Autoriteit
Consument & Markt

BUILDING THE EUROPEAN DATA ECONOMY - Input consultation

To	'CNECT-CONSULTATION-DATA-ECONOMY@ec.europa.eu'
Cc.	-
From	Anne-Jel Hoelen | Anne-Jel.Hoelen@ACM.nl (also with input of Desmond de Haan, Noortje Polman, Bart Stuut)
Date	27 April 2017
Subject	BUILDING THE EUROPEAN DATA ECONOMY - Input consultation
Annex(es)	-

Muzenstraat 41 | 2511 WB Den Haag
Postbus 16326 | 2500 BH Den Haag
T 070 722 20 00 | F 070 722 23 55
info@acm.nl | www.acm.nl | www.consuwijzer.nl

1 BUILDING THE EUROPEAN DATA ECONOMY - Input consultation – input by the Consumer Department of the Netherlands Authority for Consumers and Markets

General comments

This input complements the online consultation form as uploaded April 27th 2017 by me (Anne-Jel Hoelen, Senior Enforcement Official, Consumer Department, Authority for Consumers and Markets), anne-jel.hoelen@acm.nl).

One of the tasks of the Netherlands Authority for Consumers and Markets (ACM) enforces consumer law and protects the interests of consumers. This document represents the opinion of the Consumer Department of the ACM. The ACM is a competition and market authority as well. This document does not represent the opinion of the Competition Department and Sector Specific Market Departments.

In this consultation we also provide input to the questions that address consumers because ACM enforces consumer law and, among other things, enforces the Unfair Directive (93/13/EEC), the Electronic Commerce Directive (Directive 2000/31/EC), the Unfair Commercial Practices Directive (2005/29/EC) and the Consumer Rights Directive (2011/83/EU). ACM also enforces a number of provisions of the e-Privacy Directive (2002/58/EC). We note that there is no supervisor in the Netherlands that specifically supervises compliance with product liability rules within the meaning of compliance with the Product Liability Directive (85/374/EEC).

Sensor data & machines generated data: who is the data producer?

Several times the working paper and the consultation ‘Building the European Data Economy’ pay

attention to a possible definition of 'data producer; followed by granting this data producer the right of ownership of the data and / or the right to licence this data. In the working paper lists examples of sensors in cars that track data and send this data to the producer / manufacturer of the car for purposes of maintenance, analyses of well-functioning and the adjustment of production processes and / or the improvement of the functioning on distance.

Almost all of this is mentioned in a B2B relation. Consumer devices seem to be excluded. If consumer devices are excluded, we presume this is based on the assumption that the data generated in consumer devices are covered by the General Data Protection regulation (EU) 2016/679). For us, this leads to the following important questions: does all data that in some way is related to an identifiable individual personal data? For example are all data provided by a consumer for the purpose of obtaining digital content personal data? Does this also apply to a picture that the consumer uploads to the cloud through a cloud service account? These are similar questions as we have related certain aspects of the proposal Directive on certain aspects on the delivery of digital content[1]. Another example outside the proposal for this digital content directive is o contributing to open source software that is linked to an account of a web service specifically for writing software personal data? The question is whether this is the case. Below is explained how a consumer might be considered a data producer as well.

If it is possible that data generated by consumer equipment is *no* personal data, then the following applies in both B2B and B2C relationships. The consumer can also be data producer.
The production of data by sensors in devices is done by two parties:

- The producer of the hardware that has embedded the sensor
- The owner / user (these can be combined the same person but this is not always the case)

The sensor technique can be subject of intellectual property rights but this will not automatically result in full and exclusive ownership of the data the producer of the hardware.

The produce (which is often also the owner) of the device produces data by using the device. For the production of this data he will have costs. Costs for electricity, costs for communication and costs for the use of an electronic communication network. In most cases, these costs will not be high and in most cases these costs will be difficult to connect with these other side functions of the device. But for the answer to the question who the producer of the data is, it is not important how high these costs are in relation to the costs that are made by the producer of the device (e.g. the investments in the development of the data generating part of the device). The costs for development can be high once but these can be much lower in the end when compared to the costs the consumer / user has made over years of continuous use. The reverse situation is also possible.

The production of this sensor data can only take place through the efforts of both parties: the

[1] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on certain aspects concerning contracts for the supply of digital content (COM(2015) 634 final), see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2015:0634:FIN.

manufacturer and the user / owner. Thus, as the working paper seems to want to define, not just one data producer. The owner / user must at least be granted the right to see, use, and (possibly) let third parties process this data.

Input to: 2. Access to and re-use of non-personal data

The ACM enforces consumer law and, among other things, enforces the Unfair Directive (93/13/EEC), the Electronic Commerce Directive (Directive 2000/31/EC), the Unfair Commercial Practices Directive (2005/29/EC) and the Consumer Rights Directive (2011/83 / EU). The current rules that follow from these directives relate only to B2C situations. It might be clear that these rules do not solve the problems that exist regarding access to data in B2B situations. In the Netherlands the possibility to apply these rules also apply in B2B situations is not used.

Input to: 2.1. Accessing data

The ACM also has data sets but the ACM does not license these data sets to others. The ACM fears that others will misinterpret that data and because there are legal restrictions on licensing and because this is a strategic decision of the organization .

Input to: 2.3.1. General objectives for a future EU framework for data access

2.3.2. Access for public sector bodies and scientific research

To what extent do you agree with the following statements (1=not at all,2=to a minor extent, 3=neutral/I don't know, 4=to some extent, 5=to a great extent):

	1	2	3	4	5
Trading of non-personal machine-generated data should be enabled to a greater extent than it is today.	☐	☐	☐	☐	☉
The sharing of non-personal machine-generated data should be facilitated and incentivised.	☐	☐	☐	☐	☉
Investments made into data collection capabilities and data assets should be protected.	☐	☉	☐	☐	☐
Sensitive business and confidential data should always be safeguarded.	☐	☐	☉	☐	☐
Lock-in effects in the data market should be minimised, especially for SMEs and start-ups.	☐	☐	☐	☐	☉

Input to: 2.3.3. Access for other commercial entities

We basically agree with the following statement: More data would become available for re-use if the Commission would issue guidance on how access, use and re-use of data should be addressed in contracts (data usage licenses) – based on existing legislation (in particular the Trade Secrets Protection Directive (2016/943/EU), copyright legislation and the Database Directive (96/9/EC)).
But we believe this is only can be really effective if also the big data if collectors and producers would follow this guidance. Guidance leaves the these parties a lot of freedom. Therefore, we also think that guidance will have not have a huge impact, including economic on competition and innovation.

Opmerking [JF1]: Economische wat precies?

Autoriteit
Consument & Markt

Companies are generally cautious to share data because of (real or hypothetical) legal restrictions. If Guidance can take away these insecurities than guidance could lead to some increase in innovation.

We do not agree with the following statement: The optimal solution for making data collected by sensors embedded in machines, tools and/or devices available for re-use is to leave it entirely to the parties to decide (by contract) who should have the right to license the usage of these data, how and to whom.
The use of prescribed licenses or restrictions in use could also have a negative impact on innovation. This is as it is now, and this does not seem to work well.

We fully agree with the statement: More data would become available for re-use if more data holders used Application Programming Interfaces (APIs) to facilitate access to the data they hold, and these APIs were designed and documented in a way easy to use by third party application developers.
The best way to do this is to introduce an API label system.
The labelling of the API's would make the API more transparent while protecting Intellectual Property at the same time.
We believe the use of API's by data holders to facilitate access to the data they hold is very important but we stress that this will only is a good option if the condition is met that there is a total access to the data and that this access is permanent. if third parties have limited access this will not be sufficient. It could be considered to give any party that processes data above a certain threshold or meets certain criteria to open third parties through an API under fixed terms that are (co) determined by EU-legislation. This could also apply to consumer data / personal data, which would allow consumers to easily indicate whether and, if so, with who their data may be shared.

We agree with the following statement: More data would become available for re-use if legislation would define a set of (cross-sector or sector-specific) non-mandatory contract rules for B2B contracts, possibly coupled with an unfairness control in B2B contractual relationships) for allocating rights to access, use and re-use data collected by sensors embedded in machines, tools and/or devices were defined.
We believe that parties will not include these non-binding rules in the agreements.

We agree with the following statement in some cases: More data would become available for re-use if a set of recommended standard contract terms were to be drafted in close collaboration with stakeholders.

We possibly agree with the following statement: Would you agree with the following statement: More data would become available for re-use if a company holding data which it protects through technical means against illicit misappropriation had civil law remedies against such misappropriation (e.g. the right to seek injunctions, market exclusion, or to claim damages).
However, this option is also susceptible to abuse and may therefore be counterproductive.

We basically agree with the following statement: Would you agree with the following statement: More

data collected by sensors embedded in machines, tools and/or devices would become available for re-use if both the owner or user of the machine, tool or device and the manufacturer share the right to license the use of such data.
Then there would be fewer legal restrictions. However, it is very situation-dependent. There will always be a party for whom it is not beneficial to license the data. Would it not be better if it legislation stipulates who owns the data? If it would make clear that you the owner when you generate the data, or when you deliver the machine? The first option seems logical, but in practice it is also often the supplier of the machine.

We do not know if we agree with the following statement: More data would become available for re-use if the companies active in the production and market commercialisation of sensor-equipped machines, tools or devices were awarded an exclusive right to license the use of the data collected by the sensors embedded in such machines, tools and/or devices (a sort of sui generis intellectual property right).
It is very situation-dependent. There will always be a party for whom it is not beneficial to license the data. Would it not be better if it legislation stipulates who owns the data? If it would make clear that you the owner when you generate the data, or when you deliver the machine? The first option seems logical, but in practice it is also often the supplier of the machine. This only seems generate more restrictions.

We do not agree with the following statement: More data would become available for re-use if the persons or entities that operate sensor-equipped machines, tools or devices at their own economic risk ("data producer") were awarded an exclusive right to license the use of the data collected by these machines, tools or devices (a sort of sui generis intellectual property right), as a result of the data producer's operation, to any party it wishes (subject to legitimate data usage exceptions for e.g. manufacturers of the machines, tools or devices
The phrase "To any party" in the General Data Protection Regulation (EU) 2016/679) is not sufficiently clear. It is already better than in the situation where only the supplier has this right. With this option it is important to note which limitations there are. If everyone manages their own data, this data will be far less useful than when you merge all datal. The more data you put together, the more value of the data will have because this provides you more options to use the data and the results are more reliable.

To what extent would you agree to an obligation to license for the re-use of data generated by machines, tools or devices that you have commercialised under fair, reasonable and non-discriminatory (FRAND) terms?

- ◉ To a large extent
- ○ To some extent
- ○ To a minor extent
- ○ Not at all

To what extent would you agree to an obligation to license for the re-use of data generated in the context of your online platform through its users under fair, reasonable and non-discriminatory (FRAND) terms?

Autoriteit
Consument & Markt

- To a large extent
- To some extent
- To a minor extent
- Not at all

Input to: 3.1. Extra-contractual liabilities: IoT and robotics products and services

The examples pf IoT that cause direct and indirect damage to both consumers and organizations are easy to find. IoT devices - like every other device connected to a network - can be used for criminal activities. One example is malware like Mirai[2] (which resulted in a botnet) and BrickerBot[3]. Bots can be used as part of a botnet in large scale network attacks. The main reason for the success of these malware types is the lack of security and update regimes for IoT devices. Some malware focuses primarily on Internet consumer-related consumer devices and routers at home. Again, the inadequate updating regime is a weak spot. Users do not feel the need to update their equipment as long as this works according to the users expectations of the primary functions that match the reasons why they acquired this product in the first place. It is very likely that users of IoT devices are not aware of these risks (that even might be already realized) and it is almost certain that they do not want to facilitate different types of cybercrime. Similarly, users of IoT devices can become victims of ransomware[4]

Other examples that damage privacy and / or which could lead to direct financial damage include the Cayla doll[5] and doll houses that respond to Alexa / Amazon voice commands[6].

Material damage may occur if IoT devices are connected to the user's physical environment. For example, there are security cameras (Closed-Circuit Television) that are potentially damaging if an attacker gains access to the camera. Another example is an open network connected medical equipment.

Another problem is the IoT equipment coming from countries other than the EEA. As a rule, other rules apply, which may make it difficult for the user to obtain his right under European law.

---

[2] The malware made devices with a outdated Linux version that were connected tot he network act as bots that were controlable from a distance. Also see the Wikipdiapage on Mirai malware: https://en.wikipedia.org/wiki/Mirai_(malware)

[3] Iain Thomson, 'Forget Mirai – Brickerbot malware will kill your crap IoT devices', *The register* d.d. 8 Apr 2017, https://www.theregister.co.uk/2017/04/08/brickerbot_malware_kills_iot_devices/

[4] Lucian Constantin, 'Ransomware on smart TVs is here and removing it can be a pain', PCWorld d.d. 3 Jan 2017, http://www.pcworld.com/article/3154226/security/ransomware-on-smart-tvs-is-here-and-removing-it-can-be-a-pain.html.

[5] Stefanie Fogel, 'Germany bans creepy doll over privacy concerns', Engadget d.d. 17 feb 2017, see: https://www.engadget.com/2017/02/17/germany-bans-my-friend-cayla-doll/ . Also see Toyfail: the awareness clip from the Norwegian Consumer Council of December 5th 2016 called #toyfail: https://www.youtube.com/watch?v=IBrDmIgHb-0.

[6] https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse

All of the above put leads together to the conclusion that the abuse of IoT equipment can thus lead to reduced confidence in technical developments, loss of privacy / data protection and intangible and financial damage.

When IoT devices are used it is not clear who exactly is or are responsible and who is or are liable. IoT can consist of hardware and software components and services that can come from different manufacturers and suppliers. When using open source software, this becomes even more complex. Often software components are not updated and often the lifespan of hardware is longer (or parts thereof). Software is not subject to tear and wear but should be updated for safe use. You could say that if that does not happen, the life of the hardware is longer than that of the software.
For users, it is often unclear that the software of their product is outdated. Often the device will function according to the primary functions that made the use purchase the product. That there may be security issues and security vulnerabilities, the user often cannot see. Also the user often does not know who address with a request for an update. That there are different manufacturers and suppliers that are involved with the functioning of the device and that their obligations might be fragmented is generally unclear to the user. If damage is caused by the outdated software of the device, it is often unclear to the user who he can appeal to.

Input to 3.1. Extra-contractual liabilities: IoT and robotics products and services

In the Netherlands, the Netherlands Food and Consumer Product Safety Authority (NVWA) enforces product safety. There is no supervisor in the Netherlands that specifically monitors compliance with product liability rules as in the Product Liability Directive (85/374/EEC). ACM monitors compliance with consumer law, including compliance with the Unfair Terms Directive (93/13/EEC), the Electronic Commerce Directive (Directive 2000/31/EC), the Unfair Commercial Practices Directive (20065/29/EC) and the Consumer Rights Directive (2011/83/EU).

At the moment, ACM receives little to no signals (consisting of questions and complaints) of consumers about damage caused by a defective IoT or robotics device. Most IoT / robotics devices are not on the market for a long time yet. However, we see clear risks related to these devices.

We believe that all types of damage that are mentioned by DG Connect in the consultation (p. 37) are very realistic: physical damage as well as damage to property, as well as pure economic and other economic losses.
The question which the most difficult aspect of the process of claiming damages in the situation of damage caused by defects or malfunctioning of IoT / Robotics is, is not very relevant. If one of the steps in the process is not successful, the outcome is still the same: the consumer will not receive compensation. But if we have to choose between ‘Identifying and/or proving the defect of the IoT/robotics device (e.g. Discovering where exactly the defect occurred)’, ‘Proving the damage, Proving the casual relationship between damage and defect‘ and ‘Classifying your IoT/robotics device into a clear category (that of a service/product)’ we think it's first: Identify and / or prove the

defect to the device.

Often a problem with a claim for damages will primarily be related to the amount of damage. The consumer will then make a decision: is this damage in balance with the (usually high) costs of a damages procedure? Furthermore, the fact that an agreement often states that liability is excluded gives the consumer the impression that he has no right to claim damages. He will very likely be reluctant to start a claim for damages. For a certain type of damage, many consumers do not even know at all that they can claim for damages. If there is a vulnerability in an interactive talking IoT pop of your child who can talk to another child or your child, what is the exact harm? What would be a realistic amount in a damage claim?

Consumers will often be unaware of the potential security risks involved in IoT and robotics.

Consumers must ensure that the software of their device is up to date. But consumers do not always update the device

- because they are not aware of the risks of they don't and / or;
- because of mixed updates (a mix of security updates, functionality updates, etc., which are not always suitable for all current models) and these updates not always are fit for all the current hardware devices. The update then might results in a device that functions less or even becomes completely unusable. At the moment, consumers often have two choices in the update regime: Whether he allows the device to update itself, or does it automatically do so by the manufacturer. At the latter, therefore, there is a risk that the device will function less well.

We think that many consumers have no reluctance at all to buy IoT/robotics products or services. We think that many consumers are not aware that they buy an IoT / Robotics device and what are the associated risks, e.g. privacy risks, software security problems or cyber security problems or that the device that he buys will function far less long then he expects because of a limited or non-existent update regime. Let alone that they realize which problems they can encounter when the device malfunctions and then try to get compensation in case of damage and they have to know who to address and what the exact cause of the damage is. The trader generally does not clearly and explicit inform the consumer about these risks in his commercial communication and / or on the packaging of the product. Because IoT / Robotics products are quite new, the consumer is not familiar with the risks by experience.

We wonder if all IoT/robotics products and devices should be equipped with an event data recorder. On the one hand, it would be useful if IoT / robotics products are equipped with an event data recorder to track what the device was doing when the damage occurred . On the other hand, privacy / data protection concerns should be taken in consideration. If the device is equipped with an event data recorder this data also should be accessible to the consumer. For example, Tesla cars have an event data recorder. There are some cases know that are mostly outside the EU that involve fatal accidents with Tesla cars. It was said that Tesla refused to give the relatives of the deceased or the

survivors of the accidents access to the data to determine the cause.[7] As a result it was not possible for the relatives to determine if the accident was caused by a defect in the car, which complicates the claim for compensation. This regardless of whether this data qualifies as personal data in the EU.

In the Netherlands, there are no specific rules for liability for damage caused by new technological developments such as IoT / Robotics.

Who should bear the liability in case of damages caused by defects or malfunctioning of a smart device which combines tangible goods (a car), digital goods (an app) and services (e.g data services)? This depends on the cause of the damage. It must be clear to the consumer who he can address his claim to. It should be avoided producers / manufacturers / service procedures concerned referring from one to the other. Risk liability could be a solution. This possible risk liability could rest on the provider of the digital good (software and/or app). This provider is often the party that has the most influences on the change in the functioning of the product. In principle, the hardware will not change except from wear. The problem to detect wear can also be solved with software.

There are several suppliers of IoT/services/robots which in their agreements, substantially or totally reduce the liability of the supplier of these IoT/services/robots. These include the end-user agreements (EULAs) of a smart TV, a modem and router and many services. In case of the total liability clauses the types of liability that are excluded (property damage, financial loss etc.) are irrelevant. All categories of damages are excluded.

We doubt whether the attribution of liability in the context of IoT / autonomous systems can be settled only through contracts. We have experience in Europe in applying the rules of the Unfair Contract Terms Directive (93/13/EEC), the E-commerce Directive (2000/31/EC), Unfair Commercial Practices Directive (2005/29/EC) and the Consumer Rights Directive (2011/83/EU) on e-services in B2C-relations. Some examples are the CPC[8] joint action on, among other things, the terms and conditions of social media[9] and the CPC project on the terms and conditions of the (online) travel industry. We also know that consumers almost never read terms and conditions.[10] Reading these terms and conditions is very time consuming because of the length of the terms are so long and because the terms are often written in a complex language and / or in another language. This applies in particular to liability clauses that are often also drawn up in a manner that fits a different legal system than is applicable in the country of the consumer.

---

[7] Sam Thielman, 'The customer is always wrong: Tesla lets out self-driving car data – when it suits', Monday 3 April 2017, The Guardian, see: 'https://www.theguardian.com/technology/2017/apr/03/the-customer-is-always-wrong-tesla-lets-out-self-driving-car-data-when-it-suits. '

[8] Consumer Protection Cooperation as in Regulation 2006/2004.

[9] EC, 'The European Commission and Member States consumer authorities ask social media companies to comply with EU consumer rules' (pressrelease), d.d. 17 March 2017, see: http://europa.eu/rapid/press-release_IP-17-631_en.htm.

[10] Why is well shown in the campaigns of our Norwegian colleagues: http://www.forbrukerradet.no/terms-and-conditions-word-by-word.

Autoriteit
Consument & Markt

Input to: 3.2. Possible options and a way forward (both for consumers/end users and producers of IoT/Robotics devices)

It would be a logical risk management approach to firstly hold the party liable that is best placed able to eliminate the risk. However, we would need more information in order to make a better judgment about this matter.

In our opinion, a non-contractual liability would be most preferable for the consumer. As has been indicated before, it is often not easy for consumers to claim their rights. Liability clauses are often complicated and it is possible that multiple liable parties shift responsibility to each other, which results in consumers being pushed from pillar to post. Consumers may decide not to try to claim their rights due to uncertainty. This is why, in our view, a non-contractual liability (i.e. liability as governed by EU-law) is the most consumer-friendly way for damage caused by the improper functioning of 'smart devices', which combine tangible goods with digital products and services. The question is whether an ad hoc solution for this problem must be sought within Europe. It may otherwise well be too late. After all, 'smart devices' are in use already.

In case of damages caused by defects or malfunctioning of a smart device which combines tangible products, digital products and services we think that maybe the software manufacturer should bear the liability if it is risk liability. The provider of the digital good (software and/or app) could bear this possible risk liability. This provider has often the most possibilities to change in the functioning of the product. In principle, the hardware will not change except from wear. The problem to detect this wear can also be solved with software.

Opmerking [JF2]: Dubbele alinea

Independently of who is considered liable, there should not be a limit to the level of any possible liability claim.

On the whole, we consider guidelines with 'best practices' and/or expected care and safety standards to be a good idea, provided that these are issued by the (services of) the European Commission and correspond properly with EU law, and if it also states clearly how the guidelines relate to this EU law. The liability matter can be quite complex and involve several parties, and the guidelines could offer a certain amount of clarification. The question is whether or not the guidelines are too open-ended

If the sector posits these themselves, the question is who is going to check the guidelines on content and compliance. Without oversight on this compliance, the matter is very much left open and traders could, for example, indicate that they follow the guidelines without any actual oversight. If it is entirely optional, it is very doubtful whether companies will make use of this. In addition, it is not the intention that the guidelines bypass the democratic regulatory process. More binding certification and/or the adoption of standards are also a possibility. In this case too, it is important there is oversight on the

compliance to these guidelines. An external third party such as the CE marking[11] may also provide oversight.

Is there a need for a cyber security insurance? Yes. The question is to what amount one should be insured if there is no boundary to a possible liability claim. The question also arises whether this insurance should cover all the different types of damage. Escrow would be a possible solution for the bankruptcy proceedings of the involved traders before the products' end of life.

It is unclear to us if the current regulatory framework offers sufficient protection for damage that is sustained by an algorithm, for example by a fault in the algorithm. The liability for this is often excluded from end-user agreements.

The responsibility for the faults or accidents that are caused by integrated open algorithms depends on who has made the choice to integrate. Is it the supplier? Then the supplier should be held accountable. Is it the user? Then the user should be held accountable.

Furthermore, we see a number of other options to cover, wholly or in part, the problems of the IoT apparatus:

- mandatory software updates for the anticipated end of life of the physical device, prominently indicating the relevant time period and the risks after this period.
- Promoting security and/or privacy by design. Possibly in combination with aforementioned certification to ensure that the promoted good also receives sufficient compliance.
- Transparency for a user can be achieved by granting easy and permanent access to a log showing who or what has access to its IoT device in a simple and comprehensible manner.

Building awareness for users with respect to the dangers and their rights.

Input to: 4.1. Portability of non-personal data

To its knowledge, ACM does not make use of services which provides data other than personal data, and that we port or recover this.

Data should be accessible in a common format. The definition of a common format will change over time.

Data portability only works in the case of interoperability first, if this is not the case, one can acquire data but cannot put it to use. The technical architecture for the interoperability should not be determined by the largest player.

[11] DG Growth, 'Manufacturers', (Last update: 04/05/2017), see: http://ec.europa.eu/growth/single-market/ce-marking/manufacturers.

Autoriteit
Consument & Markt

Input to: 4.2. Interoperability and standards

We consider it to be of great importance that interoperability is maximized. The greater the interoperability, the greater the consumer's freedom of choice will be. ACM aims to create opportunities and options for consumers and businesses.

Additional contribution

We consider it of great importance that any possible regulation in this field the relation with the sector-specific regulation will clearly be shown.
We would like to stress that the average consumer will make less rational choices than is assumed by a large part of European law or consumer law.

We would gladly explain the different subjects in a personal conversation. Please contact me via the contact information given below.

Autoriteit Consument en Markt
Anne-Jel Hoelen (Senior Medewerker Toezicht, Directie Consumenten ACM)
Muzenstraat 41
2511 WB Den Haag
T: +31 70 7222218
M: +31 6 31035836
Postbus 16326
2500 BH The Hague
The Netherlands
www.acm.nl
www.consuwijzer.nl