considers that RFID technology and the “Internet of Things” are factors promoting growth and employment, capable of improving the quality of life and improving efficiency. Notably in the fight against counterfeiting, the management of electronic waste and hazardous substances.

Yet the Commission has not closed its eyes to the collateral damage the arrival of this technology could cause. Its ambition is thus to control the emergence of the phenomenon so the ethical aspects are taken into consideration, ensuring the Internet of Things is an “Internet of Things for Individuals”.

In a communication dated 15 March 2007 the Commission stated further details and information would be provided on the issues of data protection and individual privacy raised by RFID applications. This was accomplished by the recommendation of 12 May 2009 on implementing the principles of respect for individual privacy and data protection in radiofrequency-based identification applications.

On 18 June 2009 the Commission also adopted a communication entitled “The Internet of Things – an action plan for Europe”, which seeks to address all the consequences of the emergence of the Internet of Things. In 2010 the Commission intends to publish a broader Communication on privacy and trust in the ubiquitous information society.

Recommendation 2009/387/EC is of interest insofar as it is one of the first European documents which, without

---


being mandatory, is clearly moving towards a third
generation of data protection for the retail trade.
Retailers must conduct an assessment of the implications
of the application implementation for the protection of
personal data and privacy, including whether the
application could be used to monitor an individual 24.
Whether or not there is a likely threat to privacy or to
the protection of personal data, operators should inform
individuals of the presence of tags that are placed on or
embedded in products using a common European sign,
developed by European standardisation organisations, with
the support of concerned stakeholders 25.

The Commission then details implementing consumers’
right to the “silence of the chips” 26.
If the privacy and data protection impact assessment
concludes that tags that are used in a retail application and
would remain operational after the point of sale represent a
likely threat to privacy or the protection of personal data,
retailers are obliged to deactivate or remove the tags at the
point of sale, immediately and free of charge for the
consumer, unless consumers, after being informed of the
policy, give their consent to keep tags operational. The
deactivating of tags shall not require the active
involvement of the consumer 27.
Even if the privacy and data protection impact
assessment concludes that tags that would remain
operational after the point of sale do not represent a likely
threat to privacy or the protection of personal data, retailers
should make available free of charge an easy means to,
immediately or at a later stage, deactivate or remove these
tags 28.
Deactivation or removal of tags should not entail any
reduction or termination of the legal obligations of the
retailer or manufacturer towards the consumer. This
represents substantial progress, since unlike Directive
2002/58 29 and its Article 5.3, the recommendation provides
that consumers mindful of the need to protect their privacy,
should not be penalized.

Conclusions

Most players and authors concur in acknowledging that the
Internet of Things poses a threat to individual privacy and
the right to informational self-determination and that the
present protection measures cannot remedy the situation
given, inter alia, their restricted scope of application.
The technology itself may afford a partial solution to the
difficulties and threats it poses (for example, through the
option of deactivating the chips) but it must be controlled
(if the faculty exists, it must be clearly notified and not
seek refuge behind non-use of the faculty).
For the moment, no doubt in response to constant
complaints about over-regulation, the European
Commission is not legislating, but restricting itself to
issuing recommendations to Member States and
companies. Why not? The Commission will reassess the
recommendation’s impact in three years’ time. Whether
by self-regulation or legislation, the new practices created
by this increasingly omnipresent technology must be
controlled. The third generation of data protection (no
longer exclusively for personal data) will not replace
earlier ones but supplement them and adapt the law to
changing technological practices 30.

Acknowledgments

The author is especially grateful to Fanny Cotton, Jessica
Dallapiccola and Alexandre Cassart for their collaboration
for this paper.

24 Para. 5 of the recommendation.
25 Para. 9 of the recommendation. Para. 7 of the
recommendation, more ambiguous, since it provides this
obligation “without prejudice to the obligations of data
controllers, in accordance with Directives 95/46/EC and
2002/58/EC”, presages the policy of a concise, accurate
and easy to understand information policy to operators
indicating the data that may be processed using the
application, “in particular if personal data will be
processed” and whether the location of the tags will be
monitored, indicating that the information policy would
apply even if there is no processing of data of a personal
nature.
26 Expression borrowed from the communication "The
27 Para. 11 of the recommendation.
28 Only retailers processing data are covered by this
provisions pursuant to para. 14 of the recommendation.
Under the terms of para. 3.c) “‘operator’ means the natural
or legal person, public authority, agency, or any other
body, which, alone or jointly with others, determines the
purposes and means of operating an application, including
controllers of personal data using an RFID application”.
29 Para. 12 of the recommendation.
30 Directive 2002/58 of 12 July 2002 concerning the
processing of personal data and the protection of privacy in
the electronic communications sector, OJEC L201, 31 July
31 Poullet, Y., "La protection des données: un nouveau
droit constitutionnel. Pour une troisième génération de
réglementations de protection des données", 356.