SVRV Sachverständigenrat für Verbraucherfragen

Consumer Rights 2.0

Consumers in the Digital World

Report of the Advisory Council for Consumer Affairs

Report of the Advisory Council for Consumer Affairs

December 2016

Berlin, December 2016

Published by the
Advisory Council for Consumer Affairs
at the Federal Ministry of Justice and Consumer Protection
Mohrenstraße 37
10117 Berlin

Tel: +49 (0) 30 18 580-0
Fax: +49 (0) 30 18 580-9525
E-Mail: info@svr-verbraucherfragen.de
Web: www.svr-verbraucherfragen.de

This publication is available on the internet.

Contents

Foreword

The digitalisation of an ever-increasing number of goods and services is causing an unprecedented and radical shift in consumer lifestyles and habits: The distinction between suppliers and demanders is becoming blurred, and consumers are more and more frequently taking on the role of supplier of those goods or services. Regulatory tasks which were previously the prerogative of the State can now be found as the default settings in algorithms applied by private-sector companies.

The Advisory Council for Consumer Affairs (*Sachverständigenrat für Verbraucherfragen*, SVRV) has set itself the task of investigating whether consumer law as it currently stands is able to meet the requirements of a digital world. For the Advisory Council, "consumer law 2.0" means that it is no longer possible to carry on with business as usual and that consumer law urgently needs an update.

This report builds upon external studies which the Advisory Council commissioned in 2016 and upon papers published in its Working Paper Series. It continues a series of reports which the Advisory Council has published on digitalisation in trade, finance, health and crowdfunding, and it prepares the ground for forthcoming reports on digital sovereignty and consumer scoring.

The Advisory Council would like to express its particular thanks to Prof Dr Hans-W. Micklitz, who had overall responsibility for this report, to Prof Gesche Joost and Ms Helga Zander-Hayat for their outstanding support, to Ass-Prof Dr Kai Purnhagen, Prof Dr Peter Rott, Prof Dr Gerald Spindler, Ass-Prof Dr Stefan Wahlen and Prof Dr Christiane Wendehorst, who made their expertise available in the context of the external studies, and to the Advisory Council Office, especially Dr Irina Domurath, for providing contextual and administrative assistance in the writing of the report.

Berlin, December 2016

Advisory Council for Consumer Affairs

Executive Summary

I. Potential solutions as regards the law of digital services

1. Re information provided before establishing a legal relationship

The Advisory Council for Consumer Affairs recommends: (1) Before a contract is concluded the entrepreneur must inform consumers on one page in each case (500 words) about the relevant data protection requirements and about the terms and conditions. This obligation also applies when changes are made during the contract term. The entrepreneur must use typographic means to clearly highlight any subsequent changes on the one-page information document. The one-page information document and any updates are to be transmitted to consumers on a durable medium within the meaning of section 126b of the German Civil Code. (2) Each change entitles the consumer to withdraw from the contract, to which reference must be made. (3) Sanctions must be imposed against breaches of the duty to include such a reference.

2. Re package offers (including services) when concluding a contract

The Advisory Council recommends introducing the following information requirements: (1) When consumers purchase an electronic device with pre-installed software, they must be (separately) informed about the price of the device and of the software. The case-law of the European Court of Justice, which requires the opposite, must be adjusted by way of an amendment to the EU Directive. (2) Where third parties are financing digital services this must be disclosed to consumers.

3. Re the scope and legal effects of consent

The Advisory Council recommends: Data protection requirements and requirements as regards terms and conditions for consent are to be put on an equal footing. The principle of separation and transparency under Article 7(2) of the General Data Protection Regulation is to be transferred to the inclusion of terms and conditions. Only those rights and obligations which have been set out in a one-page document (see Recommendation no. 1) are binding.

4. Re determining the contracting partner

The Advisory Council recommends: (1) In accordance with the proposal put forward by France, the platform operator must provide precise information about the service's function and the nature of the legal relationships; if the platform requires consumers to open a user account, this information is to be provided before the account is created. (2) In line with its actual function, the platform operator must take on a monitoring and control function; in the event of violating these obligations it will be liable vis-à-vis the consumer. (3) A rule should be introduced in the sharing economy based on which anyone providing chargeable services via a platform is to be treated like an entrepreneur within the meaning of section 14 of the German Civil Code until the opposite is proven.

5. Re the subject of the legal relationship

The Advisory Council recommends making it clear that "as is" digital services constitute a legal relationship which is linked to rights and obligations.

The Advisory Council recommends extending the rule on information documents which must be transmitted before a legal relationship is established to include "as is" services.

The Advisory Council recommends adding those clauses which are typically found in digital contexts and, in particular, in end-user agreements to the black and grey list of prohibited clauses.

The Advisory Council recommends stepping up research into the possible use of blockchain technology and the possible legal consequences of smart contracts.

The Advisory Council recommends systematically analysing the interplay between data protection law, copyright law and private/consumer law, because only a holistic perspective opens up the possibility of finding generalised rules which could provide insights and indicate the way forward for the digital world. From the consumer perspective, what is of the greatest importance in the short term is how the monitoring of terms and conditions can be brought into line with data protection and copyright law.

The Advisory Council recommends making it clear that privacy by design and privacy by default as well as basic IT security measures are part of the definition of the "use intended under the contract" within the meaning of section 434 (1) no. 1 of the German Civil Code.

6. Re the rights resulting from the legal relationship

The Advisory Council recommends making it clear that the right of data portability is also to be understood as a right of termination by means of which consumers can demand that their data be returned free of charge and deleted on a standard, machine-readable and interoperable medium.

The Advisory Council recommends, to counteract the discrepancy between the purchase contract and digital content provided by third parties, that product warranty liability be introduced against the producer or against the importer into the EU who is also liable against the consumer as regards third-party digital services.

7. Re improving individual redress

The Advisory Council suggests that business and consumer associations should be involved in drafting model contracts for digital services which not only safeguard key elements of the content of such contracts but also link in to arbitration mechanisms.

The Advisory Board suggests closely monitoring the effects of private, commercial mechanisms on redress backed by associations.

8. Re improving collective redress

The Advisory Council agrees with the thrust of this year's Consumer Law Conference at which calls were made to add governmental monitoring (digital agency) to legal redress through associations. Based on the example set by the UK, an additional "super complaint" would be a conceivable option, a procedure in which associations could force the authorities to act by calling on a court if need be.

9. Re the suitable means for implementing the proposals

The Advisory Council advocates implementing the proposals in a manner which maintains the cohesion between the proposed rules. In view of the political sensitivities which go along with any interference with the German Civil Code, amendments to the German Civil Code should be limited to what is absolutely essential. More specifically, a presumption rule for commercial activities would have to be incorporated into sections 13 and 14 of the German Civil Code and consent under data protection law brought into line with consent under the law of general terms and conditions.

10. Re the need for an evidence-based consumer policy

The Advisory Council recommends taking the necessary precautions in order to be able to shape an evidence-based consumer *law* policy.

11. Re the problem of competence

The Advisory Council is convinced that Germany is free to take the political lead and, possibly together with other Member States, to call on the European Commission to act.

II. Potential solutions as regards regulating algorithms

1. Requirements under the Federal Data Protection Act

The Advisory Council notes that the existing rule in section 28b of the Federal Data Protection Act represents a useful starting point when it comes to regulating self-learning algorithms.

2. Requirements under the General Data Protection Regulation

The Advisory Council notes that the rudimentary approaches to regulating algorithms set out in the General Data Protection Regulation are insufficient and fall below even the standard applied in section 28b of the Federal Data Protection Act.

3. Re the three possible options for a regulatory approach

The Advisory Council notes that there are theoretically three possible options for regulating this matter:

- *proactive* (legality by design): the legislature could oblige enterprises to incorporate binding legal requirements into algorithm development;
- *reactive*: the legislature could restrict itself to obliging enterprises to comply with the law when developing algorithms (which actually goes without saying) and then focus on ex-post monitoring;
- *the happy medium:* the legislature could set a regulatory framework which combines binding governmental requirements with self-regulation.

4. Re lack of transferability of technical regulation

The Advisory Council notes that it will not be possible to regulate algorithms using the means and technologies available for regulating industrial products.

1. Re the deficits and consequences of a reactive approach

The Advisory Council is convinced that sticking to “business as usual” is, politically speaking, not a serious option. The political realm is called to drop the option of ex-post controls, the de facto approach, and to look for a regulation which does justice to the specific features of algorithms.

2. Re the limited possibilities of co-regulation

The Advisory Council notes that the widely touted co-regulation in the form of government procedural framework-setting to regulate algorithms needs to be modified.

7. Re the need for an Algorithm Act

The Advisory Council recommends

(1) putting in place the legal requirements to ensure that algorithms take account of the requirements of consumer law, data protection law, anti-discrimination law and digital security. In the case of algorithms which enter into direct contact with consumers, the underlying parameters need to be made transparent. Legal responsibility also needs to be assignable in the case of self-learning algorithms and applicable consumer protection regulations need to be complied with;

(2) ensuring that, based on standardised disclosure requirements, algorithms are disclosed to a circle of experts in the digital agency who carry out spot checks to see whether they are legally sound. Standardised software engineering procedures need to be developed to that end;

(3) that enterprises should also be called on to draw up a code of conduct on the use of personal data, artificial intelligence systems and big data analysis.

8. Re the problem of competence

Subject to more in-depth investigation, the Advisory Council believes that competence for drawing up an Algorithm Act has remained with the Member States, despite the objective of full harmonisation set out in the General Data Protection Regulation.

III. Potential solutions as regards the need for a digital agency

1. Re the need for immediate political action

The Advisory Council recommends establishing a digital agency in which previous competencies linked to digital services are pooled and expanded.

2. Re institutional embedding of the digital agency

The Advisory Council is in favour of assigning the Federal Cartel Office those tasks which are being considered as part of the digital agency's remit. This will ensure that those legal issues which the digital economy raises and which go together are not pulled apart on extraneous grounds.

3. Re the tasks and competencies of the digital agency

The Advisory Council recommends assigning all the necessary tasks to the digital agency and guaranteeing it the necessary resources so that it is in a position to proactively investigate technical and legal issues raised in the digital economy, to draw up proposals, discuss these in the public domain, develop codes of conduct with business and consumers, and to develop recommendations and proposal for the legislature.

4. Re the problem of competence

The Advisory Council recommends commissioning a legal expert opinion which addresses the question of the merging of German authorities to the extent that these are also required to implement tasks for which EU law sets legally binding institutional and procedural requirements.

Part I Purpose, structure and thread of the report

I. Three objectives

This report has three objectives:

First, to trace and evaluate the debate around the need to regulate digital consumer services. The Advisory Council takes up the discussion on the role and function of digital platforms launched in December 2015/January 2016 and broadens it to address questions around the sharing economy and the Internet of Things: Of what value are the diverse regulations proposed by the Association of German Jurists (DJT), the European Commission and academics[1] participating in the debate? Can they achieve the worthy aim of safeguarding the autonomy of consumers in the digital age?

More specifically: Taking a holistic perspective, what action is urgently necessary to adapt applicable rules to the challenges the digital world poses – from when a legal relationship is entered into until it is terminated?

Second, to give an outlook on those pressing issues and emerging problems which go along with ongoing developments in the field of digital technologies, for instance software agent systems, regulation by algorithm and the possibilities inherent to big data. Given its remit, the Advisory Council believes that its task is to point out the kinds of questions which are raised and to come up with possible solutions so as to initiate a debate about political solutions. This on no account means that it is siding with what are known as exceptionalists,[2] but is based on the realisation that it is necessary to consider the possibility that social, economic and political disruption is occurring.

More specifically: Would statutory regulation of big data in the shape of a law of algorithms be a conceivable way of getting a grip on the risks to the autonomy and sovereignty of consumer citizens?

Third, to develop concrete proposals for improving the enforcement of rights in a digital society. More than ever before, any future regulation must never lose sight of the matter of feasibility. It is hard for consumers to recognise when they are being sent personalised advertising, and yet they are supposed to enforce their own rights. How is that possible? Collective redress is getting structurally more and more difficult. The focus here is on a proposal put forward jointly by the Federal Ministry for Economic Affairs and Energy and the Federal Ministry of Justice and Consumer Protection[3] regarding a digital agency which would, firstly, have to make expertise available and, secondly, improve the means of enforcing rights.

More specifically: What should a digital agency look like, what competencies should it have and what tasks should it take on in order to safeguard consumer rights?

II. Background and scope of the report

When it comes to consumer policy, Germany more or less acts in response to impetus coming from the EU. The Federal Government's Consumer Policy Report discusses new business models and potential risks in regard to digital consumer policy and throws up basic

[1] The plural form is used throughout the report to refer to all genders. [Translator's note: This is only of relevance in the German version of the report.]
[2] The term "exceptionalist" is used in the legal debate to refer to those who affirm that disruption is a reality, see Part II, III. 2. below.
[3] Federal Ministry for Economic Affairs and Energy (BMWi)/Federal Ministry of Justice and Consumer Affairs (BMJV), Programme of Measures for More Security, Sovereignty and Self-determination in the Digital Economy < https://www.bmjv.de/SharedDocs/Downloads/DE/Artikel/Ma%C3%9Fnahmenprogramm_BMJV_BMWi.pdf?__blob=publicationFile&v=2)

questions, yet does not go into them in any great detail. The joint initiative of the Federal Ministry for Economic Affairs and the Federal Ministry of Justice and Consumer Protection may serve as evidence of that,[4] given that it says nothing about software agents, regulation by code or big data although these three areas specifically raise questions which urgently need answering.

In 2015 the Advisory Council undertook basic work in regard to the digital world and trade, the digital world and finance, and the digital world and health; the legal issues these raise were left aside, though.[5] This explains the focus of this 2016 Report. The Advisory Council will be continuing its work in 2017 and will, among other things, deliver an opinion on the controversial debate on the worth of data and the right to one's own data.

The Advisory Council commissioned five external studies in 2016 in preparation for this report:[6]

1. *M. Schmidt-Kessel*, *M. Larch, K. Erler, B. Heid, A. Grimm,* University of Bayreuth: Exploratory study on available and missing data in consumer protection law;
2. *K. Purnhagen/St. Wahlen*, University of Wageningen, the Netherlands: The term "consumer" in the 21st century, "consumer citizen" and "consumer producer";
3. *Ch. Wendehorst*, University of Vienna: Problems regarding ownership and property in regard to the Internet of Things which are directly relevant to consumers, plus a market study compiled by the Institute for Innovation and Technology (iit) in Berlin;
4. *G. Spindler*, University of Göttingen: Regulation by technology;
5. *P. Rott*, University of Kassel: Report on opening up and evaluating open questions raised and challenges faced by German consumer law policy in the 21st century.

Reference should also be made to preparatory work done by the Advisory Council in the form of the following four working papers which were drawn up in 2016 and incorporated into this report:

1. *I. Domurath/L. Kosyra*, Consumer Data Protection in the Internet of Things, SVRV Working Paper No. 3;
2. *Ph. Schmechel,* Consumer Data Protection in the EU's General Data Protection Regulation, SVRV Working Paper No. 4;
3. *I. Domurath*, Consumers and Warranties for Material Defects in the Platform Economy, SVRV Working Paper No. 5;
4. *L. Adam/H.-W. Micklitz*, Information, Advice and Intermediation in the Digital World, Legal Issues as Regards Finance, Health and Trade, SVRV Working Paper Nr. 6.

III. Structure and thread of the report

Part II of this report deals with the digital world and its consumer law policy relevance. Part III addresses digital services as reflected in contract law. Part IV looks into the future-related issues of algorithms and big data. Part V delves into new forms of institutional embedding. Parts III to V apply a standard analysis matrix: (1) identifying the problems, (2), illustrating the legal status quo influenced by reform proposals being discussed in the political and academic arena, (3) treating and discussing possible solutions.

[4] Federal Ministry for Economic Affairs and Energy/Federal Ministry of Justice and Consumer Protection (op. cit., fn. 3).
[5] See the 2015 Reports: http://www.svr-verbraucherfragen.de/veroeffentlichungen/ (German only).
[6] The reports and working papers are available (in German only) on the Advisory Council's website:http://www.svr-verbraucherfragen.de/veroeffentlichungen/.

Part II The digital world and its consumer law policy relevance

I. Legal policy context

The authoritative set of rules when it comes to private transactions between consumers and enterprises are to be found in the German Civil Code (*Bürgerliches Gesetzbuch*, BGB); consumer contract law was incorporated into that Code in 2002. Legal policy proposals aimed at radically revising the German Civil Code are a delicate matter, given that they would shake the very foundations of a society which is based on private law. In 2016 the Association of German Jurists tackled the question of whether the German Civil Code needs updating in the age of digitalisation. The expert F. Faust[7] proposed making minor corrections to the German Civil Code although he believes it is in principle possible to tackle the legal issues which digitalisation raises[8] using the range of tried and tested tools available in the Code. That is not to say, though, that there are no critics of such an approach. The overwhelming majority of jurists wants to leave the interplay between private actions and judicial scrutiny well alone.[9]

The one-sided focus on consumer protection legislation being subject to judicial scrutiny, as is currently the case, is problematical. The 2016 Consumer Law Conference addressed the need for and feasibility of administrative scrutiny of consumer protection legislation.[10] The majority of speakers at the conference came out in favour of expanding administrative enforcement of rights in regard to economic consumer protection, regardless of the challenges which digitalisation poses. They believe that official redress should not replace the current model in which control is in the hands of consumer and business associations (referred to in German as the "*Verbandsmodell*"), but that it should supplement it. The notion of official monitoring of terms and conditions, of unfair advertising and, further, of consumer legislation in regulated markets is highly problematical in the context of German law, civil law and German civil-law political theory because it shakes the very foundations of a private-law system in which the enforcement of rights is equal to the enforcement of individual rights before a court. As far as collective redress by way of a cease-and-desist order against terms and condition and unfair advertising is concerned, the general thinking is that the established model of legal redress before the courts should remain.

Of course the balance has shifted in recent years – when it comes to individual redress towards alternative dispute resolution methods (on the instigation of the EU) and when it comes to collective redress towards greater emphasis on collective means of redress over and above cease-and-desist orders, from the importance of a cease-and-desist declaration upstream of a cease-and-desist order towards the controversially discussed introduction of a general collective right to compensation. A proposal may well be put forward in the course of the current legislative term which, in the Federal Ministry of Justice's view, will end up extending associations' right of legal standing.[11] In addition to cease-and-desist orders

---

[7] Faust, *Digitale Wirtschaft – Analoges Recht – Braucht das BGB ein Update?* (report presented at the 71st Conference of the Association of German Jurists in 2016).

[8] In the same vein as Balkin, "The Path of Robotics Law", *California Law Review Circuit*, Vol. 6, June 2015, p. 45: "We should try not to think about characteristics of technology as if these features were independent of how people use technology in their lives and in their social relations with others. Because the use of technology in social life evolves, and because people continually find new ways to employ technology for good or for ill, it may be unhelpful to freeze certain features of use at a particular moment and label them 'essential'."

[9] For a plea for continuity see Dechamps, "Digitale Wirtschaft – das Instrumentarium des BGB genügt", (2016), *Anwaltsblatt*, p. 632; Graf von Westphalen is critical of continuing on the same path, see Graf von Westphalen, "Digitale Revolution – und das Recht bleibt wie es ist?", (2016), *Anwaltsblatt*, p. 619; Blocher, "The next big thing – Blockchain – Bitcoin – Smart Contracts", (2016), *Anwaltsblatt*, p. 612.

[10] Among others, Brönneke/Micklitz/Rott. A publication including the talks edited by H. Schulte-Nölke is in preparation.

[11] Gesell/Meller-Hannich/Stadler, "Musterfeststellungsklage in Verbrauchersachen", *NJW-Aktuell*, Standpunkt, Vol. 5/2016, p. 14–15.

associations are also to be given the option of filing collective claims for damages. The proposal does not break the mould of the *Verbandsmodell* which is currently dominant in Germany.[12]

Collective redress by a consumer authority – as a complement to the *Verbandsmodell* – would lead to a key shift in terms of scrutiny. This would only make sense if it were possible to team up the existing, tried and tested means of enforcement before the courts with the proposed official monitoring. Even though administrative decisions can and must be reviewed by a court, a glance at those EU Member States which have already established a consumer protection authority with the right of legal standing shows that governmental monitoring goes along with a certain amount of de-judicalisation, that is less judicial scrutiny.[13] The current Grand Coalition Government in Germany is more inclined to entrust the task of monitoring terms and conditions and unfair competition to the Federal Cartel Office.

In the course of implementing the EU's Distance Selling Directive, the German legislature introduced the term "consumer" into the German Civil Code in 2000. Key rules of substantive consumer law were then also incorporated in 2002, namely the law of general terms and conditions, regulations on the modalities of contract conclusion (in the case of direct sales and distance selling) as well as rules on specific types of contract (purchase law, time-sharing and consumer credit). Since then these parts of the German Civil Code have been a source of constant legislative disquiet on account of the activities of the EU. Backed by the political majority of the Member States, the EU has become the driving force when it comes to consumer law developments since the 1990s. At the 2012 Conference of the Association of German Jurists one expert[14] proposed taking consumer law out of the German Civil Code altogether and drawing up a separate code. More and more people, reputable German legal scholars, are beginning to agree with him.[15] It is true that since 2002 the German Civil Code appears to be constantly under construction because EU requirements on doorstop selling, distance selling, consumer credit, time-sharing and now travel law have been fundamentally revised since the turn of the millennium.

This trend appears to be repeating itself when one considers the rising debate on digitalising the German Civil Code. All the proposals – in so far as they in fact voice the need for regulation – aim to amend the relevant rules in the German Civil Code, for example the term "consumer", the term "ownership", the law of general terms and conditions, or the term "tort". Following structural logic, this means that the law of digital services would have to be split up. What in fact belongs together would have to be pulled apart and incorporated into the various categories applied in the German Civil Code. The system of classification applied in the German Civil Code takes precedence over the rational logic of the subject matter. This line of thinking necessarily leads to a shortening of perspective, since the German Civil Code and its catalogue of rules determines the possibilities for dealing with legal problems.

What is being overlooked here is the fact that the EU's General Data Protection Regulation and the emerging implementation act overlap with the law of general terms and conditions

[12] "*Verbandsmodell*" refers to the fact that the monitoring of terms and conditions and of advertising is the responsibility of consumer and business associations.

[13] Rott, *Rechtsvergleichende Aspekte der behördlichen Durchsetzung von Verbraucherschutz*, Report submitted to the Federal Ministry of Justice and Consumer Protection, file no. V B1-7008-3-3-52 24/2016. A legal comparison as regards the monitoring of terms and conditions and of fair trading shows that Germany is the exception. No other country has so many different types of court procedures and judicial decisions. Whether more court proceedings equals more consumer protection is another matter entirely, though.

[14] Micklitz, *Brauchen Konsumenten und Unternehmen eine neue Architektur des Verbraucherrechts?*, (report submitted to the 69th Conference of the Association of German Jurists in 2012) p. 129.

[15] Wagner, "Der Verbrauchsgüterkauf in den Händen des EuGH: Überzogener Verbraucherschutz oder ökonomische Realität", (2016), *Zeitschrift für Europäisches Privatrecht*, Vol. 1, p. 87–120, p. 119.

and with fair trading law.[16] One could even hypothesise that the General Data Protection Regulation has been superimposed on the German Civil Code and that it provides the framework not only for data protection but also for the trade in data. A possible medium-term alternative would be a self-contained regulation on digital services as a whole, with all the associated questions and problems as regards contract and tort law in legislation complementary to the General Data Protection Regulation. However, this report, which takes a holistic perspective, first and foremost aims to investigate in what areas action urgently needs to be taken in terms of adapting applicable rules to the challenges posed by the digital world. The entire process will be considered, from when consumers enter into a legal relationship until they terminate that legal relationship.

II. Fundamental decision as regards the scope of digitalisation

Reducing the challenges which digital society faces to the question of whether the German Civil Code or other legislation needs reforming falls short. In fact, it is necessary to look beyond the German Civil Code and legal relationships, to shift from a *micro* to a *macro* perspective, to the question of whether our digital society needs another legal framework, one which can meet the challenges before the possible problems begin to take on more concrete shape in contractual or quasi-contractual questions. It is necessary to look beyond the law to fundamental questions concerning the state, business and society in the age of digitalisation. The scientific debate across all those disciplines which are linked to the issue of digitalisation is divided into two camps: On the one hand there are those who do *not* regard digitalisation phenomena as bringing about radical social, economic, political and philosophical changes; on the other hand there are those who believe that *disruption* is occurring in the development of western industrial and service economies.[17]

1. Continuity

The "business as usual" approach can be found in legal opinions which largely dismiss the changing social environment and define the term "digital content" in line with traditional conceptual jurisprudence and then break it down into the relevant legal questions, namely those regarding media neutrality, data as payment, the content of obligations, the law of general terms and conditions, consumer contracts and special obligations, fulfilment of a contract on digital content, purchase and works contracts, rental agreements and contracts on the drawing up of digital content. Other topics include liability in the context of free services and the protection of data. There is a profusion of literature, which is constantly growing, on each complex of issues which exhausts itself in debating the pros and cons of the need for regulation. The 2016 Conference of the Association of German Jurists set out to address one big issue, the question of the century as it were (unless, given that this is the 21st century and given the scope of digitalisation, it could even be called the question of the millennium): Are the legal rules on business transactions dating back to the 19th century – following the industrial revolution in the second half of the 19th century and the 20th century shift from a manufacturing to a consumption- and service-oriented society – in principle suited to overcoming the challenges posed by 21st century digital society?

The Association of German Jurists sees itself as the mouthpiece of all German – perhaps even of all German-speaking – jurists, practitioners, lawyers, judges and scholars. However, the number of participants attending the civil-law section of the 2016 Conference of the Association of German Jurists fell shockingly below its high demands in terms of content. Depending on one's point of view, one could either play down the relevance of the Association of German Jurists or investigate the reasons for the low attendance figures. The

[16] See Schmechel, *Verbraucherdatenschutzrecht in der EU Grundverordnung*, SVRV Working Paper No. 4.

[17] Brownsword is extremely useful, see *The E-Commerce Directive, Consumer Transactions, and the Digital Single Market: Questions of Regulatory Fitness, Regulatory Disconnection and Rule Discretion*, a talk given at the SECOLA Conference in Tartu in 2016. The manuscript was made available to the authors.

fact remains that the Association of German Jurists has over the many years since it was established very successfully captured the basic attitude of, perhaps even the basic mood among, jurists, at any rate the "prevailing" mood. That is why it is worth emphasising the conclusion F. Faust drew in a report submitted to the 2016 Conference, especially since the majority of those attending endorsed it:

> *Hypothesis no. 13: No new types of contract should be created for contracts relating to digital content.*
>
> *Hypothesis no. 17: It would not be possible to incorporate a "right to one's own data" into section 823 (1) of the German Civil Code. (Instead a new rule should be included in section 303a of the Criminal Code [Strafgesetzbuch, StGB] as protective legislation within the meaning of section 823 (2) of the German Civil Code.)*[18]

The debate is by no means over. In 2017 scholars and teachers of civil law will be looking at the exact same issue. It will be interesting to see what side of the debate the talks and discussions will come down on.[19] At this point, however, and in the context of taking our "fundamental decision", the details of any proposals worth considering are not (yet) the issue. Rather, the question is whether the social, economic and technological circumstances have changed or will change to such an extent that political action beyond making mere marginal corrections is what is needed. Restraint similar to that expressed by *F. Faust* can be found in the reports commissioned by the Advisory Council and rendered by *K. Purnhagen/St. Wahlen*,[20] *Ch. Wendehorst*[21] and *G. Spindler.*[22] In so far as they actually make any, their proposals are limited to possibly supplementing the relevant passages in the German Civil Code, to the term "consumer", the law of general terms and conditions, and the definition of "ownership". That even applies where the analysis leads one to expect something completely different. *Ch. Wendehorst*, for example, feels that

> *"The Internet of Things will doubtless lead to a structural erosion of ownership and property*."

A little further on, on the same page she writes:

> *"Overall, on account of this development consumers are losing the freedom which ownership is supposed to give them and, on account of the price they have to pay when purchasing Internet of Things devices, they are becoming* ***even more heavily dependent than if they had only rented the product*** *[emphasis in original]."*[23]

D. Post[24] described this attitude as "unexceptionalist" and its proponents as "*unexceptionalists*". Accordingly, online and offline transactions should be treated the same as far as possible. Specific rules are not, in principle, required. One need only consider EU Directive 2011/83/EU on consumer rights, in which direct (doorstep) and distance selling are approximated as far as possible – and then the difficulties which such approximation brings when it comes to dogmatic fine-tuning.

---

[18] That is effectively a classical case of how the German Civil Code remains formally intact, no changes are made but the relevant questions are shifted into other legislation.
[19] These will be published in the *Archiv für die civilistische Praxis*.
[20] Purnhagen/Wahlen, *Der Verbraucherbegriff im 21. Jahrhundert, Verbraucherbürger und Verbraucherproduzent*, Report commissioned by the Advisory Council for Consumer Affairs at the Federal Ministry of Justice and Consumer Protection, August 2016.
[21] Wendehorst, *Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge*, Report commissioned by the Advisory Council for Consumer Affairs at the Federal Ministry of Justice and Consumer Protection, October 2016.
[22] *Regulierung durch Technik*, Report commissioned by the Advisory Council for Consumer Affairs at the Federal Ministry of Justice and Consumer Protection, November 2016.
[23] Wendehorst (op. cit., fn. 21), p. 62.
[24] Post, *In Search of Jefferson's Moose,* (OUP, 2015), p. 186.

The guiding principle of treating online and offline enterprises the same also runs like a red thread through the Federal Ministry for Economic Affairs' Green Paper on Digital Platforms.[25] This might be acceptable if there were an easy answer to the following crucial question: Can offline and online transactions be treated the same or is there a fundamental difference between the two which not only justifies but requires that they be treated differently? All too often the need for equal treatment is presupposed, cutting off all further discussion, not least because it is borne by the central idea that the law is uniform, that it applies equally to all – a maxim adopted by the French Revolution which quite rightly still has a formative influence.

The unexceptionalists are also referred to as "contractualists". They seek to overcome the challenges which technology poses by defining a contract as something which is concluded consensually and autonomously between two people. The crucial maxims here are self-responsibility and the freedom to contract, i.e. self-regulation rather than state regulation. What applies to contract law in principle also ought to apply to all other relevant legal fields. As a result, the focus is put on introducing sectoral rules for the Internet, telecommunications and energy, an approach which the EU has been forcefully promoting for the last 30 years. In the same way as the basic rules of contract law cannot be understood until rules applicable to consumer goods purchases have been incorporated, focusing on the horizontal relevance of anti-trust law or fair trading law obscures a multitude of special rules which are applicable to regulated markets and/or consumers. After all, the power of the claim to general application is specifically its rationality. Any deviation needs to be justified. It is telecommunications law in particular which causes upheavals in the course of digitalisation, because key digital services are excluded from the specific sectoral rules.[26] The all-important question is whether digitalisation means we need to adopt a new perspective which is entirely oriented to the specifics of the digital world and which places the focus on the changes made compared to the old world and old law. Put another way: What if what is "special" becomes the "new normal" or if this special law continues expanding and leads to a fragmentation of the law, which only leaves the new normal with having a catch-all function?[27]

2. Disruption

Is disruption happening? Will it happen? How will it manifest itself – as evolution or revolution? Those who proclaim that a rupture with the past is occurring argue that the phenomenon of digitalisation can best be captured by means of the formula "from atoms to bits".[28] Prior to digitalisation, the universe comprised only two levels or layers: a physical and a social. The physical layer comprises atoms and all material things, houses, automobiles, people and animals. The social layer comprises all those phenomena which the law describes as immaterial, that is rights, enterprises and status-related rules. Digitalisation adds a third layer. In the words of A. Murray: "*Much as atoms can be used in the physical world to construct everything from the human liver to an Airbus 380, bits are the basic building blocks of the information society.*"[29]

M. Hildebrandt speaks of a "new animism"[30] which characterises the "onlife" world:[31]

---

[25] In particular Schweitzer <https://www.bmwi.de/BMWi/Redaktion/PDF/G/gruenbuch-digitale-plattformen,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pd> (last retrieved 24 Nov. 2016).
[26] Chapter 4 (Challenges for Telecommunications Law) is convincing <https://www.bmwi.de/BMWi/Redaktion/PDF/G/gruenbuch-digitale-plattformen,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf> (last retrieved 24 Nov. 2016).
[27] Luhmann and Teubner, following Luhmann, both repeatedly stress that the stratification of society, as reflected in fragmented law, is irreversible. Teubner also makes it clear that new irritants keep popping up, see "Legal Irritants: Good Faith in British Law or How Unifying Law Ends Up in New Divergences" (1998), *61 Modern Law Review*, 1998, p. 11.
[28] Searle, *The Construction of Social Reality*, (Allan Lane, The Penguin Press, 1995).
[29] Murray, *Information Technology Law: The Law and Society*, 2nd ed. (OUP, 2013), p. 5.
[30] Hildebrandt, *Smart Technologies and the End(s) of Law* (Cheltenham: Edward Elgar, 2015) viii.
[31] Hildebrandt (op. cit., fn. 30), p. 8.

> *"… our life world is increasingly populated with things that are trained to foresee our behaviours and pre-empt our intent. These things are no longer stand-alone devices; they are progressively becoming interconnected via the cloud, which enables them to share their 'experience' of us to improve their functionality. We are in fact surrounded by adaptive systems that display a new kind of mindless agency. (...) The environment is thus becoming ever more animated. At the same time we are learning slowly but steadily to foresee that we are being foreseen, accepting that things know our moods, our purchasing habits, our mobility patterns, our political and sexual preferences and our sweet spots. We are on the verge of shifting from using technologies to interacting with them, negotiating their defaults, pre-empting their intent while they do the same to us."*[32]

In this *onlife* (not online) world, the consumption of products is personalised, anticipatory and automated. Of course, this new world of consumption will always need a contract or at least a legal relationship which humans conclude/enter into via a service. From the moment a human enters the digital world, though, smart technology takes over. In the *onlife* world the boundaries between the offline and online worlds become blurred, the distinction between consumer transactions which are negotiated by humans and those which are managed and implemented by software agents even more so.

One can and must go very much further and ask whether, in the onlife world, consumer protection regulations will be replaced by smart technologies. Instead of consumer protection by law and legislation we will have consumer protection by technology and self-regulation or, to put it more succinctly: regulation by technology. The perspective shifts again. The focus is on technologies such as blockchain, Bitcoin and smart contracts, which have not yet become established beyond the fringes of the business world (speed trading) and in particular have not yet entered consumer law. Estimates as to what chances legislation has of being replaced by technology vary greatly. *G. Spindler*'s assessment is cautiously sceptical, because the law cannot be translated into the black and white logic on which software is based.[33] *W. Blocher*, by contrast, is quite euphoric when it comes to the prospects of regulation by technology, not least in the sense of its inherent possibilities for (re)gaining autonomy and for reversing legal relationships (from B2C to C2B).[34]

Those who get a sense that fundamental technological and social changes are close at hand must, logically, be described as *exceptionalists*. They seek what is "new" and feel that the world has changed, that the relationship between humans and technology has been entirely redefined. They call for a *Digital Code* "to safeguard civil liberties in the age of Internet capitalism".[35] *Cyberbutlers*,[36] our constant companions who still sounded rather utopian back in 2000, have long since become a reality. However, our contracts with service providers often have decade-long terms. Our legal system is not set up to cope with these kinds of temporal dimensions. You do not have to look to the future to draw this consequence. Most of us have been using Google on a daily basis for years, the same goes for Facebook. Google and Facebook have collated data about our lives, and these form the basis of their business models. Digital services contracts, that is in so far as they are contracts in the

---

[32] Hildebrandt (op. cit., fn. 30), at viii-ix.
[33] Spindler, (op. cit., fn. 22), likewise Idelberger, *Connected Contracts Reloaded – Blockchains as Contractual Networks*, talk given at the SECOLA Conference in Tartu in 2016, publication in preparation.
[34] Blocher "The next big thing: Blockchain – Bitcoin – Smart Contracts – Wie das disruptive Potential der Distributed Ledger Technology (nicht nur) das Recht fordern wird" (2016), *8+9 Anwaltsblatt*, p. 612.
[35] Graf von Westphalen (op.cit., fn. 9), p. 626, though very much focused on the risks which digitalisation incurs for humans (especially making reference to Schirrmacher, *Technologischer Totalitarismus*, Suhrkamp Verlag, 2014).
[36] Ford, "Save the Robots: Cyber Profiling and Your So-Called Life" (2000), *52 Stanford Law Review,* p. 1572.

sense of a two-sided legal transaction, establish a continuing obligation which stands alongside traditional types of contracts such as rental, credit and energy agreements.[37]

III. Possible consequences of the debate around continuity v. disruption

What are the consequences for the legislature of this tension between the old and new, between continuity and disruption? Do we need legal regulations for contracts which consumers conclude with their cyberbutler? Do we need more and more far-reaching interference on the part of the legislature in order to control self-regulation or self-regulation which is becoming increasingly independent ex ante? If so, then the advocates prove to be *regulators*: Instead of freedom of contract and self-regulation they want the legislature to be responsible for ex-ante scrutiny and supervision, perhaps coupled with the need for competent governmental agencies to rectify self-regulation ex post where necessary.

Where does the European Commission stand on this issue and how far has the German legislature got in terms of its planning and deliberations? The European Commission is rushing ahead, saying there is a strong need to continue developing contract law. Its Communication dated May 2015 is very telling:[38]

> *"Digital contracts for Europe – Unleashing the potential of e-commerce"*

Further on:[39]

> *"4. ACTING BEFORE IT IS TOO LATE*
>
> *"We need to act now on the digital dimension...*
>
> *"The pace of commercial and technological change due to digitalisation is very fast, not only in the EU, but worldwide. The EU needs to act now to ensure that business standards and consumer rights will be set according to common EU rules respecting a high level of consumer protection and providing for a modern business friendly environment. It is of utmost necessity to create the framework allowing the benefits of digitalisation to materialise, so that EU businesses can become more competitive and consumers can have trust in high-level EU consumer protection standards. By acting now, the EU will set the policy trend and the standards according to which this important part of digitalisation will happen."*

The Commission has gone further than merely making announcements: In December 2015 it put forward two proposals, one on the regulation of digital content and one on online and other distance sales of goods.[40] Both Proposals aim at full harmonisation, and both are the subject of intense legal policy and academic debate.[41] That debate revolves around the canon of questions which the Association of German Jurists already raised, namely meeting

---

[37] Nogler/Reifner (eds), *Life Time Contracts,* <http://www.eusoco.eu/wp-content/uploads/2013/10/eusoco_book_outline.pdf> (last retrieved 24 Nov. 2016).

[38] European Commission, Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee – Digital contracts for Europe – Unleashing the potential of e-commerce, COM(2015) 633 final, Brussels, 9.12.2015.

[39] COM(2015) 633 final (op. cit., fn. 38).

[40] European Commission, 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, Brussels, 9.12.2015; and European Commission, Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods, COM(2015) 635 final, Brussels, 9.12.2015.

[41] EuCML has addressed this subject matter in a number of publications. Three books deserve special mention: Wendehorst/Zöching, *Ein neues Vertragsrecht für den digitalen Binnenmarkt*, Wendehorst/Zöching (eds) (Manz Verlag, 2016); Franceshi, *European Contract Law and the Digital Single Market, The Implications of the Digital Revolution*, (Intersentia Verlag, 2016); and Schulze/Staudenmayer, *Digital Revolution: Challenges for Contract Law in Practice,* (Nomos Verlag, 2016).

the digital challenges by means of contract law. What is behind this strong rhetoric? Is the EU calling for a new legal order?

R. Brownsword[42] looked at both Proposals with a view to the difference between unexceptionalists and exceptionalists and came to the conclusion that the European Commission has to be classed as an unexceptionlist. What is more relevant from a consumer policy perspective is that the Commission is attempting, with the help of these two Proposals, to roll back the previously guaranteed level of consumer protection in regard to online purchase contracts in favour of trade and commerce. More specifically, there is a certain degree of tension between the Consumer Goods Directive 1999/44/EC on the one hand and the Consumer Rights Directive 2011/83/EU, which regulates direct and distances sales, on the other. The two Proposals interleave the two Directives. Yet again, the much-criticised objective of full harmonisation leads to less protection, this time, though, less protection as already guaranteed in EU directives. In other words, online trade serves to harmonise consumer law for the online and offline worlds, to the consumer's detriment. The new technology and the proclaimed need to expand online trade serve to legitimise the Commission's approach.

The Federal Government's 2016 Consumer Policy Report[43] does not address the fundamental question, namely regulation of the "onlife" world. However, the report does state the following, much in the same vein as the European Commission:

> *"Digitalisation doubtless does also have its economic advantages, but it poses new challenges when it comes to consumer protection. It is the job of policy-makers to put in place the regulatory framework for binding and effective consumer protection standards in the digital world. Strengthening self-determination, guaranteeing freedom of choice and transparency, comprehensive and comprehensible consumer information, and security in the Internet are decisive. That is the key to more consumer confidence, which is necessary if new business models and digital innovations are to succeed. Consumer data protection is of particular relevance in this regard."*

The report addresses neither of the two Commission Proposals. The measures announced by the Federal Government make no reference whatsoever to the fundamental problem, nor to the question of whether digital legal relations require specific rules, to name just this example from the context of possible regulatory approaches. The Federal Government restricts itself to the correction of details, as do the vast majority of legal scholars.

The approach adopted by the Federal Ministry for Economic Affairs and Energy in its Green Paper on Digital Platforms appears to be much more fundamental in its approach, because it is more open in the matter itself.[44] That may well be down to the nature of a green paper, which seeks to ask questions rather than to provide answers. These are expected to be delivered in the upcoming White Book in the spring of 2017. We will have to wait and see whether they will be exceptionalist or unexceptionalist answers. Questions around the Guidelines on *Data Sovereignty – Input for the Creation of Private Digital Autonomy* and the call for a digital agency are particularly relevant from the point of view of consumer protection:[45]

> *"A digital agency in the guise of a high-performing and internationally interconnected federal-level centre of expertise could have these remits. It could support other specialist authorities (such as the Federal Cartel Office and*

[42] Brownsword, *The E-Commerce Directive, Consumer Transactions, and the Digital Single Market: Questions of Regulatory Fitness, Regulatory Disconnection and Rule Redirection*, talk given on 18 June 2016 at the SECOLA Conference in Tartu, Estonia, http://www.secola.org/.
[43] Bundestag Printed Paper 18/9495, 25 Aug. 2016, p. 10.
[44] As at May 2016; a white book containing concrete proposals is set to be published in spring 2017, p. 64.
[45] Faust (op. cit., fn. 7) p. 66.

consumer protection offices) in the digitalisation process and also identify and eliminate obstacles to implementing policy strategies. Like the Federal Environment Office and the Federal Office for Migration and Refugees, a new digital agency can help to meet one of the key social challenges we face."

The impetus for the latter came in the autumn of 2015 from the Federal Ministry for Economic Affairs and Energy/Federal Ministry of Justice and Consumer Protection's Programme of Measures for More Security, Sovereignty and Self-determination in the Digital Economy – Challenges and Action for Society, Business and Consumers.[46] Depending on their interpretation and orientation, data sovereignty, digital autonomy and the digital agency could become milestones in the development of digital consumer law.

Part III Legal relationships in regard to digital services

The micro perspective seeks to address the well-known and mounting problems as regards consumer law, including consumer data protection law. The focus is increasingly being placed on four topics which are oriented to social issues and not to a system of classification of whatever shape or form which is predetermined by the legal system. This list of topics is, however, not necessarily to be regarded as exhaustive. The Internet of Things is becoming the ostensible phenomenon in which consumer law and data protection law are increasingly becoming intertwined. "A new dimension has been added to the world of information and communication technologies: from anytime, anyplace connectivity for anyone, we will now have connectivity for anything."[47] According to a report published by the UK Government,[48] more than 14 billion devices worldwide were already connected to the Internet in 2014.

This deterritorialised connectivity of things which is also devoid of any temporal context gives rise to numerous problems. For example, ethical issues raise the fundamental question of how we as humans should act and behave.[49] The Internet of Things is of relevance to ethical issues on account of the changes made to key terms because of how technology connects the world of things with our everyday lives. The fact that things can communicate with each other entails a considerable loss of control on the part of humans. This raises questions around social justice, trust, the blurring of contexts and the lack of consumers' and citizens' neutrality and autonomy.

Part III of this report addresses the legal questions which arise from this deterritorialised connectivity. They concern the conclusion of contracts, contracting parties, problems around the legal classification of the actions of platforms, liability for defects, IT security, data protection and problems regarding the enforcement of rights in deterritorialised contexts. The following issues will be discussed against this backdrop:

- Issues around the conclusion of a contract and liability,
- The role and function of platforms,
- Data protection and IT security and
- The deterritorialisation of consumption. (Consumers often do not know where an enterprise is domiciled; if it is domiciled abroad, a complicated set of legal building

[46] Federal Ministry for Economic Affairs and Energy/Federal Ministry of Justice and Consumer Protection, (op. cit., fn. 3).
[47] <http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf> (last retrieved 17 Nov. 2016).
[48] <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf> (last retrieved 17 Nov. 2016).
[49] This paragraph is based on Haarkötter, "Eine neue Ethik für das Internet der Dinge?": <https://www.bpb.de/dialog/netzdebatte/198471/eine-neue-ethik-fuer-das-internet-der-dinge> (last retrieved 18 Nov. 2016).

blocks is available which has a great deal to offer legal scholars but is of very little benefit to consumers.)

Part III concludes with a discussion of viable solutions. So far, enterprises have in practice dictated the matter by way of their terms and conditions, advertising and regulation by design. The field has now recently also come to the attention of jurists. The result is an overwhelming array of suggestions for solving certain legal issues, or not as the case may be. Only the EU has so far reacted to this development by making any legislative proposals in the form of the General Data Protection Regulation and its 2015 Proposal on digital content in consumer contracts. The Association of German Jurists has looked into the matter. However, it has not really been in any position to make any suggestions for solving what are as yet unanswered questions.

I. Conclusion of contract

This section addresses the civil-law problems which arise in connection with Internet of Things devices. In particular, they include the packaging of services, the obligations on digital service providers offering "as is" services[50] regulated by means of terms and conditions, and the special problem of the classification, under civil law, of declarations of intent when automated systems are used in the Internet of Things.

1. Information and packaging

Hardware and software

Today, when consumers purchase technical devices the software is generally pre-installed. The practice of packaging services is not ruled out per se under fair trading law; the incentive effect of a good offer is always a desirable consequence of performance-based competition.[51] The European Court of Justice (ECJ) recently ruled that pre-installed software on a computer was not an unfair commercial practice. The case revolved around the question of whether the lack of price information regarding individual programs represents a misleading commercial practice within the meaning of Article 5(4)(a) and Article 7 of the Unfair Commercial Practices Directive 2005/29/EC. The ECJ came to the conclusion that the mere lack of price information did not result in any misleading of consumers, since the lack of information regarding individual programs was neither suited to preventing consumers from making an informed transaction decision, nor to causing them to take a transaction decision which they would otherwise not have taken. The price of individual programs did not, therefore, represent material information within the meaning of Article 7(4) of Directive 2005/29/EC and the omission of that information was not misleading.[52] This interpretation is contestable because it misconstrues the role and function of Article 7(4), which not least demands transparency ahead of the conclusion of a contract in order to permit competition. Accordingly, an informed decision is one which not only serves the consumer but also potential competition between the suppliers of the individual price components.

Services and data

Another much-debated issue which needs to be addressed in the context of digital services, whether they are provided by commodity dealers, app stores or other platforms, is that of "data as payment". This problem is, firstly, discussed in the context of the debate on consumer sovereignty and in the debate on data protection v. data sovereignty; secondly,

[50] Consumers have no influence on the service provided. The supplier can adapt the service at any time.

[51] Ohly, "Das neue UWG – Mehr Freiheit für den Wettbewerb?", (2004), *Gewerblicher Rechtsschutz und Urheberrecht*, Vol. 11, p. 889–900, p. 897, with further references.

[52] Case C-310/15, Vincent Deroo-Blanquart v. Sony Europe Limited, successor in law to Sony France SA, EU:C:2016:633.

legal problems arise when characterising contracts and their termination. The focus in the following will be on consumer law issues.[53]

Many contracts for digital services turn out to be "free of charge", either in the case of the purchase of free apps or the free use of platforms. At the same time most business models are built around consumer data being used to optimise digital services. This begs the question of whether consumers are not in fact "paying" for the use of the app or platform and what consequences that has for consumer protection law.

Section 312 (1) of the German Civil Code provides that sections 312 to 312h of the Code are only applicable to non-gratuitous contracts, as a result of which "data as payment" would lead to the applicability of a variety of other consumer protection provisions. However, this provision is likely not compatible with Community law.[54] Non-gratuitousness may also have consequences for the liability standard applied (see, e.g., sections 521 and 599 of the German Civil Code).[55] However, the reductions in liability in the German Civil Code appear not to fit, at least not to a contract of use concluded between a platform operator and a consumer. A relationship between a supplier and consumer will generally lead to a typical "contract under the German Civil Code".

2. Information: consent and terms and conditions

Before concluding a contract consumers are inundated with information. The problems which they face in working through and understanding all this information have become a commonplace in discussions around information overload.[56]

Using terms and conditions serves to standardise and structure information. The aim is to make it easier to access the economic system of mass production and mass sales in the distance selling system. The monitoring of contract terms is based on the understanding that on account of their being structurally unequal consumers have no means of influencing the content of those terms.[57] Nevertheless, the limits to monitoring terms and conditions when it comes to providing effective consumer protection are now well-known. The European Commission recently published a study on problems consumers have with terms and conditions which confirms that the majority of consumers neither read the terms and conditions nor find out about their rights in any other way.[58]

3. Information and the subject matter of the legal relationship

Many digital services are provided in the context of enduring legal relationships. This in particular raises the question of whether and to what extent manufacturers are obliged to make updates available for the software they produce beyond the end of the contract term, and whether and to what extent consumers are obliged to install those updates. The 2016 Conference of the Association of German Jurists concluded that the manufacturer was to be under no obligation to provide updates, because it is to be left to consumers to decide whether they actually want the update.

---

[53] The Advisory Council will be looking into data sovereignty in the course of 2017.
[54] Faust, *Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update*?, (report submitted to the 71st Conference of the Association of German Jurists in 2016), S.A12.
[55] Faust, (op. cit., fn. 54), S.A13.
[56] The debate began in sociology and psychology (see Simmel, *Die Großstädte und das Geistesleben,* (1903) and Miller, "The magic number seven, plus or minus two: some limits on our capacity for processing information", (1956), *Psychological Review*, p. 81–97) but has now also been taken up in the economic/legal literature, see, e.g., Paredes, "Blinded by the Light: Information Overload and Its Consequences for Securities Regulation", (2003), *Washington University Law Quarterly*, Vol. 81, p. 417.
[57] See Raiser, *Das Recht der Allgemeinen Geschäftsbedingungen*, (Hermann Gentner Verlag, 1961) for a fundamental approach to this issue.
[58] Elshout et al., *Study on Consumers' Attitudes towards Terms and Conditions (T&Cs),* Final report, European Commission, Directorate-General for Justice and Consumers, 21 March 2016, Brussels.

However, at least one important exception should be made to this basic principle, and that concerns IT security. This is due to the great vulnerability of digital services to hacking and malware, above all on account of the low level of security mechanisms which manufacturers provide, usually based on a standard set of default passwords. Personalised passwords for Internet of Things devices such as refrigerators, washing machines, television sets etc. are not yet very widespread or common. The vulnerability of the Internet of Things network as a whole was recently made clear during the Distributed Denial-of-Service (DoS) attack on 21 October 2016, when home routers and Internet of Things devices were infected with malware and websites such as Twitter, PayPal and Airbnb were then taken down by fake traffic. This was possible because the malware created a botnet comprising the millions of infected computers which were used to launch targeted attacks on one of the main servers used by many websites.[59]

System and program updates could provide potential protective mechanisms against such malware. The option of introducing a manufacturer's obligation raises the question of whether guaranteeing IT security is a "cardinal obligation" under the obligation pursuant to section 241 (2) of the German Civil Code. What is clear is that the statutory obligation to provide IT security, including software maintenance and upgrades or updates, generally represents an obligation to protect pursuant to section 241 of the German Civil Code.[60] Software maintenance comprises all those services which keep the purchased software fully functional or restore its functionality.[61]

However, the technical changes to which software is subject cannot automatically give rise to a permanent maintenance agreement.[62] Section 19 of the Act against Restraints of Competition (*Gesetz gegen Wettbewerbsbeschränkungen*, GWB) at most results in a statutory obligation when the software supplier has a dominant position on the market. Whether section 242 of the German Civil Code leads to an obligation to provide updates is controversial. On the one hand it could result analogously in the obligation to supply spare parts for at least five years.[63] In that case it is still relevant whether the maintenance services are only a subsidiary obligation (only claims for damages) or a separate contractual obligation (right of fulfilment).[64] According to *H.-W. Moritz*,[65] where software maintenance is a free service, it must generally be regarded as merely a subsidiary obligation. However, as soon as customers have to pay a fee, it will have to be regarded as a primary obligation. Irrespective of the criterion of whether a fee has been paid, it will likely have to be regarded as a primary obligation if the maintenance agreement has been explicitly set out in the software licence agreement.

On the other hand, one must ask whether consumers are obliged to protect themselves against malware attacks by acquiring and installing important system and program updates. *Spindler* affirms such an obligation at least for automatic or semi-automatic system and

[59] Regarding the general risks, see Spindler, *Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären*, (study commissioned by the Federal Office for Information Security) p. 30 et seqq.
[60] Schmidl, *Corporate Compliance Handbuch der Haftungsvermeidung in Unternehmen,* Hauschka/Moosmayer/Lösler (eds), (3rd ed., 2016, C.H. Beck Verlag), margin no. 129 in section 28 on the law of IT security.
[61] Moritz, *Computerrechtshandbuch Informationstechnologie in der Rechts- und Wirtschaftspraxis,* Kilian/Heussen (eds), (32nd supplement, 2013, C.H. Beck Verlag), margin no. 190 et seqq. regarding claims for defects in the case of hardware and software contracts.
[62] See Moritz, (op. cit., fn. 61), margin no. 199 et seq. regarding claims for defects in the case of hardware and software contracts.
[63] Hoeren, *Vertragsrecht und AGB-Klauselwerke*, Graf von Westphalen/Thüsing (eds), (38th supplement, 2016, C.H. Beck Verlag), margin no. 77 regarding IT contracts.
[64] Schmidl, *BGB-Schuldrecht Kommentar*, Dauner-Lieb/Langen (eds), 3rd ed., 2016, Nomos Verlag, margin no. 137 regarding the German Civil Code, Annex IV re sections 535 to 580a: The Law of Software Contracts.
[65] Moritz, (op. cit., fn. 61), margin nos 196 to 197 regarding claims for defects in the case of hardware and software contracts.

program updates which can be installed via an update service embedded in the system, as such installation is economically reasonable.[66]

The interplay between a manufacturer's and a consumer's obligations when it comes to the safety of the IT network and the devices which are produced and used complement public-law regulation in the field of product safety and civil-law product liability.

4. The special issue of the Internet of Things: use of e-people

One issue which needs to be clarified when it comes to the conclusion of contracts in the Internet of Things is whether the rules set out in the German Civil Code are sufficient to cover declarations of intent made by automated or autonomous systems or liability issues in the case of defaults and damage. Can a washing machine make a declaration of intent to purchase washing detergent by means of an order process which is triggered automatically? Can a refrigerator be held liable for automated but incorrect purchases? Can a self-driving car be held liable in the case of an accident?

Conclusion of contract: declarations of intent

A basic distinction needs to be drawn in the Internet of Things between two different systems: automated systems in which users themselves determine the outcome by setting parameters and autonomous systems which control the extent of their own behaviour and can act without any input from the user.[67] Taking the example of an Internet-connected washing machine in a smart home that would mean that if the washing machine independently orders washing detergent once the fill level drops below a certain point which has been predetermined by the user (brand, size of package and online shop), it represents an automated system. If the washing machine can order the washing detergent independently, then it is acting autonomously.

The rules in the German Civil Code ought, for the time being, to be sufficient to cover to specifics as regards the conclusion of contract. The example of the automated ordering of washing detergent "by the washing machine" is, in principle, the converse of a contract concluded for vending machines.[68] The washing machine's user makes an anticipated offer within the meaning of sections 133 and 157 of the German Civil Code under the condition of the proper functioning and availability of the specific washing detergent from the specific dealer and, possibly, at a specific price (section 158 (1) of the German Civil Code). The online shop then accepts the offer at the latest when it sends the goods to the customer (sections 133 and 157 of the German Civil Code).

Liability for criminal acts

When it comes to contractual liability, it is the type of underlying contract with the respective contracting partner (see below regarding the problem of platforms) which is decisive. When it comes to the liability of the producer, it is in particular the rules of section 823 of the German Civil Code which are relevant. According to those provisions, the manufacturer must ensure, within the bounds of what is technically feasible and economically reasonable, that the absolute rights of the users of the product are not violated (on account of the trader creating a source of risk by placing a faulty product on the market) or that a third party's absolute

[66] Spindler, *Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären* (op. cit., fn. 59) p. 124 et seq.
[67] Sosnitza, "Das Internet der Dinge – Herausforderung oder gewohntes Terrain für das Zivilrecht?", (2016), *Computer und Recht*, Vol. 11, p. 764–772, p. 765.
[68] Sosnitza, (op. cit., fn. 67) p. 766.

rights are not violated.[69] This category includes design fault, manufacturing defects (including IT security gaps),[70] instruction errors and product monitoring defects.[71]

A design fault arises when the technical concept is incorrect, for example the software in a smart device is programmed in such a way that it does not prevent the avoidable violation of absolute rights.[72] Manufacturing defects, including IT security gaps,[73] arise through faulty manufacturing. In the case of instruction defects the manufacturer is also liable for damage which arises on account of the fact that, contrary to its obligation, the manufacturer did not draw the user's attention to the risks which may arise during use despite fault-free manufacturing of the product. IT security gaps, too, are design faults. In order to meet the product monitoring obligation, a manufacturer must collect all the product-related information which reveal a product's risk features. If this information permits conclusions to be drawn regarding the danger inherent in the product, then the manufacturer is also under the active obligation to take measures to minimise the risk.[74]

The applicability of section 823 et seqq. of the German Civil Code is problematical in regard to autonomous systems if the manufacturer is not at fault. Only in the case of lack of due diligence would the manufacturer be liable in any way. According to *Bräutigam* and *Klindt*, in such cases parallels might possibly be drawn to strict liability under section 933 of the German Civil Code (animal owner's liability).[75] It is doubtful, though, whether mechanical learning leads to comparable unpredictability. The unpredictability of a system's decisions would be the decisive condition for the person who set up the system to be held liable. The crucial issue here is to what extent autonomous systems are able to take unpredictable decisions based on their underlying algorithms or whether they are always able to choose the "best" option from among a number of foreseen scenarios and data sets in the context of a new, previously unforeseen scenario. The key thing is how the underlying algorithm is constructed. Account must be taken of the fact that the design of a machine-learning system is based on generalisation beyond those data sets which have been input into the system; that is they build a model out of the sample inputs.[76] That means that the legal interpretation of "unpredictability" will cause problems, since an algorithm is set up in such a way that it can react to unforeseen events, but this response is dependent on the data and "decision-making paths" previously input by the programmer.

II. The role of online platforms

Legal relationships in the context of the Internet of Things are complex, and not just on account of the IT systems which are involved. The various possible constellations of

[69] Hamm Higher Regional Court, judgment of 21 Dec. 2010 (file no. 21 U 14/08); Federal Court of Justice, judgment of 31 Oct. 2006 (file no. VI ZR 223/05) (Karlsruhe Higher Regional Court).
[70] Spindler, *beck-online. GROSSKOMMENTAR,* Gsell/Krüger/Lorenz/Mayer (eds), Spickhoff (ed.), as at 1 April 2016, C.H. Beck Verlag, margin no. 645 re section 823 of the German Civil Code.
[71] Staudinger, *Bürgerliches Gesetzbuch Handkommentar*, Schulze (ed.), 9th ed., 2017, Nomos Verlag, margin no. 172 re section 823 of the German Civil Code.
[72] Liability pursuant to section 823 et seqq. of the German Civil Code also covers software, because in the context of section 823 et seqq. of the German Civil Code the characteristics and thus the dispute is not relevant to whether software is defined as a thing, see Spindler, "IT-Sicherheit und Produkthaftung – Sicherheitslücken, Pflichten der Hersteller und der Softwarenutzer", (2004), *Neue Juristische Wochenschrift*, Vol. 44, p. 3145–3208, p. 3145.
[73] Conrad, *Handbuch IT- und Datenschutzrecht*, Auer-Reisdorff/Conrad (eds), (2nd ed., 2016, C.H. Beck Verlag), margin no. 382 re section 33, Compliance, IT Security, Correctness of Data Processing.
[74] Nietsch, *Verbraucherrecht*, Tamm/Tonner (eds), (2nd ed., 2016, Nomos Verlag), margin no. 68 re section 823 (1) of the German Civil Code.
[75] Bräutigam/Klindt, "Industrie 4.0, das Internet der Dinge und das Recht", (2016), *Neue Juristische Wochenschrift*, Vol. 16, p. 1137–1142, p. 1139.
[76] Domingos, "*A Few Useful Things to Know about Machine Learning*", University of Washington, <https://homes.cs.washington.edu/~pedrod/papers/cacm12.pdf> (last retrieved 28 Nov. 2016).

contracting parties raise further legal questions. Since platforms[77] can act as intermediaries to facilitate the conclusion of a contract between suppliers and demanders and can, in certain circumstances, even be actively involved in shaping those contracts, uncertainties are beginning to mount regarding who the contracting party is, what type of contract is being concluded as well as liability issues.

1. Vagueness of the terminology applied

Given their numerous different types of business models, questions arise as to how to classify platforms. There is no standardised definition of what a platform is. Various attempts have been made, for example based on the consumer's objective, economic criteria or the type of offer. It is difficult to precisely classify platforms on account of their complexity, the numerous different business models applied and the resulting consumer protection issues. As a lowest common denominator, platforms have been defined as a place where demand and supply are brought together and the platform operator exercises a controlling function.[78]

This is not to deny the need to categorise platforms. Functional approaches based on the materiality of the transaction (goods or services?), the actual transfer of ownership, role swapping between supplier and consumer, or the durability of activities undertaken on the platform are definitely useful.[79] However, were other types of platforms to be included as well, the spectrum of functionalities might prove narrow, or too detailed. The traditional binary nature of legal provisions (a subject matter can either be subsumed under a provision or not) reaches its limits here. Digital platforms operate in an extremely flexible, innovative business sector which is undergoing rapid and constant change. As a result the rigid categorisation and definition of what platforms are becomes less the issue than accumulating approaches which contribute to a legal understanding of them.

2. Pattern of problems: information, supplier, liability, transparency and competition[80]

Regardless of the fact that no definition of what platforms are is yet available, what they all have in common is a number of recurring problems. Some will at least be covered by existing legal provisions, others only with difficulty.[81] The problems can be divided into information problems (knowing who your contracting partner is) and the complexity of legal relationships, contractual obligations, liability issues and problems concerning competition law.

Information problem: knowing who the supplier is and that supplier's status

On account of the nature of websites and contradictory terms and conditions, consumers sometimes do not know whether they are concluding a contract with a platform operator or supplier; often it is even unclear whether they are actually concluding a contract. Use of an Internet platform is as a rule dependent on the platform operator supplying conditions of use. The creation of a user account can be classed as the conclusion of a contract of use,[82] at

[77] In the following the term "platform" is used synonymously with "online platform". For a definition, see: Federal Ministry for Economic Affairs and Energy, *Grünbuch Digitale Plattformen*, 2016. http://www.bmwi.de/DE/Themen/Digitale-Welt/Netzpolitik/digitale-plattformen.html (last retrieved 30 Nov. 2016), p. 27.

[78] Adam/Micklitz, *Information, Beratung und Vermittlung in der digitalen Welt, Rechtsfragen in Finanzen, Gesundheit und Handel*, SVRV Working Paper Nr. 6.

[79] For example for the sharing economy, see Purnhagen/Wahlen, (op. cit., fn. 20), p.14.

[80] This section is based on Adam/Micklitz (op. cit., fn. 78).

[81] The complex of legal relationships would become even more complicated if one were also to incorporate advertisers as the "fourth player". Similar provisions would be applicable to advertisers as apply to providers in their relationship with consumers; in particular account would in addition have to be taken of competition law provisions. The obligations incumbent upon the platform operator in regard to advertisers' compliance with statutory law could also be addressed once more.

[82] See Glossner, *Münchner Anwaltshandbuch IT-Recht,* Leupold et al. (eds), (3rd ed., 2013, C.H. Beck Verlag), margin no. 358 in Part 2: The Law of E-Commerce; and for app stores: Loos, "Standard

least when the consumer has to pay to use the site. Consumers are generally not aware of this consequence.

The lawfulness of such a contract of use can be questioned for various reasons. First of all, platform operators can make use of a number of liability exemptions, for example under section 10 of the Telemedia Act (*Telemediengesetz*, TMG) or based on terms and conditions with which the operators exclude themselves from the contractual relationship between the supplier and consumer. The platform operator generally also exempts himself from the obligation to permanently maintain the online structures without making any changes; an arbitrary block function to exclude users is not uncommon. Another matter which needs discussing is the consumer's intention to conclude the contract if he has not read the various conditions. It may also not be clear whether a supplier has the status of a consumer or that of an entrepreneur. This puts the onus not only on the consumer but also on the supplier, since the latter must be ready to bear the full thrust of sanctions imposed under consumer protection law if the supplier at some point acquires the status of enterprise.

Liability issues in the triangular relationship between the supplier, platform operator and consumer

Liability issues in the triangular relationship between the supplier, platform operator and consumer have also not yet been clarified. Is the platform operator to be co-responsible for fulfilling the supplier's obligations, at least as far as consumer protection obligations are concerned? Or is the platform operator even to be liable as a "second contracting party" where the consumer cannot hold the supplier liable?[83]

Even if one assumes that a contract of use has been concluded, then it is still doubtful whether the terms and conditions would stand up to monitoring. Criticism can, first, be raised of how the terms and conditions are presented (incorporation): The *browse wrap* method is often used, in which the terms are made available via an additional hypertext link. The *web wrap* method, by contrast, means that users have to find another link or the terms elsewhere on the platform's website. A summary study of British platforms identified the following types of liability limitation clauses:[84] Contractual liability and liability for criminal acts are frequently limited. Clauses which limit liability for computer failures, viruses and other technical problems are especially popular. Access clauses which permit platform operators to close down the platform at will or to deny consumers access at will are, likewise, not uncommon. Sometimes the terms and conditions will permit unilateral price changes. Arbitration clauses and exclusive jurisdiction agreements are widespread. In the case of liability these provisions will be to the consumer's detriment, since their effectiveness on many platform sites will be cast in doubt.

Competition: manipulated reviews

Many platforms use internal systems to rate products, services and the reliability of suppliers in order to increase trust in the service they provide. There have been attempts, on the one hand, to prevent platforms themselves manipulating these reviews. In 2012 the UK Advertising Standards Authority, for example, ruled that it was misleading for TripAdvisor to claim in its advertising that its travel reviews are written by "real travellers" although the platform operator does not monitor them.[85] According to the European Commission, the

---

Terms for the Use of the Apple App Store and the Google Play Store", (2016), *Journal of European Consumer and Market Law*, p. 10–15, p. 11.

[83] See Domurath, *Sachmängelhaftung in der Plattformökonomie,* SVRV Working Paper No. 3 as regards this issue.

[84] Riefa, *Consumer Protection and Online Auction Platforms – Towards a Safer Legal Framework* (Markets and the Law 2015), p. 125 et seqq.

[85] ASA Complaint Ref. A11-166867, 1 Feb. 2012, <https://www.asa.org.uk/Rulings/Adjudications/2012/2/TripAdvisor-LLC/SHP_ADJ_166867.aspx#.V586zK7Ix69> (last retrieved 20 Oct. 2016).

technique of "dimming" also breaches the Unfair Commercial Practices Directive.[86] A rating system may not paint an excessively positive picture of the supplier.[87]

On the other hand, there is now a proper market for manipulated online reviews. In an initiative launched in 2013 called Operation Clean Turf, New York Attorney General Eric Schneiderman identified a total of 19 enterprises specialising in fake reviews.[88] *Amazon* has already sued 1,000 users for posting fake reviews as well as several enterprises whose business models are based on fake reviews.[89]

One particular problem from the consumer's perspective is that it is hard to identify manipulated reviews. One possible remedy is Cornell University's Reviewskeptic,[90] an algorithm which unmasks fake hotel reviews, by its own account with a probability of 90%. No 22 of Annex I to the EU Unfair Commercial Practices Directive prohibits "falsely representing oneself as a customer" – which could represent the connecting factor for a ban on fake reviews.[91]

Competition: lack of transparency in search results lists

The lack of transparency in search results lists is also criticised by many. A search engine can act as a passive "conduit" (i.e. which only creates links between Internet users), as an "editor" (i.e. which, like a newspaper editor, decides what to show and what not to show) or as an "adviser" (i.e. whom users can trust in regard to the suggestions made).[92] Search engine optimisation exacerbates this problem.[93]

The blending of advertising and information and opaque results lists can mislead consumers.[94] Berlin Regional Court issued a decision much in this vein, ruling that popularity rankings on a hotel booking portal influenced by commission payments constitute impermissible misleading advertising.[95] The same must also apply to search engine results provided by other online portals. The blending of advertising and information impairs consumers' judgment. Even if competition law were able to remedy this issue, doubts would have to be raised as to how effectively rights can be enforced, since this is left to consumer protection agencies and to competitors, who are competent under the Act against Unfair Competition (*Gesetz gegen den unlauteren Wettbewerb*, UWG). This may no longer be sufficient given the platforms' increasing market power.

---

[86] Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, as at 25 May 2016, SWD(2016) 163 final, COM(2016) 320, p.136, <http://ec.europa.eu/justice/consumer-marketing/files/ucp_guidance_en.pdf> (last retrieved 20 Oct. 2016).

[87] Düsseldorf Higher Regional Court, judgment of 19 Feb. 2013 (case nos I-20 U 55/12, 20 U 55/12).

[88] They were made to pay fines of between US$ 2,500 and 100,000; <http://www.businessinsider.com/new-york-cracks-down-on-fake-yelp-reviews-2013-9?IR=T> (last retrieved 20 Oct. 2016).

[89] <https://www.theguardian.com/technology/2015/oct/18/amazon-sues-1000-fake-reviewers> (last retrieved 20 Oct. 2016).

[90] <http://reviewskeptic.com/> (last retrieved 20 Oct. 2016).

[91] Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, as at 25 May 2016, SWD(2016) 163 final, COM(2016) 320, p.140, <http://ec.europa.eu/justice/consumer-marketing/files/ucp_guidance_en.pdf> (last retrieved 20 Oct. 2016).

[92] See Grimmelmann, "Speech Engines", (2014), *93 Minnesota Law Review*, p. 868–952 for a more detailed analysis.

[93] See, e.g., Schirmbacher/Engelbrecht, "Suchmaschinenoptimierung und (un)zulässige SEO-Maßnahmen", (2015), *Computer und Recht*, Vol. 10, p. 659–664.

[94] The same conclusion is drawn by Scardamaglia/Daly, "Google, online search and consumer confusion in Australia, (2016), *24 International Journal of Law and Information Technology*, p. 203–228.

[95] Berlin Regional Court, order of 25 Aug. 2011 (file no. 16 O 418/11).

3. The example of health apps[96]

Like other apps, health apps use a three-pole system of actors in which the app creator, the app store and the consumer enter into legal relationships with each other. This creates various legal problems, especially as regards the contracting party, the effectiveness of terms and conditions, and liability issues. These will be discussed in the following by way of example.[97]

Uncertainty regarding the contracting party

What contractual relationships arise between the individual actors following the purchase of a health app? Generally speaking, official iOS and Windows app stores only sell apps for their own operating systems via their own official sales channels. On account of their market power, many suppliers create their apps for iOS and Windows; in consequence they are forced to accept the official app stores' sales terms. The following analysis focuses on the Apple App Store. The situation is similarly complex for other sales channels, such as Google Play, Microsoft Windows Phone Marketplace, BlackBerry App World and the *Amazon* App Store for Android.[98]

The conditions applicable in the relationship between Apple and the supplier of the app are set out in detail in the iOS Developer Program License Agreement ("iOS Agreement"). Under that Agreement, the law of Luxembourg applies.[99] In its relationship with the supplier of a chargeable app, Apple has the status of a "*commissaire*" under the law of Luxembourg, which is comparable to that of a German "commission agent" pursuant to section 383 et seqq. of the German Commercial Code (*Handelsgesetzbuch*, HGB) who acts in his own name for another's account.[100] In the case of free apps, Apple is the supplier's "legal agent". When it comes to sales to end consumers in Germany, Apple is therefore a "commissaire" under the law of Luxembourg.[101] From the supplier's perspective, the App Store is the consumer's contracting partner (distributer).

However, the contract between the App Store and the supplier (the iOS Agreement) conflicts with that between the App Store and the consumer (the iTunes terms). Consumers will probably feel that they are concluding a contract with the supplier. However, no reference is made anywhere to the fact that a contract is to be concluded with the supplier, which is why consumers can ultimately assume that they have only concluded a contract with the App Store.[102] In the end it is not clear who the contracting party is, which will, in turn, have consequences in the event of a liability case.

Unequivocal legal situation on account of the Apple App Store's terms and conditions

The legal uncertainties increase when one analyses the Apple App Store's Terms of Use.[103] They refer to German law,[104] which is why section 305 et seqq. of the German Civil Code is applicable.

---

[96] This section is based on Adam/Micklitz (op. cit., fn. 78).
[97] The following section is essentially based on Solmecke/Taeger/Feldmann (eds) *Mobile Apps, Rechtsfragen und rechtliche Rahmenbedingungen,* Solmecke/Taeger/Feldmann (eds), (De Gruyter Verlag, 2013), Chapter 3.
[98] See, as regards the other providers, Engelhardt in, *Mobile Apps, Rechtsfragen und rechtliche Rahmenbedingungen,* Solmecke/Taeger/Feldmann (eds), (De Gruyter Verlag, 2013), margin no. 177 et seqq. and 302 et seqq. re Chapter 3.
[99] <https://developer.apple.com/programs/terms/ios/standard/ios_program_standard_agreement_20140909.pdf>, see p. 47 (last retrieved 28 Nov. 2016).
[100] Engelhardt in (op. cit., fn. 98), margin no. 180 re Chapter 3.
[101] No. 7.1 of the iOS Agreement read in conjunction with Schedule 1, section 1 and Exhibit A re Schedule 1.
[102] See also Lachenmann in *Mobile Apps, Rechtsfragen und rechtliche Rahmenbedingungen,* Solmecke/Taeger/Feldmann (eds), (De Gruyter Verlag, 2013), margin no. 342 re Chapter 3.
[103] Lachenmann, (op. cit., fn. 102), margin no. 323 et seqq. re Chapter 3.

However, it is not, for instance, clear whether the terms regarding the downloading of individual apps are actually incorporated pursuant to section 305 of the German Civil Code or whether they represent a framework agreement within the meaning of section 305 (3) of that Code. Both options are inconclusive. On the one hand, the terms cannot apply to the purchase of individual apps because they are only shown to consumers once when they create an iTunes account for the Apple App Store. When purchasing individual apps they are neither shown again nor is reference made to them. If one assumes that each time an individual app is downloaded a new contract is concluded with the App Store, then the Terms of Use are not effectively incorporated for any of these individual contracts for the Apple App Store.[105] On the other hand, classifying the terms as a framework agreement which then applies to the purchase of each app is also inconclusive:[106] If that were the case, then Apple would have to make explicit reference to the Terms of Use and to the fact that these will apply each time an app is downloaded when a consumer opens an iTunes account. Taking the consumer's perspective, it can be assumed that merely creating "access" does not mean concluding a framework agreement for all subsequent app downloads. However, it is not only unclear that the Terms of Use are being incorporated and to which contract they are applicable (creating an iTunes account or downloading an app), the effectiveness of the terms themselves is also unclear (even if one assumes that they had been effectively incorporated). Two problems are striking here: the confusing nature of the Terms of Use and the limitations on liability.

What is clear is that the App Store's terms not only refer to the mobile App Store, but also to the iTunes Stores, the Mac App Store, the App Store for Apple TV, the iBook Store and the Apple Music Service. A document which, depending on its format, can run to around 20 pages contains terms and conditions for six different Apple services; paragraphs are not numbered. Various topics are intermingled and the document is extremely confusing.

4. Current state of the debate on a reform of platforms

The focus in the following will be on two reform proposals: First, France has submitted various bills to the European Commission in the notification procedure under Directive 2015/1535/EU[107] and the now amended Directive 98/34/EC.[108] Second, the Research Group on the Law of Digital Services (RG Digital Services) has published a Discussion Draft of a Directive on Online Intermediary Platforms.[109]

Information asymmetries

Articles 19 and 20 of the French Digital Republic Bill concern general information requirements incumbent on online portals. Accordingly, a platform[110]

> "*shall be obliged to provide trustworthy, clear and transparent information on the general terms and conditions of use for the intermediation service they provide*

---

likewise Loos, "Standard Terms for the Use of the Apple App Store and the Google Play Store", (2015), *Journal of European Consumer and Market Law*, p. 10–15.

[104] <http://www.apple.com/legal/internet-services/itunes/de/terms.html> (last retrieved 20 Oct. 2016), Section J "Anwendbares Recht".

[105] This is the conclusion drawn by Lachenmann in (op. cit., fn. 102), margin no. 318 re Chapter 3.

[106] Likewise in Lachenmann, (op. cit., fn. 102), margin no. 319. re Chapter 3.

[107] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) (OJ L 241, 17.9.2015, p.1).

[108] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations (OJ L 204, 21.7.1998, p. 37).

[109] Research Group on the Law of Digital Services, "Discussion Draft of a Directive on Online Intermediary Platforms", (2016), *Journal of European Consumer and Market Law*, p. 164–169.

[110] Notification Number 2015/626/F <http://ec.europa.eu/growth/tools-databases/tris/en/search/?trisaction=search.detail&year=2015&num=626> (last retrieved 20 Oct. 2016).

and on the arrangements for referencing, classifying and dereferencing content, goods or services to which this service provides access. They must clearly show whether there is a contractual relationship or capital links with those referenced, whether there is any compensation by those referenced and, where applicable, the impact of this on how content, goods or services offered are classified."

Article 21 of the Digital Republic Bill specifically concerns rating portals.[111] Under the provision, which is to be incorporated into the French Consumer Code,

> *"any person involved in the activity of collecting, moderating or distributing consumer opinions online, as the main party or an accessory, is obliged to issue truthful, clear and transparent information on the methods used to check the opinions posted online. They shall specify whether or not the opinions that they have posted online have been checked and, if they have, indicate the main characteristics of the checks performed."*

The Bill is to be given concrete form in a decree on information requirements specifically for comparison websites.[112] Under this draft, all comparison websites must specify in a directly and easily accessible dedicated section how the comparison service works. It must include the following information: (1) the different ranking criteria of offers of goods and services and their definition; (2) the existence or non-existence of a contractual relationship or capital links between the comparison site and the professionals listed; (3) the existence or non-existence of any payment to the site by the professionals listed and, where appropriate, the impact thereof on the ranking of offers; (4) details of the cost components and the possibility that additional charges will be added; (5) if applicable, the differences between the commercial guarantees of the products compared; (6) completeness or non-completeness of the offers for goods or services compared and the number of listed sites or businesses; (7) the updating time frame and method of offers compared. Information is also to be displayed on each comparison results page, namely the ranking criteria and, in particular, whether or not a fee is charged for the listing ("linking").

According to the expert evaluators, the European Commission contradicted the bills, but without publishing its opposing opinion. The Commission essentially criticised the fact that the Unfair Commercial Practices Directive and the E-Commerce Directive stood in the way of existing and fully harmonised legal frameworks. Irrespective of the issue of full harmonisation, which can be made out here, it is doubtful what purpose further information requirements could actually serve. The meaningfulness of information requirements has not been proven,[113] and it is doubtful whether the French Bill will have a sustainable impact on platform economics. It does, however, appear to make sense as regards identifying the contracting party.

A draft of a *Platform Directive* is also currently being discussed in the literature. The RG Digital Services is leading the way and has put forward a Draft Directive.[114] The Research Group proposes including certain disclosure requirements, in the same way as the French Bill does. The authors propose introducing information requirements in respect of details of the contractual relationships between the consumer, supplier and platform operator. The proposal leaves it open how that information is to be provided. One possible solution, in the

---

[111] Notification Number 2015/630/F, <http://ec.europa.eu/growth/tools-databases/tris/en/search/?trisaction=search.detail&year=2015&num=630> (last retrieved 20 Oct. 2016).
[112] Notification Number 2015/498/F, <http://ec.europa.eu/growth/tools-databases/tris/en/search/?trisaction=search.detail&year=2015&num=498> (last retrieved 20 Oct. 2016).
[113] Ben-Shahar/Schneider, *More than you wanted to know,* (Princeton University Press 2014).
[114] Busch/Schulte-Nölke/Wiewiórowska-Domagalska/Zoll, "The Rise of the Platform Economy: A New Challenge for EU Consumer Law?", (2016), *Journal of European Consumer and Market Law*, p. 3–10; Busch/Dannemann/Schulte-Nölke/Wieworowska-Domagalska/Zoll, "On the Law of Digital Services: Discussion Draft of a Directive on Online Intermediary Platforms", (2016), *Journal of European Consumer and Market Law*, p.164–169.

case of a platform with user accounts, would be that attention would have to be drawn to the information in a separate step when an account was being created, for example by means of pictogrammes or governmental rating systems.

Definition of "platform"

The French Bill proposes the following definition:

> *"Under the terms of this Article, online platforms are deemed to be activities consisting of classifying or referencing content, goods or services offered or uploaded by third parties, or of electronically connecting several parties with a view to selling goods or providing services (including free of charge), or exchanging or sharing goods or services. Persons exercising this activity in a professional capacity are qualified as online platforms."*[115]

Article 2 of the RG Digital Services' proposal contains the following definition, however:

> *"'online intermediary platform' means an information society service accessible through the Internet or by similar digital means which enables customers to conclude contracts with suppliers of goods, services or digital content. This does not include services which only identify relevant suppliers and which direct customers to those suppliers' websites or contact details."*[116]

The Research Group's suggestion thus has rather limited scope: the connecting factor is the platform as the place of conclusion of the contract. This means that ratings platforms would not fall under the scope of application of the legislation because the contract between the consumer and supplier is generally concluded in the real world. In the end, what is required is a very nuanced regulation applicable to a small number of platforms. In the light of Article 8 of the proposed directive that is regrettable, because this provision on rating systems could easily be applied to ratings platforms.

Liability issues

The problem of the liability of intermediaries is not new to the legal system. A medieval market place could be described as an intermediary which brought together supply and demand. Special rules apply for brokers and for intermediaries under travel law and in the case of financial services. Nevertheless, it appears appropriate to seek a separate solution for Internet portals. Unlike in their relationships with brokers, travel agents or credit intermediaries, consumers often do not pay a portal anything and do not even conclude a contract of use. Dealings on Internet platforms cannot be compared with a broad brush to agency business either since the context of platform economics is missing. Securities and insurance markets pose a much greater risk to consumers than the overwhelming majority of Internet platforms do.

The RG Digital Services' proposal for a directive addresses various liability options and duties to protect.[117] When it comes to the platform operator's own duties to protect consumers, Article 7 of the proposal suggests that the platform operator be obliged to immediately pass on all communication between the consumer and the supplier if it provides

---

[115] Article 19 of the French Digital Republic Bill, Notification Number 2015/626/F in the European Commission's Notification Procedure <http://ec.europa.eu/growth/tools-databases/tris/en/search/?trisaction=search.detail&year=2015&num=626> (last retrieved 20 Oct. 2016).

[116] Busch/Dannemann/Schulte-Nölke/Wieworowska-Domagalska/Zoll, "On the Law of Digital Services: Discussion Draft of a Directive on Online Intermediary Platforms", (2016), *Journal of European Consumer and Market Law*, p. 164–169.

[117] Busch/Schulte-Nölke/Wiewiórowska-Domagalska/Zoll, "The Rise of the Platform Economy: A New Challenge for EU Consumer Law?", (2016), *Journal of European Consumer and Market Law*, p. 3–10; Busch/Dannemann/Schulte-Nölke/Wieworowska-Domagalska/Zoll, "On the Law of Digital Services: Discussion Draft of a Directive on Online Intermediary Platforms", (2016), *Journal of European Consumer and Market Law*, p. 164–169.

a general system of communication on the platform. Under Article 7(2) of the proposal, when consumers have access to the platform operator they also have access to the supplier. That seems to make sense, since it ought not to be possible for the platform operator to thwart the supplier's information requirements. The platform operator's position of power is thus also appropriately limited. To protect platform users (both consumers and suppliers), Article 9 of the proposal requires that platform operators must intervene where the operator learns of any criminal behaviour or behaviour which interferes with users' physical integrity, privacy, property or liberty. That represents a generous extension of obligations compared to the E-Commerce Directive, which only concerns liability for information which is transmitted. The liability gap would thus have been closed.

Further, the proposal provides for a specific liability system for platform operators. The basic standard is set out in Article 16(1) of the proposal: Whoever only presents himself as an intermediary is not liable. Exceptions are listed in Articles 17 to 20. Under Article 18, the platform operator is jointly liable if the operator exercises special influence on the supplier. Article 19 lays down liability in the event of the platform operator making damaging, misleading statements about consumers, suppliers, the goods or services offered, and digital content. Article 20 brilliantly rounds off the liability system and demands liability for guarantees which the platform operator gives regarding the supplier/consumer or goods/services offered.

Outlook

Of what value are the liability rules contained in the Research Group's proposal? On the one hand, the proposed directive presents quite a balanced liability regime: It introduces no general responsibility on the part of the platform operator, but distinguishes between different cases. Article 14 could be sufficient as regards identifying suppliers on platforms.[118] Comparisons with travel law are obvious:[119] Article 13(1)(2) of the Package Travel Directive[120] provides for the possibility of the travel agent being liable for providing the contractually agreed package travel services. The proposals are reminiscent of the concept of linked contracts under section 358 et seqq. of the German Civil Code. In fact the contract concluded between a supplier and consumer is based on the platform operator providing the required virtual environment, whereby the platform operator becomes the indispensible intermediary.[121]

Instead of expanding the platform operators' own duties to protect as well as liability, one option would be to impose monitoring and control obligations. That way platform operators would not be elevated to the position of partner in liability but more to the rank of "contact person". To do that the system of exemptions applied in the E-Commerce Directive would have to be amended. One possibility – which the European Commission also addresses in its Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices[122] – would be to introduce an obligation to shape the platform's structures in such a way as to enable, or even force, them to conform to consumer protection

[118] See, in this context, Schröder/Bühlmann, "Übernahme der Anbieterkennzeichnung durch den Portalbetreiber – ein Modell für Deutschland?", (2012), *Computer und Recht*, Vol. 5, p. 318–324.
[119] Busch/Schulte-Nölke/Wiewiórowska-Domagalska/Zoll, "The Rise of the Platform Economy: A New Challenge for EU Consumer Law?", (2016), *Journal of European Consumer and Market Law*, p. 3–10, p. 8.
[120] Directive (EU) 2015/2302 of the European Parliament and of the Council of 25 November 2015 on package travel and linked travel arrangements.
[121] Please refer to Loos, "Standard Terms for the Use of the Apple App Store and the Google Play Store", (2016), *Journal of European Consumer and Market Law*, p. 10–15, p. 11, as regards this link between contracts and the application of the Unfair Commercial Practices Directive and the Consumer Law Directive.
[122] Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, as at 25 May 2016, SWD(2016) 163 final, COM(2016) 320, p.126 et seq., <http://ec.europa.eu/justice/consumer-marketing/files/ucp_guidance_en.pdf> (last retrieved 20 Oct. 2016).

law – Article 14 of the Research Group's proposal for a directive is thus to be endorsed. If a supplier is forced during the registration process to provide information under consumer protection law, then the platform can easily monitor compliance. If a platform is unlawful in terms of its structure, consumer organisations, which are responsible for enforcing rights, would have a direct point of contact. The platform operator would have fewer risks to contend with than in the case of the above-mentioned proposal for a real platform directive.

III. Consumer data protection

It is impossible to discuss the Internet of Things and the law of digital services without going into data protection law.[123] A Privacy Sweep by the Global Privacy Enforcement Network[124] in which 25 different data protection authorities investigated how enterprises communicate their privacy policies to consumers found "alarming" shortfalls for more than 300 Internet of Things devices. In particular, they did not provide consumers with sufficient information about how their personal information was collected and processed nor about their rights in this respect.

Data protection plays a key role on various levels in the context of the provision of digital services. Substantive law problems arise which are in part structurally similar to the contract law problems which arise in the context of digital services (e.g. the packaging of offers with data or the monitoring of terms in privacy notices). Problems specific to data protection law are primarily the erosion of the need for consent and guaranteed data protection in international data traffic. A discussion of the inconclusive level of protection in regard to transnational transactions leads into an explanation of the consequences of deterritorialisation in regard to digital consumer law (see IV. below.).

1. Prohibition of coupling

If consent to the processing of one's personal data is formulated as a binding condition for contract performance although the data processor does not actually need the data for that purpose, then the voluntariness of that consent pursuant to Article 7(4) and Recital 43 of the General Data Protection Regulation is called into question. Article 7(4) of the Regulation goes beyond section 28 (3b) of the Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG),[125] which only concerns the coupling of consent to address trading and advertising with the conclusion of a contract.

This means it is disputable whether the prohibition of coupling in fact prohibits "paying" with one's data.[126] It must be considered whether the protection of the general right of personality pursued in the Federal Data Protection Act by means of a prohibition subject to approval possibly permits data protection law and fair trading law to be treated differently (the latter being concerned with the misleading of market participants).[127]

2. Monitoring of terms and conditions in privacy notices

Privacy notices are subject to monitoring because they are generally presented to and accepted by consumers in a formulaic manner and consumers are often in a structurally weaker negotiating position. Where one party is in a weaker position, under data protection law the voluntariness of consent within the meaning of section 4 of the Federal Data

[123] This section is based on Schmechel, (op. cit., fn. 16) and Domurath/Kosyra, *Verbraucherdatenschutz im Internet der Dinge*, SVRV Working Paper Series No. 3.
[124] Information available on the website of the Irish Data Protection Commissioner: <https://www.dataprotection.ie/docs/23-9-2016-International-Privacy-Sweep-2016/i/1597.htm> (last retrieved 24 Nov. 2016).
[125] Kühling/Martini, "Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?", (2016), *Europäische Zeitschrift für Wirtschaftsrecht*, Vol. 12, p. 448–454, p. 451.
[126] For a critical analysis of the prohibition of coupling, see Schantz, "Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht", (2016), *Neue Juristische Wochenschrift*, Vol. 26, p. 1841–1847, p. 1845.
[127] See Domurath/Kosyra, (op. cit., fn. 123).

Protection Act is called into question. The prohibition of coupling means that low-level pressure is to be avoided. Pressure can also arise independently of any linking of access to digital services with the consumer's personal data, for example when a consumer has to act within a short timeframe.

The fact that privacy notices can be monitored under the law of general terms and conditions shows that some clauses could be ineffective pursuant to sections 307 and 308 of the German Civil Code as they, one-sidedly, oblige consumers to review and monitor amended clauses and place consumers at an inappropriate disadvantage because they are unaware that their data are being passed on to third parties.[128]

3. Personal nature of data and data protection by technology

In principle, the question here is to what extent digital service providers may collect personal data from consumers and to what rules that collection of data is subject. This is, in particular, relevant when consumers "pay" with their data for what is ostensibly a free service. Where service providers anonymise consumer data, the Federal Data Protection Act is no longer applicable. If the data are not anonymised, for example because they are pseudonymised or directly personal, the collection and processing of these data are subject to the provisions of the Federal Data Protection Act.

Of relevance here is the potential of technology models which can guarantee data protection in the Internet, both in regard to digital services and the Internet of Things in general, above all privacy by design, certification, data protection compliance in enterprises etc. "Privacy by design" refers to account being taken of the protection of the private sphere when designing a device or service which "invades the private sphere", in particular by means of built-in anonymisation methods. Alternatively, data are to be pseudonymised, which means that it is possible to trace the information back to a specific individual, for example to safeguard the interest in criminal prosecution. "Privacy by default" refers to basic technical or organisational settings aimed at effectively implementing data protection principles such as data minimisation and protecting the rights of data subjects. Both privacy by design and privacy by default have now been regulated in Article 25 of the General Data Protection Regulation. Generally speaking, it can be said that data protection by technical means is increasingly coming to the fore.

4. Consent through "business purposes"

One specific question which is raised in regard to digital services is that of the legitimacy of the data collection. Data collection and processing can be legitimised by means of consent pursuant to section 4 of the Federal Data Protection Act (Article 6(1)(a) of the General Data Protection Regulation) or section 28 of the Federal Data Protection Act (Article 6(1)(b) of the Regulation). Generally speaking, there is a danger that instead of choosing complicated solutions involving consent, enterprises will choose to expand data collection and processing via section 28 of the Federal Data Protection Act.[129] Proliferated use of section 28 of the Federal Data Protection Act could erode the need for consent and the principle of data economy. It is not known to what extent the purpose cited in the privacy notice is in actual fact one which is required for contract performance. No empirical studies on this issue are yet available.

5. International data transfers

Safeguarding the protection of data transferred abroad is a consumer policy imperative. Various initiatives are hitting legal obstacles. The Safe Harbor Agreement between the EU and the United States of America was declared void by the European Court of Justice in a decision which caused quite a sensation.[130] Its successor, the Privacy Shield, has already

[128] See Domurath/Kosyra, (op. cit., fn. 123), Section D. V.
[129] See also Wendehorst, (op. cit., fn. 21), p. 50–52.
[130] Case C-362/14, Maximilian Schrems v. Data Protection Officer, EU:C:2015:650.

come under criticism. On account of the numerous exceptions it contains it does not appear to provide an appropriate level of protection. The assumption that an appropriate level of protection is guaranteed when certification is voluntary risks coming to nothing. Data subjects have no effective means of enforcing their rights before the US courts. Another criticism which can be raised is that data protection authorities, including collective holders of rights, are excluded from arbitration.[131] Data protection specialists criticise the contractual alternative, the "Export/Import Contract Template", on which many enterprises (including Facebook) already base their international data transfers. The Irish Data Protection Authority is currently preparing a preliminary ruling procedure.[132]

IV. Deterritorialisation and the enforcement of rights

The enforcement of consumer rights rests on two well-established pillars and one which is still under construction. Individual redress forms the first pillar, collective redress, especially by consumer associations by way of a cease-and-desist order, the second. The third pillar, which is only beginning to take shape, is official redress; it is successively taking hold from the outside in, so to speak, from the European, transnational level down to the national, German level.

The digitalisation of the economy, society and the law not only draws attention to the shortcomings of substantive law, but above all to those in institutions, procedures and instruments available for cross-border legal redress. Legal redress itself, especially questions around collective redress, has been discussed not only in Germany, but across Europe and the world for the past 20 years. Germany is very cautiously feeling its way towards new forms of collective redress. Nevertheless, this report does not address the enforcement of rights as such, or its opportunities and risks. The focus here is very specifically on the digital economy and digital society, specifically the peculiarities arising in the face of digitalisation when it comes to enforcing rights.

1. Re the impact on consumer rights

G. Spindler/Ch. Thorun refer in a report they submitted to the registered society *Selbstregulierung Informationswirtschaft*[133] to the problems of legal redress as some of the key problems faced in the digital economy. Taking the micro perspective of legal relationships which consumers enter into in order to participate in the digital world, it appears that **the decisive problem** is the deterritorialisation of legal relationships and thus also the deterritorialisation of legal redress.

Although there are no valid empirical surveys which could undermine this assessment, an analysis of the available academic literature does appear to suggest that consumers are bowing to reality: participation coupled with trust and fatalism. If consumers want to participate in the digital world, they not only have to hand over their personal data, they also embark on transactions in the course of which they cannot see which enterprises they are dealing with, what exactly the subject matter of the legal relationship is, let alone where these enterprises are based and how they will be able to enforce their rights if the enterprise is based in the EU or elsewhere outside of Europe. In its recent case-law, especially that referring to a cross-border context, the European Court of Justice speaks of "the consumer's weak position vis-à-vis the seller or supplier, as regards in particular his level of

[131] As regards a criticism of the Privacy Shield, see the Article 29 Data Protection Working Party's (2016) Opinion 01/2016 on the EU–U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016, 16/EN, WP 238, p. 3, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf> (last retrieved 15 Nov. 2016).
[132] http://www.europe-v-facebook.org/PA_MCs.pdf (last retrieved 15 Nov. 2016).
[133] See <https://sriw.de/images/pdf/Spindler_Thorun-Eckpunkte_digitale_Ordnungspolitik_final.pdf > (last retrieved 28 Nov. 2016), since published as Spindler/Thorun, "Die Rolle der Ko-Regulierung in der Informationsgesellschaft: Handlungsempfehlung für eine digitale Ordnungspolitik", (2016), *MultiMedia und Recht-Beilage*, Vol. 1, p. 1–28.

knowledge".[134] The idea is still prevalent that consumers inform themselves about their rights. In our specific context, consumers could find out about an enterprise's terms and conditions.

Assuming that terms and conditions are even available in German and also assuming that consumers actually read them, then they would recently have been able to learn the following about *Amazon*:

> *"The law of Luxembourg applies, and the application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded."*

Following the ECJ's judgment in the *Amazon* case, clause 14 of the Conditions of Use and Sale now read as follows:

> *"These conditions are governed by and construed in accordance with the laws of the Grand Duchy of Luxembourg, and the application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. We both agree to submit to the non-exclusive jurisdiction of the courts of the district of Luxembourg City, which means that you may bring a claim to enforce your consumer protection rights in connection with these Conditions of Use in Luxembourg or in the EU country in which you live. The European Commission provides for an online dispute resolution platform, which you can access here: (...). If you would like to bring a matter to our attention, please contact us."*

By contrast, the jurisdiction clauses cited in Facebook's, Twitter's and Google's respective Terms of Service read as follows:

> Facebook:
>
> *"You will resolve any claim, cause of action or dispute (claim) you have with us arising out of or relating to this Statement or Facebook exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County, and you agree to submit to the personal jurisdiction of such courts for the purpose of litigating all such claims. The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions."*
>
> Twitter*:*
>
> *"These Terms are an agreement between you and Twitter International Company, an Irish company with registered office at The Academy, 42 Pearse Street, Dublin 2, Ireland. If you have any questions about these Terms, please contact us."*
>
> Google:
>
> *"These Terms and any disputes resulting from or in connection with them are subject to German law, excluding the United Nations Convention of Contracts for the International Sale of Goods. This choice of law is of no consequence as regards the law which is applicable to the respective service. If you are a consumer, then statutory provisions apply for all disputes resulting from or in connection with these Terms. If you are not a consumer, the exclusive place of jurisdiction for all disputes resulting from or in connection with these Terms is Hamburg."*

How meaningful is any of the above? The *Amazon* case will serve for a discussion of the problems involved. German customers of *Amazon, Facebook* and *Twitter* learn that it is not German law, but the law of Luxembourg, California or Ireland which applies. That may be

[134] Case C-191/15, Verein für Konsumenteninformation v. Amazon EU Sàrl, EU:C:2016:612; Case C-26/13, Árpád Kásler, Hajnalka Káslerné Rábai v.OTP Jelzálogbank Zrt, EU:C:2015:262.

disconcerting, because it is not German law. Nevertheless, *P. Rott*[135] asks, slightly ironically, in a discussion of the ECJ's judgment whether consumers would be better informed if reference were made to German law, as is the case in Google's Terms. The fact that the United Nations Convention of Contracts for the International Sale of Goods does not apply will mean very little to most consumers. In times in which behavioural research is all the rage, it would be very interesting to investigate what associations, hopes or fears a choice of law clause triggers. The Member States and the EU are working on the political level to convince consumers that the (as yet) 28 Member State legal systems are all equal. Consumers are to feel just as protected by the law of Luxembourg than by German law. Choosing German law may, therefore, have a calming effect, at any rate more calming than when consumers choose the law of Luxembourg. But what if US or Indian law were to apply and not the law of Luxembourg?

Another interesting question from the consumer perspective would be whether, after choosing a legal system, they could waive their right to legal redress and, if so, how this ex-ante waiver would influence the subject matter and volume of Internet transactions. Or put another way: Are consumers prepared, when German law applies, to order more and more valuable goods or services?

In legal reality, the average consumer will not bother asking these sorts of questions. Obstacles in consumers' path are "clicked away" so they can achieve their objective. Naturally, that sort of behaviour is highly rational. If consumers first had to find out about all the possible consequences, the time and effort they would have to invest would be much greater than the possible risk were difficulties to arise in the processing of an order. Waiving the right to legal redress is a necessary but also logical consequence. And all the more so since in countless cases transactions proceed smoothly.

Despite all the trust consumers place in that enterprises behaving properly, together with a dash of fatalism, they are still left with a certain sense of unease. That takes on concrete shape where the potential risk exceeds a certain attention threshold, either on account of the nature of the problem (unsafe children's toys) or on account of its prevalence (powerlessness in the face of transnationals' privacy policies). How else would the case of *Schrems v. Data Protection Officer*[136] have become so well-known across the world? This unease lies dormant and rises to the surface when an event reaches citizens at least on an emotional level. In that case, those organisations involved in enforcing consumer rights very quickly come into focus, as does the more or less overtly raised question of whether these organisations are doing enough to safeguard consumer rights beyond national boundaries, whether they are helping consumers to assert their rights or whether they are protecting them against possible damage through preventative monitoring. It is logical to assume that consumers, were they to be asked, would tend to be critical, above all if they were surveyed after a large-scale consumer policy incident.

That is not to say that policy-makers in Germany and in the EU have not reacted in any way. In the course of integrating EU markets, policy-makers have responded by developing a whole arsenal of legal instruments which have one thing in common: They put the onus on the individual. Consumers are to assert their rights themselves, even beyond national borders. In cross-border legal disputes within the EU consumers are guaranteed that Germany is their place of jurisdiction, but not that German law will be applicable. The question is whether previous legal policy has achieved those goals it set out to achieve and whether the opportunities and possibilities available have actually improved. There is room for doubt, even though no robust data are yet available. That is the only explanation for why the EU is massively expanding individual legal redress below the court level and why it wants cross-border collective redress to be placed on a completely new footing.

[135] Rott, "Das IPR der Verbraucherverbandsklage", (2016), *Europäische Zeitschrift für Wirtschaftsrecht,* Vol. 19, p. 733–736, p. 733.
[136] Case C-362/14, Maximilian Schrems v. Data Protection Officer, EU:C:2015:650.

2. Individual legal redress

The shift away from courts to all sorts of different forms of alternative dispute resolution is nothing new. It is inherent to consumer law and, ultimately, a result of the objective that these forums are to make it easier and simpler for consumers to enforce their rights. However, this development has further accelerated with the rise of the digital economy.

Online trading as a whole, regardless of the type of product or service offered, is permeated by voluntary dispute resolution on various levels, by associations in the relevant sector and arbitration and conciliation bodies.[137] Ombudspeople have gained great significance for financial service providers. The entry into force on 1 April 2016 of the Consumer Dispute Resolution Act (*Verbraucherstreitbeilegungsgesetz*, VBSG) places what was up until then an extremely heterogeneous and complex system of voluntary dispute resolution in Germany on a uniform footing. The Federal Office of Justice has since published a list of recognised bodies.[138] This was occasioned by two EU legislative acts: the Online Dispute Resolution (ODR) Regulation and the Alternative Dispute Resolution (ADR) Directive.[139]

The basic idea is that all forms of dispute resolution are covered, both private and public, though excluding pure customer complaints bodies and other dispute resolution facilities run or funded only by a single enterprise or by associated enterprises, or active only on behalf of such enterprises or associated enterprises (section 1 (2) of the Consumer Dispute Resolution Act). The key question will be which of the diverse online trading mechanisms are covered by the exemption or whether operators, even if they could rely on the exemption, decide to upgrade or restructure. The entire system is in flux, and it will be interesting to see which path those involved will choose to take. It is not yet clear what will happen to conciliation offices recognised by Germany's *Land* departments of justice.[140]

The ODR platform is to become a first point of contact. Parties will propose various dispute resolution agencies or a complaint will be passed straight on to such an agency if the parties have previously reached agreement. The Member States will designate points of contact which are to notify the parties of which agency has been chosen. The whole of the subsequent procedure will be carried out online via the platform. Theoretically, this will result in new types of Europe-wide dispute resolution mechanisms which go well beyond the objective set out in the ODR Regulation. The provisions have been implemented in sections 38 to 40 of the Consumer Dispute Resolution Act: Section 38 of the Act regulates cooperation between the consumer conciliation board and those institutions which are responsible for the out-of-court resolution of comparable disputes, in the implementation of the Directive in another Member State of the EU or EEA. Section 39 designates the consumer dispute resolution body responsible in its capacity as point of contact for cooperation in online disputes. Under section 40, the Federal Ministry of Justice and Consumer Protection assumes the obligation under EU law to support consumers in enforcing their rights. The Ministry can delegate this task to "a legal person under private law, a partnership with legal capacity or another suitable body". Responsibility for professional and legal oversight remains with the Ministry.

The flesh still needs to be added to the bare bones of these provisions. It will remain to be seen whether, in doing so, it will be possible to ensure that consumers in the EU and the EEA actually use the platform to resolve disputes without taking recourse to the courts.

---

[137] See the references included in Adam/Micklitz, (op. cit., fn. 78).

[138] As at 31 Aug. 2016 <https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Verbraucherschutz/Liste_Verbraucherschlichtungsstellen.pdf?__blob=publicationFile&v=15> (last retrieved 28 Nov. 2016).

[139] Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR) (OJ L 165, 18.6.2013, p.1).

[140] See Micklitz, "Brauchen Konsumenten und Unternehmen eine neue Architektur des Verbraucherrechts?", (2012), *Neue Juristische Wochenschrift, Beilage*, Vol. 3, p. 77–81, p. 77 et seq.

However, digitalisation opens up new paths for enforcing rights which are reflected neither in EU law nor in German law. One such example is the enforcement of passenger rights with the help of commercial intermediaries who assert a consumer's rights against payment of a percentage share.[141] Several such providers exist.[142] They generally only take on clear-cut cases. It is undeniable that they help many consumers to enforce their rights in cases where those consumers would probably not have taken on the matter themselves. That is why the success rate is so high and is relied on so heavily in advertising. The provider Flightright, for instance, only files claims for damages for flight delays under the corresponding Flight Compensation Regulation (EC) No 261/2004.[143] Consumers are left to deal with the more risky cases themselves, though. They have to seek out a consumer advice centre or get a lawyer on the case. Such models are also conceivable in regard to either incorrect advice or incorrect information on a massive scale. Unequivocal legislative standards would, however, be needed which clearly define the preconditions for a claim for damages and leave no doubt as to calculating the amount of the damage. The EU legislature only laid down lump sums in the Flight Compensation Regulation.

3. Cross-border collective redress

The increase in cross-border trade was fostering the deterritorialisation of consumer problems long before the questions raised by the spread of digital technology were moved to the top of the political agenda. The focus has been on advertising practices and terms and conditions. The Member States have left it to the EU to develop uniform substantive standards, either minimum standards in the case of terms and conditions or maximum standards in the case of commercial practices. By creating the cease-and-desist order the EU set up a procedural "minimum standard under EU law" in parallel to substantive law.[144] In accordance with the provisions of secondary EU law, each Member State is obliged to nominate a body having legal standing, either a consumer association and/or a consumer authority. Directive 98/27/EC (now Directive 2009/22/EC) raised legal redress by associations to the European level. It required the reciprocal recognition of legal standing, but left the Member States to delineate the legal interest in bringing proceedings. In the 1990s the European Commission still had high hopes for consumer associations as civil society players. Taking the number of actions brought as a benchmark, the number of cross-border suits has remained low in the EU. One exception is where neighbouring states speak the same language, as in the case of Belgium and France or Germany and Austria.

The scientific effort involved in analysing the complex legal issues involved bears no relation to their practical relevance. Digitalisation has done nothing to change that either. Consumer associations file actions against unfair terms and conditions or unfair and misleading market practices by those enterprises which are felt to be the digital market leader in a particular country, despite the fact that substantive law is largely harmonised and despite the ability to initiate cross-border proceedings which enable associations to protect their consumers against legal violations committed in another EU Member State. One practical reason may be that today's digital world is dictated by US corporations, which tend not to set up branches in every EU Member State. Jurisdiction clauses, arbitration clauses and choice-of-law agreements are problematical from the consumer perspective. Ryanair has opened up a new round in the debate because it now prohibits customers from assigning their rights under the

[141] See Rott, "Claims Management Services: An Alternative to ADR?", (2016), *European Review of Private Law,* p.143–160.
[142] For instance <https://www.claimflights.de/impressum> or <http://www.flightright.de/?pk_campaign=aw-brand&date=250815a&g> (both last retrieved 20 Oct. 2016).
[143] Regulation (EC) No 261/2004 of the European Parliament and of the Council of 11 February 2004 establishing common rules on compensation and assistance to passengers in the event of denied boarding and of cancellation or long delay of flights, and repealing Regulation (EEC) No 295/91 (OJ L 46, 17.2.2004, p. 1).
[144] Reich/Micklitz, *Europäisches Verbraucherrecht*, (4th ed., 2003, Nomos Verlag), § 30.11.

Flight Compensation Regulation to private companies which claim consumers' entitlements to Europe-wide compensation of up to 600 euros against payment of a fixed percentage share. The details of these extremely complex issues and their relevance for consumers in Germany will be discussed in the following based on *Amazon*'s choice of law clause, which came to the attention of the Austrian consumer association.

Internationally active companies need to decide whether they can get consumers in the EU to "choose" the law of the enterprise's place of business via the terms and conditions and not by entering into individual agreements. In terms of the conflict of laws, enterprises need to find those Member States in which the choice of law made in the terms and conditions is permitted under the provisions of Article 3(5) of Rome I (Regulation (EC) No 593/2008 of 17 June 2008). To our knowledge there is no Member State which prohibits the choice of law per se. That would mean that, for all consumers in the EU, legal protection would initially be focused on an enterprise's home state. The home state would thus be required to put in place substantive protection in the form of minimum standards applicable to that enterprise across the whole of the EU. Whether consumers in Member States other than the enterprise's home state can continue to retain the protection provided by their home country legal system will depend on the favourability principle set out in Article 6(2) of Rome I. The Member States' 28 legal systems would have to be compared on a substantive law level and implicitly or explicitly evaluated. The Member States as well as the European Commission have so far avoided undertaking such a "qualitative" comparison. Which legal system is the "best"? What criteria will make a legal system "better" in regard to minimum harmonisation and full harmonisation? *Who* is to compare each of the legal systems with the other 27? These are legally complex and politically sensitive issues which very quickly reveal the limits of what is feasible.

But more is at stake. Procedurally speaking, by permitting the choice of law to be defined in the terms and conditions, an enterprise's home state is saddled with implementing minimum standards under EU law for consumers across the whole of the EU. In a federal state such as Germany, this consequence is laid down in the constitution. This may or may not be desirable within the EU. Unlike substantive law, the favourability principle does not apply to procedural law. The EU's legal system and the European Court of Justice assume that procedural rules are on principle equal. This principle has run right through the ECJ's case-law since the Brussels Agreement entered into force in 1980. The ECJ's power of interpretation as regards the conflict of laws (Rome I and Rome II, prior to that the Rome Convention of 19 June 1980, effective since 1 April 1991)[145] is more recent. The limits to national autonomy when it comes to shaping the procedure result from the principle of equivalence and effectiveness.[146]

But what if it were to emerge that one Member State had to carry the full burden of legal protection for all EU consumers? Would the other Member States have to fund that Member State's body with legal standing? Would consumer organisations have to cooperate across borders? Would they have to, and could they if they had to? Would there be any obligation under EU law to cooperate loyally well beyond the context of Regulation 2006/2004? What about where, due to under-funding, legal redress is made "significantly more difficult" or "virtually impossible", for example in Germany (terms applied in the ECJ's case-law since 1976)[147] because the body only exists on paper? Would subsidiary national jurisdiction in the consumer's home country then apply? And how would that kind of factual situation, which does not appear so far-fetched given the realities of consumer procedural law in Europe,[148] fit

[145] References in Reich et al., *European Consumer L*aw, (2nd ed., 2014, Intersentia Verlag), §§ 7.2–7.17.
[146] See, most recently, Case C-497/13, Faber v. Autobedrij Hazet Ochten. EU:C:2015:357.
[147] See Reich, *General Principles of EU Civil Law*, (Intersentia Verlag, 2013), § 4.3.
[148] See, regarding the problems associated with legal redress, the Consumer Justice Enforcement Forum II's report of May 2016, <http://www.beuc.eu/publications/beuc-x-2016-051_cojef_ii-enforcement_of_consumer_rights.pdf> (last retrieved 28 Nov. 2016).

with the European Court of Human Rights' case-law? Could, should and would consumer associations have to file actions in Strasbourg, arguing that they were unable to assert their right to a hearing in accordance with the law?

In the cross-border context the legal situation in regard to the right to representative action gets even more complex because there may be a discrepancy between procedural and substantive law, at any rate when the right to representative action is subjected to the logic of the conflict of laws, which Article 1(2) of Directive 98/27/EC (Article 2(2) of Directive 2009/22) appears to do. Where conflict-of-law rules lead back to the enterprise's home state, the association bringing the action has to examine whether the substantive requirements in the chosen law on monitoring terms and conditions deviate from the home country's law to the consumer's detriment. Apart from the purely practical difficulty, who will take on this task? An association based in the consumer's home country or a court based in the home country? Or an expert commissioned by the association or the court, who will be paid by whom? The question is to what extent national bodies with legal standing are being "put off" such an interpretation of conflict-of-law rules when it comes to enforcing rights. The fatal consequence as regards legal redress would, in the extreme case, be that the association which is in principle competent and authorised does not file an action because it feels that proceedings in the home country, as defined under another EU Member State's law, are too time-consuming and expensive and the association in the enterprise's home state, which also has legal standing, does not act because it lacks the incentive and resources to want to enforce consumer rights across the whole of the EU. Legal protection would in practice only be provided where the applicable law was the domestic law of the association with legal standing.

In its *Amazon* ruling the European Court of Justice did not prohibit choice of law clauses but linked their permissibility to the condition that entrepreneurs must notify consumers in their terms and conditions of the fact that they retain what may possibly be a greater level of legal protection in their home country even if another EU Member State's legal system has been chosen. In this ruling the ECJ offered consumer associations and consumers stones not bread. Consumer associations are invited to initiate more proceedings in order to find out how far the enterprises' disclosure requirement goes. The Advocate General answered the extremely delicate question of whether entrepreneurs are now required to compare 28 legal systems and to inform consumers in a targeted manner in the negative; the ECJ, however, left the question open. It seems hard to believe that the ECJ is saddling enterprises with this burden. That would mean that the reference to the fact that better rights continue to exist in the home country only needs to be phrased quite generally. Consumers will then find a reference in the terms and conditions which means very little or nothing at all to them. It would then be better if they were to read that they are better off in EU Member State X than in EU Member State Y. The parallelism between the right of representative action against terms and conditions and individual proceedings, which the ECJ announced with so much verve, results in consumers being left to their own devices when it comes to enforcing their rights. The only thing which would help consumers would be if they were given a clear, uniform solution which they could then work with. What we are left with is a not insignificant amount of legal uncertainty as regards the extent of information which needs to be included in terms and conditions and as regards the relevance of the favourability principle in individual redress proceedings.

Digitalisation permits the exact opposite, namely collective redress of consumer rights to be more efficiently organised, specifically when it comes to registering claims, the possibility of standardisation and information collection. That presupposes that consumers have the required access and digital skills to be able to enforce their rights and that institutions have digital skills and digital infrastructure at their disposal. Dovetailing the existing legal world with the digital world is a structural imperative. This development is still in its infancy, especially since the legislature has still not created the preconditions for collective redress. The only possible option would be to use digital technology to open up the option of class actions.

4. Cross-border cooperation between authorities

At the turn of the millennium a hiatus in European consumer policy left deep marks in EU statutory law. Since the Lisbon Summit in 2000, EU consumer law and consumer policy have been under the aegis of economic efficiency. The outward sign of this is the swing from minimum to full harmonisation effected in Directive 2005/29/EC, which, against resistance from Germany, created a special rule for consumer-oriented advertising. Neglecting to include associations' right of collective action in the restructured European international private law in Rome I and Rome II is further evidence. The fact that no political decision was taken on where to place collective redress within the overall system meant that in the *Amazon* case the ECJ had to make a decision which was of wide-ranging relevance when it comes to determining responsibilities for the monitoring of terms and conditions in the Single Market.[149]

Viewed in retrospect, however, another document is of much greater relevance as regards the increasingly powerful trend within the EU towards consumer protection by authorities, and that is Regulation 2006/2004 on cross-border cooperation in consumer protection. The Regulation obliges Member States and thus also Germany to nominate a government institution which bears lead responsibility for this cooperation. In Germany, cross-border cooperation is coordinated by the Federal Ministry of Justice and Consumer Protection, which acts in the capacity of central liaison office. The Ministry generally passes the requests for administrative assistance it receives from other countries to other agencies within Germany for review. Where applicable, these issue a warning or file a legal action. In addition to the Ministry, the Federal Aviation Office, the Federal Finance Supervisory Authority, the Federal Railway Authority and various federal state authorities are involved. Germany invested a great deal of energy in these negotiations to ensure that consumer associations (and the Central Office for the Prevention of Unfair Competition) are likewise involved. These bodies are primarily commissioned by the Federal Ministry of Justice and Consumer Protection where actions are to be brought against German enterprises in the interests of consumers in other EU Member States.

However one wishes to rate this cooperation, it marks a turning point. Germany and Austria are the only Member States which have no governmental authority responsible for monitoring abusive terms and conditions and unfair advertising but where these matters are decided in the courts.

There is little in the way of concrete details concerning the practical relevance of this procedure, which was introduced 10 years ago.[150] The network has no doubt fostered cross-border information sharing and thus also the ability to identify those consumer issues which are of cross-border relevance. Regulation 2006/2004 has not led to any more legal actions being brought than before, although that was a theoretical possibility. It is, likewise, not known what concrete successes the Regulation has achieved in helping consumers to enforce their rights. Following an evaluation of the previous Regulation, the European Commission on 25 May 2016 proposed fundamentally expanding the competencies of those authorities responsible for cross-border cooperation.[151] The Proposal, whose future is

[149] See Micklitz/Reich, "Das IPR der Verbraucherverbandsklage gegen missbräuchliche AGB", (2015), *Europäisches Wirtschafts- und Steuerrecht*, Vol. 4, p. 181–193; this is a report commissioned by the Association for Consumer Information (VKI) which was included in the proceedings. While Advocate General Saugmandsgaard shares our legal opinion, in Case C-191/15 VKI v. Amazon, EU:C:2016:388 the ECJ saddles consumers and national courts with the task of finding out whether, in an individual case, national law provides greater protection than that "chosen" in the terms and conditions.

[150] Rott, *Rechtsvergleichende Aspekte der behördlichen Durchsetzung von Verbraucherschutz*, Report submitted to the Federal Ministry of Justice and Consumer Protection, file no. V B1-7008-3-3-52 24/2016.

[151] COM(2016), 283 final. Proposal for a Regulation of the European Parliament and of the Council on cooperation between national authorities responsible for the enforcement of consumer protection laws, <https://ec.europa.eu/transparency/regdoc/rep/1/2016/DE/1-2016-283-DE-F1-1.PDF> (last retrieved 28 Nov. 2016).

uncertain, would strengthen official redress, especially in regard to instruments required to assert rights which are now for the first time to include a rule on compensation. Authorities would be given the possibility, within the scope of the Regulation, of also compensating consumers' collective damages. The Proposal focuses in particular on the digital economy. The relevant passages in this context are highlighted in the following.[152]

> *Article 8*
> **Minimum powers of competent authorities**
> 1. Each competent authority shall have the investigation and enforcement powers necessary for the application of this Regulation and shall exercise them in accordance with this Regulation and national law.
> 2. Each competent authority shall have at least the following powers and exercise them under the conditions set out in Article 9, to:
>
> (a) have access to any relevant document, data or information related to an infringement under this Regulation, in any form or format and **irrespective of the medium on which or the place where they are stored**;
>
> (b) require the supply by any natural or legal person, including banks, internet service providers, domain registries and registrars and hosting service providers of any relevant information, data or document in any format or form and **irrespective of the medium** on which or the place where they are stored, for the purpose of among others identifying and following financial and data flows, or of ascertaining the identity of persons involved in financial and data flows, bank account information and ownership of websites;
>
> (c) require any public authority, body or agency within the Member State of the competent authority to supply any relevant information, data or document in any format or form and **irrespective of the medium** on which or the place where they are stored, for the purpose among others, of identifying and following of financial and data flows, or of ascertaining the identity of persons involved in financial and data flows, bank account information and ownership of websites;
>
> (d) carry out the necessary on-site inspections, including in particular the power to enter any premises, land or means of transport or to request other authorities to do so in order to examine, seize, take or obtain copies of information, data or documents, **irrespective of the medium** on which they are stored; to seal any premises or information, data or documents for a necessary period and to the extent necessary for the inspection; to request any representative or member of the staff of the trader concerned to give explanations on facts, information or documents relating to the subject matter of the inspection and to record the answers;
>
> (e) purchase goods or services as test purchases in order to detect infringements under this Regulation and obtain evidence;
>
> (f) purchase goods or services under a cover identity in order to detect infringements and to obtain evidence;
>
> (g) adopt interim measures to prevent the risk of serious and irreparable harm to consumers, **in particular the suspension of a website, domain or a similar digital site**, service or account;
>
> (h) start investigations or procedures to bring about the cessation or prohibition of intra-Union infringements or widespread infringements of its own initiative and where appropriate to publish information about this;

[152] Article 8, p. 30, COM(2016), 283 final. Proposal for a Regulation of the European Parliament and of the Council on cooperation between national authorities responsible for the enforcement of consumer protection laws, <https://ec.europa.eu/transparency/regdoc/rep/1/2016/DE/1-2016-283-DE-F1-1.PDF> (last retrieved 28 Nov. 2016).

(i) obtain a commitment from the trader responsible for the intra-Union infringement or widespread infringement to cease the infringement and **where appropriate to compensate consumers for the harm caused**;
(j) request in writing the cessation of the infringement by the trader;
(k) bring about the cessation or the prohibition of the infringement;
(l) close down **a website, domain or similar digital site**, service or account or a part of it, including by requesting a third party or other public authority to implement such measures;
(m) impose penalties, including fines and penalty payments, for intra-Union infringements and widespread infringements and for the failure to comply with any decision, order, interim measure, commitment or other measure adopted pursuant to this Regulation;
(n) **order the trader responsible for the intra-Union infringement or widespread infringement to compensate consumers that have suffered harm as a consequence of the infringement including, among others, monetary compensation, offering consumers the option to terminate the contract or other measures ensuring redress to consumers who have been harmed as a result of the infringement**;
(o) **order the restitution of profits obtained as a result of infringements, including an order that those profits are paid to the public purse or to a beneficiary designated by the competent authority or under national legislation**;
(p) publish any final decisions, interim measures or orders, including the publication of the identity of the trader responsible for the intra-Union infringement or widespread infringement;
(q) consult **consumers, consumer organisations**, designated bodies and other persons concerned about the effectiveness of the proposed commitments **in ceasing the infringement and removing the harm caused by it**.

The fate of the Proposal is not yet known. The fact remains that, should it ever be implemented in this or a similar form, it would perhaps for the first time provide the opportunity to adequately respond to the deterritorialisation of consumer problems in the digital world and to create a European equivalent to the US class action.

V. Potential solutions as regards the law of digital services

Any potential solution must above all be geared to maintaining consumers' autonomy in the digital world – during the contract negotiation phase, when a contract is being concluded, throughout the often long contract term as well as after the contract has been terminated. What is needed is a holistic approach which is not concerned with thinking inside legal boxes, but where sensible solutions are sought to real problems. It is clear that in such an analysis there will be a certain amount of intermixing of private law and public law, of substantive law (data protection law, the law of terms and conditions, fair trading law and consumer contract law) with procedural law (individual and collective redress at national and international level).

A survey of the current situation reveals a number of serious problems which existing legislation cannot solve. Consumers face completely new forms of distribution. Suppliers link the sale of a product to the software needed to use it. These package offers (see no. 2 below) impede competition, that is if it is to be possible or desirable for suppliers to compete for the different parts. Transparency as regards the costs of such package offers is not required. Access is linked to the disclosure of personal data, which can only be processed with consumers' consent. Consumers generally give their consent, regardless of the content and extent of the legal requirements, which have increased on account of the General Data Protection Regulation. The scope, extent and reach of such consent are not generally obvious and even if they are made transparent, they are hard to grasp in terms of their dimensions (see no. 3 below). Seventy-five years ago, it was believed that a review of

incorporation of terms would be enough to get a grip on terms and conditions, which were getting out of hand at the time.[153] Considering the increased requirements being made of consent to data processing, history is now repeating itself.

Once consumers have paid for access to the Internet and digital services with their data, question after question arises regarding the legal relationships they have entered into (see no. 1 below). Is there even a legal relationship? If so, of what kind? Is it a contract or a legal relationship sui generis? In the case of online business, who is the contracting party (see no. 4 below)? Where is the contracting party domiciled? What is the subject matter of the contract (see no. 5 below) if it is not the transfer of ownership but only the use of a right?[154] What options are there for getting out of a contract once it has been concluded, given that it may have a ten-year term? Is it technically possible to extract the consumer's data from the database of those enterprises which are processing these data? What rights does the consumer have vis-à-vis whom (see no. 6 below) when something goes wrong? Against the seller/supplier, who is often domiciled in another European country? How can those rights be asserted before a German court with the help of dispute resolution forums? Who is controlling whether everything is above board in this digital world?

The model laid down in law provides that consumer associations are meant to handle those cases which consumers cannot manage themselves or by means of individual redress mechanisms (see no. 7 and no. 8 below). Consumer associations are supposed to be in charge of monitoring market practices and terms and conditions across all enterprises (and borders). They not only need the know-how to be able to apply legal provisions, but also to understand and categorise the technical processes which are behind the law of digital services. This policy approach is not flanked by a class action which the consumer associations or individual consumers or lawyers acting on behalf of consumers could use to file for compensation when things go wrong. The most important and most widespread means of collective redress is a cease-and desist-order, a stop-order mechanism which is limited to banning illegal practices ex nunc, but which again leaves it, cum grano salis, to each individual consumer to know how and whether they are going to claim damages from an entrepreneur who is acting illegally. The cautious approaches to safeguarding collective consumer interests by administrative means adopted by the Federal Financial Supervisory Authority and the Federal Network Agency and in cross-border matters by official EU and OECD networks may signal that a paradigm shift is underway. Currently, though, no suitable complement to private-law consumer protection is available to consumer authorities with general competencies, especially when it comes to compensating affected consumers.[155]

The Advisory Council feels there is an urgent need to adapt existing rules to the challenges of the digital world. Taking the holistic perspective – from establishing a legal relationship to leaving a digital legal relationship – the Advisory Council proposes the following 11 measures which cover four different types of digital legal relationship.[156] These measures are based on

[153] That is the solution Italy chose in 1942 when it undertook a major reform of its *Codice Civile*.
[154] Wendehorst (op. cit., fn. 21).
[155] For information on the activities of the Consumer Protection Cooperation (CPC) network and the International Consumer Protection and Enforcement Network (ICPEN), see http://ec.europa.eu/internal_market/scoreboard/performance_by_governance_tool/consumer_protection_cooperation_network/index_en.htm and http://www.bmjv.de/DE/Verbraucherportal/Verbraucherinformation/ICPEN/ICPEN_node.html, (both last retrieved 24 Nov. 2016). The networks mainly collate information (e.g. by means of "sweeps") and attempt to solve problems through direct negotiations with enterprises.
[156] (1) Free digital services; (2) the role and function of online platforms in providing information, advice and mediation; (3) the deterritorialisation of consumption (consumers often do not know where the enterprise is domiciled; if it is domiciled abroad a complicated set of legal building blocks is available which has a great deal to offer legal science but very little to offer consumers); (4) the Internet of Things.

the principle of legal clarity and legal certainty for consumers, a sufficient but also necessary condition for maintaining the autonomy of consumers.[157]

The following list includes only those *key* demands which we feel need to be *urgently* actioned. It also includes policy-advisory considerations regarding implementation of the recommendations (see nos 9 to 11). The reasons as well as further details can be found in the relevant parts of this report, the third-party report commissioned by the Advisory Council and in the working papers to which reference is made.

1. Re information provided before establishing a legal relationship

Before establishing a legal relationship consumers are inundated with a wealth of information. Numerous statutory information and disclosure requirements are supposed to ensure that consumers become aware of the consequences under data protection law, that they are familiarised with the subject matter of the contract and all the contractual rights and obligations under the terms and conditions, and that they realise the extent and scope of the end-user agreement. The Advisory Council feels that the rules on information provision need to be more clearly structured, they need to be reduced in number where possible and compliance ensured by means of sanctioning mechanisms.

Regulation (EU) No 1286/2014 of the European Parliament and of the Council of 26 November 2014 on key information documents for packaged retail products and insurance-based investment products (PRIIPs) can serve as the model. The draft of an Ordinance on Promoting Transparency in the Telecommunications Market (TC Transparency Ordinance)[158] is also on the right track. Both the Regulation and the Ordinance stipulate that enterprises uniformly use the prescribed sample information documents. Administrative sanctions can be imposed against any breaches and the provision of erroneous information can lead to civil-law liability. Information on data protection, terms and conditions, and the end-user agreement should be provided in a standardised form which should be structured together with business and consumer associations. The extent and the linguistic comprehensibility of the information should be geared to readers' cognitive abilities. New designs should be employed.

Digital legal relationships are intended to be permanent. This most definitely applies to "as is" services, which cover a broad spectrum of services ranging from Google to social networks. Consumer rights can only be upheld if additional safeguards are incorporated for the duration of the legal relationship and in the event of its termination. In view of the key nature of the information provided in the information documents, consumers must be given the option of withdrawing from the contract if changes are made. Their attention must be drawn to this fact. In cases where the contract is continued over a number of years with the consumer's agreement, that consumer should be given the option of requiring the entrepreneur to provide an update in which all the changes are summarised in an information document and made available to them.

The Advisory Council recommends: (1) Before the contract is concluded the entrepreneur must inform consumers on *one page in each case* (500 words) about the relevant data protection requirements and about the terms and conditions. This obligation also applies when changes are made during the contract term. The entrepreneur must use typographic means to clearly highlight any subsequent changes on the one-page information document. The one-page information document and any updates are to be transmitted to consumers on a durable medium within the meaning of section 126b of the German Civil Code. (2) Each change entitles the

[157] See Rott, *Gutachten zur Erschließung und Bewertung offener Fragen und Herausforderungen der deutschen Verbraucherrechtspolitik im 21. Jahrhundert*, Report commissioned by the Advisory Council for Consumer Affairs at the Federal Ministry of Justice and Consumer Protection, November 2016.
[158] Ordinance for Promoting Transparency in the Telecommunications Market (TC Transparency Ordinance), Bundestag Printed Paper 18/1804 (Ordinance) of 15 June 2016.

consumer to withdraw from the contract, to which reference must be made. (3) Sanctions must be imposed against breaches of the duty to include such a reference.

2. Re package offers (including services) when concluding a contract

Electronic devices which provide access to the Internet are generally offered in conjunction with pre-installed software. Consumers can only access the services available on the Internet after registering. There's no such thing as a free lunch, not even on the Internet. It is decisive for a functioning market economy for consumers to be aware of each individual cost item, such as the price of the electronic device, the price of the software and the "price" of the supposedly free service. The only objective of competition policy is to "unpack" the various services as far as possible. If such unpacking is not possible, consumers should at least be aware of the aforementioned costs for the various services. Where third parties are paying for advertising, their contribution to the financing is to be clearly indicated.

The Advisory Council recommends introducing the following information requirements: (1) When consumers purchase an electronic device with pre-installed software, they must be (separately) informed about the price of the device and of the software. The case-law of the European Court of Justice, which requires the opposite, must be adjusted by way of an amendment to the EU Directive. (2) Where third parties are financing digital services this must be disclosed to consumers.

3. Re the scope and legal effects of consent

Article 4 no. 11 of the General Data Protection Regulation sets out the substantive requirements made of the consent which consumers must give; that consent does not, however, necessarily have to be explicit, it can also be given by implication or in the terms and conditions. In the latter case, the principle of transparency and separation under the provisions of Article 7(2) of the General Data Protection Regulation applies, which goes further than the existing law of general terms and conditions. The basic idea behind the rule in the General Data Protection Regulation should be transferred to the law of general terms and conditions.[159] It is not apparent why greater requirements are made of consent to data processing than of consent to terms and conditions.

Information regarding the terms and conditions must be provided in a one-page information document; consumers can agree by ticking a box, as has previously been the case.[160]

The Advisory Council recommends: Data protection requirements and requirements as regards terms and conditions for consent are to be put on an equal footing. The principle of separation and transparency under Article 7(2) of the General Data Protection Regulation is to be transferred to the inclusion of terms and conditions. Only those rights and obligations which have been set out in a one-page document (see Recommendation no. 1) are binding.

4. Re determining the contracting partner

When consumers effect legal transactions via a platform, it is often difficult for them to recognise whether they have entered into a contractual relationship with the platform or not and what services the platform provides (free information, free or chargeable referral, or a free or chargeable advisory service). The added problem in the sharing economy is that consumers do not know whether the service providers are themselves a consumer or an entrepreneur. The solution to this problem is to reverse the burden of proof. In reality, platforms already in effect exercise control over the available information or could at least do so.[161]

---

[159] See Part III, I. 2. below.
[160] Which they currently hardly ever do, see Domurath/Kosyra (op. cit., fn. 123); Schmechel (op. cit., fn. 16).
[161] Adam/Micklitz (op. cit., fn. 78).

The Advisory Council recommends: (1) In accordance with the proposal put forward by France, the platform operator must provide precise information about the service's function and the nature of the legal relationships; if the platform requires consumers to open a user account, this information is to be provided before the account is created. (2) In line with its actual function, the platform operator must take on a monitoring and control function; in the event of violating these obligations it will be liable vis-à-vis the consumer. (3) A rule should be introduced in the sharing economy based on which anyone providing chargeable services via a platform is to be treated like an entrepreneur within the meaning of section 14 of the German Civil Code until the opposite is proven.

5. Re the subject of the legal relationship

In the case of "as is" digital services, the legislature needs to clarify whether a contractual relationship or a quasi-contractual relationship with mutual rights and obligations has been established. Section 312 (1) of the German Civil Code, which requires non-gratuitous performance in the case of a contract, is not only not compatible with EU law, it also does not reflect reality on the Internet. Consumers de facto pay for the digital service with their data.

The Advisory Council recommends making it clear that "as is" digital services constitute a legal relationship which is linked to rights and obligations.

In the case of "as is" digital services, the provider is responsible for determining and altering the services to be provided. Since a legal relationship has been established, providers of "as is" services are subject to the exact same requirements as the providers of chargeable services. They must provide information in two information documents on the planned processing of data and the subject matter of the contract defined via terms and conditions, as well as about any changes made during the contract term.

The Advisory Council recommends extending the rule on information documents which must be transmitted before a legal relationship is established to include "as is" services.

One of the key challenges in the digital world is the "structural erosion of ownership".[162] Where a consumer purchases an electronic device, the property is without function until the device can be used together with software. The fundamental subject matter of the contract is thus the possibility of using the software installed on the electronic device. Its scope is defined under copyright law and given concrete form in the terms and conditions. Users have long been formulating their demands under the heading of "fair use".

The Advisory Council recommends adding those clauses which are typically found in digital contexts and, in particular, in end-user agreements to the black and grey list of prohibited clauses.

Those questions which have arisen following the introduction of smart contracts have as yet not been solved. According to Gerald Spindler, a smart contract is a program for self-executing intelligent contracts.[163] A smart contract can be implemented directly using blockchain technology. It enables the conclusion of a contract to be monitored electronically. Factual reasons why, for example, an instalment has not been paid cannot be processed in the system.

The Advisory Council recommends stepping up research into the possible use of blockchain technology and the possible legal consequences of smart contracts.

Three different legal fields come together when the subject matter of the legal relationships is put in concrete form, although their legal effects are compatible only to a very limited degree:

[162] The phrase was coined by Wendehorst (op. cit., fn. 21).
[163] From Spindler's report (op. cit., fn. 22), which makes reference to the Ethereum platform: https://www.ethereum.org/ (last retrieved 6 Sept. 2016).

data protection law, copyright law, and civil and consumer law. The shifting of a great deal of legislative competence onto the EU has increased the preponderance of overlapping rules. The combination of data protection and copyright law determines the rules applicable in the digital economy and is superimposed on classic civil-law rules laid down in the German Civil Code. This development goes beyond consumer law and also affects B2C contracts. The process is in particular used in the financial sector as such (crypto currencies such as Bitcoin and Ethereum). However, first pilot projects using blockchains are also being run in the United States in other areas, such as the energy sector to sideline energy providers and to be able to effect energy trade more cheaply and directly via producers, for instance prosumers.[164] The problem becomes particularly virulent on account of the use of terms and conditions which shape the services contract, influence the end-user agreement and indicate that there are points of contact with data protection law.[165]

The Advisory Council recommends systematically analysing the interplay between data protection law, copyright law and private/consumer law, because only a holistic perspective opens up the possibility of finding generalised rules which could provide insights and indicate the way forward for the digital world. From the consumer perspective, what is of the greatest importance in the short term is how the monitoring of terms and conditions can be brought into line with data protection and copyright law.

When merging previously distinct legal fields we have to reconsider whether and how counterperformance "in data" has an impact on the subject matter of the contract. The Advisory Council will be issuing a separate opinion on this issue in summer 2017.

Ch. Wendehorst[166] argues that non-compliance with the data protection safeguards under Article 25 of the General Data Protection Regulation on data protection by technology is to be regarded as a material defect within the meaning of section 434 of the German Civil Code. However, on account of its being geared to the functionality of the item purchased, the current definition of "material defect", Wendehorst claims, is not suited to defining *privacy by design* and *privacy by default* as criteria for contractual conformity. According to *Gerald Spindler*,[167] the basic IT security of products represents an essential protective and ancillary contractual obligation.

The Advisory Council recommends making it clear that privacy by design and privacy by default as well as basic IT security measures are part of the definition of the "use intended under the contract" within the meaning of section 434 (1) no. 1 of the German Civil Code.

6. Re the rights resulting from the legal relationship

The right of data portability was introduced in Article 20 of the General Data Protection Regulation following the ECJ's *Google* ruling. The right aims to give consumers the option of moving their online profile from one social network, for instance, to another with only one click of the mouse. Many questions this right raises have not yet been answered and need investigating in more depth: How similar do the networks need to be? How can data portability be effected technically? How are third-party rights to be safeguarded? How can we prevent potential costs being taken into account as a ground for exclusion? The question of how the right of data portability is dovetailed with contract law has not yet been answered. Once again, data protection law and contract law need to be synchronised. The wording of Article 20 of the General Data Protection Regulation does not make it clear whether consumers can only assert the right if they wish to transfer data to another provider or

[164] The Consumer Association North Rhine-Westphalia published a short study and a position paper: http://www.verbraucherzentrale.nrw/blockchain (last retrieved 24 Nov. 2016).
[165] Wendehorst (op. cit., fn. 21).
[166] Wendehorst (op. cit., fn. 21) p. 68 et seq.
[167] Spindler, *Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären* (op. cit., fn. 59), in particular p. 12 et seqq.

whether they can also request that the data be returned if they do not plan to change providers. It is precisely the right of such transferral to the consumer which needs to be guaranteed.

The Advisory Council recommends making it clear that the right of data portability is also to be understood as a right of termination by means of which consumers can demand that their data be returned free of charge and deleted on a standard, machine-readable and interoperable medium.

The Internet of Things raises specific legal questions on account, firstly, of the digital content of the contract (interoperability, security, functionality, maintenance, updates, patches, privacy by design and by default) and, secondly, because of the discrepancy between the purchase contract and the embedded digital content, outsourced digital content, updates of digital content, digital services and data access, which are generally provided by third parties.[168] Both issues are a matter for intense debate. Account must here be taken of the fact that, from the consumer's perspective, the purchase contract and digital content provided by third parties are a self-contained entity, even though they are legally separate. Neither a unified model, nor an agency model, nor a guarantee model provides satisfactory solutions, because these options tend to hold the dealer/seller liable for third-party services. The solution might be to introduce product warranty liability, which is primarily directed against the producer of a technical device who is liable vis-à-vis the consumer for providing third-party digital services or rather vis-à-vis the importer domiciled in the EU who imports the products into the EU.

The Advisory Council recommends, to counteract the discrepancy between the purchase contract and digital content provided by third parties, that product warranty liability be introduced against the producer or against the importer into the EU who is also liable against the consumer as regards third-party digital services.

7. Re improving individual redress

When enacted to implement the ADR Directive and the ODR Regulation, the Consumer Dispute Resolution Act created a uniform framework for out-of-court dispute resolution, both in the national and EU context. In view of the fact that it only entered into force on 1 April 2016, it is still too early for an evaluation.[169] Under section 43 (2) of the Consumer Dispute Resolution Act, the functioning of the arbitration board is to be evaluated by 31 December 2020. The Advisory Council believes it is key that the necessary precautions are taken now in order to be able to evaluate that information which comes together in the arbitration boards. This evaluation should distinguish between the type of legal conflict, the involved enterprises, the affected sectors and the products. Legal practice without law, as it were, is to be avoided, especially when the stored data are located elsewhere in Europe. Even though out-of-court dispute resolution aims at reaching compromises, these too must be based on the law. To ensure this is the case, the information (and in particular the evaluation) produced in the arbitration boards needs to be published. Section 34 of the Consumer Dispute Resolution Act makes only very vague requirements which lead us to expect there will be a high degree of heterogeneity.[170]

Model contracts could contribute to finding digital contracts by means of arbitration. Business and consumer associations could together make a key contribution to increasing legal certainty.

[168] Wendehorst (op. cit., fn. 21).
[169] For an academic perspective, see the special issue of the magazine *Verbraucher und Recht* on the introduction of the Consumer Dispute Resolution Act, 2016.
[170] See Part V, III. 3. regarding the possibilities for action available to digital agencies if they were able to make systematic use of the data.

The Advisory Council suggests that business and consumer associations should be involved in drafting model contracts for digital services which not only safeguard key elements of the content of such contracts but also link in to arbitration mechanisms.

The focus should be on new forms of private action. Passenger rights are one such example. These are asserted with the help of commercially active intermediaries who realise consumer rights against payment of a percentage share.[171] They undeniably help many consumers to assert their rights. However, providers of such services only handle clear-cut cases. Consumers are left alone to deal with high-risk cases or are referred to publicly-funded consumer associations. Recently, some airlines have also taken to ruling out the option of assigning rights to intermediaries in their terms and conditions (e.g. Ryanair).

The Advisory Board suggests closely monitoring the effects of private, commercial mechanisms on redress backed by associations.

8. Re improving collective redress

At the interface between market practices and terms and conditions, the German system of legal redress is based solely on a privately organised system of collective redress by consumer associations and by industry associations. When it comes to monitoring terms and conditions, trade associations are de facto not an option. Although they do in fact have legal standing, in the 40 years since the introduction of the right of representative action (*Verbandsklage*), use has been made of this option under very rare circumstances. For instance, a private action lies with the Federation of German Consumer Associations, which is funded by the Federal Government, and with those consumer associations which the *Länder* (federal sates) have given sufficient means to realise the right of representative action. In the field of fair trading law the trade associations handle around two thirds of cases, some of which at least concern consumer interests. The other third of cases are dealt with by the aforementioned consumer associations. Where there are points of contact with consumer data protection, consumer associations have been entitled, since 2016, to file a cease-and-desist order against enterprises. However, it is the often under-funded data protection authorities which are primarily responsible, even though the representative actions consumer associations have brought have made a key contribution to clarifying what the requirements for consent are under data protection law.

Despite the considerable legislative effort involved, cross-border representative action is hardly an option in practice. The questions of jurisdiction, applicable law and enforcement of a German judgment abroad or, vice versa, of a foreign decision in Germany are too difficult to answer. Existing EU legislation is not tailored to collective representative action and raises numerous legal questions for the clarification of which – in addition to the procedure under Regulation 2006/2004 on cross-border cooperation in consumer protection[172] – the consumer associations are fairly unwilling to spend their scare resources. That is why consumer organisations in the EU Member States, with the help of the European umbrella association BEUC, identify cross-border practices against which the national associations can take coordinated action. Official cross-border networks cannot fill this gap, including on account of a lack of the necessary powers of intervention beyond a cease-and-desist order.

It appears, given the current state of the political debate, that one solution could be to expand the Federal Cartel Office. If this expansion were linear, it would also lead to an expansion of the legal remedies available to the Federal Cartel Office to include the monitoring of advertising and of terms and conditions. As opposed to the warning procedure and cease-and-desist claim, the Federal Cartel Office could, under section 32 (2a) of the Act against Restraints of Competition, order reimbursement of the benefits generated. This provision could be extended to include disadvantages which consumers suffer on account of

[171] See Rott, "Claims Management Services: An Alternative to ADR?", (2016), *European Review of Private Law*, p. 143–160.
[172] See Part III, IV. 3. and 4. above.

impermissible business terms or unfair advertising. This would be entirely in the spirit of Article 8 of the proposal put forward by the European Commission for the reform of Regulation 2006/2004, which was supposed to serve as the benchmark for those minimum legal remedies which are to be available. These mechanisms for official redress in consumer protection are on no account supposed to replace the work of the consumer organisations, but they can be a sensible complement to it. However, it would have to be guaranteed that the digital agency exercises its powers to assert consumer rights independently and not out of any economic or political considerations.

The Advisory Council agrees with the thrust of this year's Consumer Law Conference at which calls were made to add governmental monitoring (digital agency) to legal redress through associations. Based on the example set by the UK, an additional "super complaint" would be a conceivable option, a procedure in which associations could force the authorities to act by calling on a court if need be.

9. Re the suitable means for implementing the proposals

The proposed solutions touch on a number of statutory provisions. This is due to the different logic applied to the provisions of consumer protection law in the German Civil Code and efforts to synchronise data protection law and the law of general terms and conditions.

The Advisory Council advocates implementing the proposals in a manner which maintains the cohesion between the proposed rules. In view of the political sensitivities which go along with any interference with the German Civil Code, amendments to the German Civil Code should be limited to what is absolutely essential. More specifically, a presumption rule for commercial activities would have to be incorporated into sections 13 and 14 of the German Civil Code and consent under data protection law brought into line with consent under the law of general terms and conditions.

10. Re the need for an evidence-based consumer policy

The Advisory Council commissioned an exploratory study into which data are available in consumer protection law and which are not.[173] Point VIII of the report enumerates a long list of gaps and makes concrete proposals for how these gaps are to be filled. There are hardly any politically robust data on consumer protection law, beyond needs- and project-based results. Data capture using parameters which are standardised across Europe driven forward by means of market watchdog projects promises to bring about improvements in the field of legal advisory services and legal representation provided by consumer associations in the *Länder*. Such efforts have, however, not yet been undertaken in other areas.

The Advisory Council recommends taking the necessary precautions in order to be able to shape an evidence-based consumer *law* policy.

11. Re the problem of competence

The proposed solutions will impact on the European Union's system of competencies. A distinction has to be drawn between directives which merely lay down a minimum level of harmonisation, such as Directive 93/13/EEC and Directive 1999/44/EC on the sale of consumer goods, and those directives aiming at full harmonisation. In particular, these include the E-Commerce Directive 2000/31/EC, Directive 2005/29/EC on unfair commercial practices and Directive 2011/83/EU on consumer rights. The definitions of "consumer" and "entrepreneur" are not fully harmonised.

[173] Schmidt-Kessel, Larch, Erler, Heid, Grimm, *Exploraionsstudie zu vorhandenen und fehlenden Daten im Verbraucherschutzrecht*, Report commissioned by the Advisory Council for Consumer Affairs at the Federal Ministry of Justice and Consumer Protection, June 2016.

France's attempts to adopt rules on information provision via platforms to the benefit of French consumers met with resistance from the European Commission, including on account of the fact that they touch on the area of application of the E-Commerce Directive and the Directive on unfair commercial practices. In the light of this perspective, it is to be expected that the European Commission will also resist the following proposals:

- Packaging of offers (including services),
- Data protection information document,
- Determining the contracting partner,
- Control and monitoring function of platforms,
- Fair use of copyright-protected software programs and, possibly,
- Product warranty liability.

An answer should be found, by way of a legal opinion, to the following question: How precisely should the solution options be defined to avoid conflict with EU law as far as possible and to strengthen national autonomy of action?

The Advisory Council is convinced that Germany is free to take the political lead and, possibly together with other Member States, to call on the European Commission to act.

Part IV Algorithms, software agents, code and big data

The macro perspective aims to provide an outlook on the pressing issues and possible solutions associated with ongoing developments in regard to digital technologies in the fields of software agent systems, regulation by algorithm and the potential of big data. Discussions about how these terms are to be defined and delimited from one another vary greatly according to which discipline is involved. The Advisory Council uses the terms as follows: "Code"[174] is the generic term used to describe programming languages in general. An "algorithm" is part of a code and is implemented in various programming languages; it describes certain programming logics. A "software agent" is a program (based on code and more specifically on algorithms) which can act relatively autonomously – depending on the type of agent it can respond to the environment and interact "socially" with other agents.

In line with its remit, the Advisory Council regards its task as identifying groups of questions and coming up with possible solutions so as to initiate a debate on political solutions. At the superordinate level of digitalisation, three big transformation processes can be made out which are based on the emergence of self-learning algorithms,[175] of big data and transformation technologies. These big transformation processes offer consumers as yet unknown potential for autonomous and social action via the Internet, but they also generate new risks of as yet unknown dimensions. The transformation processes can potentially

- link access to goods and services to discriminatory conditions,
- facilitate unfair commercial practices not on the basis of false information but based on a better understanding of consumer behaviour,
- modify the Internet code at will unless algorithms are described in legal relationships, which is still generally not the case.

[174] Lessig, "The Law of the Horse: What Cyberlaw Might Teach", (1999), *Harvard Law Review* 113, p. 50–549, p. 506, fn. 15; later Lessig, *Code and Other Laws of Cyberspace* (New York: Basic 1999); *Lessig*, *Code V2* (New York: Basic 2006), p. 506, fn. 15 refers to "the software and the hardware that constitutes cyberspace as it is – or, more accurately, the rules and instructions embedded in the software and hardware that together constitute cyberspace as it is…".

[175] Sartor, "Cognitive Automata and the Law: Electronic Contracting and the Intentionality of Software Agents", (2009), *17 Artificial Intelligence and Law,* p. 253; "digital entities capable of executing autonomously the mandates assigned to them".

Since *L. Lessig*'s groundbreaking 1999 article a debate has again and again arisen about the ability to regulate and the need to regulate those rules which business itself created and which dominate both access to and the functioning and content of the Internet. Today the focus is less on the "code" than on the question of whether and to what extent algorithms *can* and *should* be subject to regulation. *Should* refers to the political need or desirability.

The German legislature took unilateral action by laying down rules on scoring in section 28b of the Federal Data Protection Act. One can fitly argue the pros and cons of the political necessity for doing so, in particular how much sense this German rule makes. However, should it be possible to justify the need for this intervention, then it appears to make little sense in hoping that it will be possible to find an EU or international solution which can be coordinated with the United States, China, Russia and India. Concrete political action will also be required to launch a debate at the international level.

The question of political necessity needs to be kept separate from that of technical feasibility, that is whether one *can*. Where humans are responsible for an algorithm, the solution appears to be simple, that is if one ignores the fact that programmers and lawyers each speak their own languages. Self-learning algorithms present new obstacles, because they raise no more and no less than the matter of to what extent legal rules can be translated into the Internet's binary code. It seems that the legislature will find it comparatively easy to come up with a rule on data profiling. The General Data Protection Regulation already addresses the issue. But here, too, the problems seem to go much deeper than merely disclosing the relevant profiling technologies.

I. Algorithms and artificial intelligence

What is decisive from the legal perspective is whether it is possible to determine responsibilities, because that is precisely what is up for discussion where self-learning algorithms are concerned. It is useful to distinguish between the design laid down by the software program and the action to be potentially carried out.

1. Responsibilities

The software program defines the design, but not the action to be potentially carried out. The following example may make the distinction between the two types of algorithm clear: Take two salespeople, one who works in a department store, the other in a bazaar. The owner of the department store instructs the salesperson to sell product X for Y euros, product X1 for Y1 euros, etc. If the product is faulty, the salesperson is instructed to grant a 20% rebate. The aim is clear: The owner wants to cover all conceivable options by giving precise instructions. The salesperson may not in fact stick to these rules, but that would then mean going against instructions. The owner of the bazaar chooses an entirely different approach, saying that he paid X1 and Y1 for product X and product Y, that the salesperson is to make as much profit as he wants, to negotiate the prices himself. If the potential buyer is wealthy, the salesperson is to start at a high price. Buyers of X nationality tend to like Y products, women prefer Y products. The salesperson is free to give or promise customers add-ons. The owner is only interested in the salesperson making as much profit as possible. The second owner only gives the salesperson a goal, but leaves the salesperson to decide how to achieve it.

The first case can be evaluated ex ante, the second needs an ex-post review, because it is only possible to find out exactly how the salesperson made use of the leeway granted after the sale has been made. If both tasks are assigned to computer software, then the crucial question is this: Legally speaking, these types of actions are not neutral. They may breach applicable law if carried out by humans. The law cannot directly impose rules on software agents, since software agents cannot "understand" and cannot "read" the law. The law would have to have been programmed into the software agents. On the other hand, software

agents are "fully designable":[176] They are what the programmer makes them. How that can be done, how and whether programming languages and legal language are in fact compatible or can be made compatible is a question which the computer and legal sciences will have to investigate together.

In practice, enterprises use algorithms to profile consumers, to design online information and advisory programs ranging from financial services (known as robo-advisers) to health apps, and to offer "as is" digital services.[177] The spectrum is broad: from simple algorithms which ask for four or five items of information and then deliver information on that basis, up to highly complex algorithms which send Internet users the information they requested and link it to advertising and sales offers. Consumers themselves could become users of software agents as soon as the Internet of Things takes on more concrete shape, for example in the case of refrigerators ordering food from a supermarket.

2. Legal classification

Principal Agent Theory can be used to fruitful effect when it comes to assigning legal responsibilities. If it is possible to identify the principal, then the law has no problem when it comes to legal classification. In the course of adopting the E-Commerce Directive the question came up of how to legally classify the automatic forwarding of an email. At that time the question above all revolved around access when the consumer (buyer) receives an automatic reply. These legal issues are a thing of the past, because their classification did not in fact prove to be seriously difficult.[178] A legal assessment of self-learning algorithms will prove more difficult, since it ultimately raises the question of how artificial intelligence (AI) impacts the legal system, whether the agent is no longer to be assigned to the principal, whether the software agent itself becomes an autonomously acting legal subject or the principal who has configured the self-learning algorithm still has ultimate responsibility. *In other words: Who is the principal and who is the agent?*

This is, of course, not the place to present the debate around AI, let alone to take a stand on that debate. Mention need here only be made of the fact that the academic debate has two shortcomings: First, AI experts do not understand the law, and lawyers do not understand AI. Second, the debate is dominated by stereotypical thinking, with the exceptionalists on one side and the unexceptionalists on the other, and only a few exceptions.[179] The only question at issue here is how to assess self-learning algorithms: Do self-learning algorithms only adapt their results based on the type and nature of the data processed or do they also change the source code itself?

The answer does not appear to be so simple. Self-learning should not be equated with changing or even rewriting the source code. How "autonomous" the algorithm is in turn depends on the source code itself. The problem can be discussed using an example:[180]

> *"The algorithm's task (stated by a user) is to display a commercial to 1000 people who have the highest chance of buying a product, say: insomnia pills. This is the human input. The programmer does not know what people will be 'available' (how many, or what data will be available) when writing the algorithm. What the algorithm gets from the user is that insomnia pills are for people who cannot sleep. Self-learning process is the following: algorithm itself collects data about*

[176] Pasquale, *The Black Box Society: The Secret Algorithms behind Money and Information* (Harvard University Press, 2015).
[177] Adam/Micklitz (op. cit., fn. 78).
[178] Micklitz, "Fernabsatz und e-commerce im Schuldrechtsmodernisierungsgesetz", (2001), *Europäische Zeitschrift für Wirtschaftsrecht*, Vol. 5, p. 133–143.
[179] There are exceptions, though: Solum, "Legal Personhood for Artificial Intelligence", (1991–1992), *North Carolina Law Review*, p. 1231, and Sartor, "Cognitive Automata and the Law: Electronic Contracting and the Intentionality of Software Agents", (2009), *17 Artificial Intelligence and Law*, p. 253.
[180] Palka, PhD student in his fourth year at the European University Institute in Florence.

people and discovers patterns – people in age X on average sleep in hours Y-Z; stress causes insomnia; events x, y, z cause stress -> based on this, if someone is in age X and is not asleep in hours Y-Z and undergoes an event x or y or z, the program decides to display the commercial to such a person. Later, it evaluates its own choice by seeing how many of these people actually clicked the link. It might see that most of the people who clicked where living in the cities, or in northern countries, etc. It would add this to its database for the future etc. It generally learns a lot about people from observing what they do, how they respond to incentives etc. In this sense, when the algorithm gets the task 'display the commercial to 1000 people having the highest chance of buying it' a few months later, it can 'decide' to show it to a completely different set of people, possibly in a more effective way. Even though no human re-programmed it. It did re-program itself in a manner foreseen by the programmer, but not in the direction foreseen (direction was 'chosen' by the software itself). That is why 'autonomous' is not autonomous in a human sense. It is limited. But it is not merely automatic. Whether this is the change of the source code, or just modification of a database, depends on particular programming technique and our terminology – but at least for legal purposes, this does not matter that much. What matters is that the process was not merely 'automatic'."

The difference is relevant because a software agent can make a choice which is legally not correct. In the above example the scenario could be regarded as a prohibited type of aggressive advertising. In a slightly modified form the choice could be regarded as discrimination based on gender or ethnicity (where higher prices are offered to those who are prepared to pay more; the potential addressees of advertising are uncoupled on the basis of their political opinion or sexual orientation). Both anti-discrimination law[181] and fair trading law[182] establish boundaries for such practices. The fact that systematic breaches of the law are possible is one key reason why rules on algorithms should be enshrined in law. Such illegal practices are generally hidden from view, although they are certainly no mirage, as first empirical studies have already shown.[183] If a self-learning algorithm "decides" not to pass information on to a particular country, the potential users are uncoupled from access. The software agent operates on the basis of a predefined goal, but the software agent itself chooses which concrete actions to take to achieve that goal. The way in which the software agent decides to take which action is pre-programmed, but no-one can predict precisely what the software agent will do.

---

[181] For instance, section 19 (1) of the General Act on Equal Treatment (*Allgemeines Gleichbehandlungsgesetz*, AGG): "Any discrimination on the grounds of race or ethnic origin, sex, religion, disability, age or sexual orientation shall be illegal when establishing, executing or terminating civil-law obligations". As far as EU directives are concerned, see: Directive 2000/43/EC implementing the principle of equal treatment between persons irrespective of racial or ethnic origin and Directive 2004/113/EC implementing the principle of equal treatment between men and women in the access to and supply of goods and services, prohibiting discrimination in access to goods and services, based on race and gender respectively; see also Brownsword, *The E-Commerce Directive, Consumer Transactions, and the Digital Single Market: Questions of Regulatory Fitness, Regulatory Disconnection and Rule Redirection*, lecture given on 18 June 2016 at the SECOLA conference in Tartu, Estonia.

[182] See Directive 2005/29/EC on Unfair Commercial Practices, in which "to materially distort the economic behaviour of consumers" is defined as "using a commercial practice to appreciably impair the consumer's ability to make an informed decision, thereby causing the consumer to take a transactional decision that he would not have taken otherwise", which would include the late-night advertising example; see Brownsword, *The E-Commerce Directive, Consumer Transactions, and the Digital Single Market: Questions of Regulatory Fitness, Regulatory Disconnection and Rule Redirection*, lecture given on 18 June 2016 at the SECOLA conference in Tartu, Estonia.

[183] Sweeney, "Discrimination in Online Ad Delivery" (2013), *Communications of the ACM*, Vol. 56 No. 5, p. 44–54; Chander, "The Racist Algorithm?", (2017), *115 Michigan Law Review*, Forthcoming UC Davis Legal Studies Research Paper No. 498.

As well as this internal perspective, that is the relationship between the principal and the agent, account also needs to be taken of the network effect. The complexity of self-learning algorithms is based on the interaction between systems, between the algorithms themselves in an interconnected environment. This represents an emergence in which responsibility is distributed across many actors. In an interconnected city, for example, numerous sensors and systems interact with driverless cars. It is conceivable that in future systems will be able to continue developing their own algorithms, in which case algorithms will write algorithms.

Now it is not the case that these algorithms are operating in a legal vacuum so to speak, only that software agents are not explicitly regulated by law. Under the law as it currently stands, software agents are regarded as tools applied by humans, by an enterprise or a body responsible for the algorithm. Whenever a software agent produces discriminatory, unfair or misleading market practices, the person or body responsible for producing the algorithm will be held responsible. As things currently stand, the law of general terms and conditions, anti-discrimination law and, above all, fair trading law play a key role. The only sanction provided for under German law is a stop-order mechanism, that is the incriminating practice is prohibited ex nunc.

At least that is what it looks like on paper. However, since the actions which software agents take are largely hidden from view, there is little chance of legal breaches being found out. As a result, enterprises' willingness to abide by the law necessarily drops too. Applying the terminology of economic legal analysis, this means that where the costs of incorporating legal requirements into the algorithm are higher than the potential loss after illegal actions are found out, enterprises will see little need to comply with legal rules ex ante. This leads to the call for algorithms, even self-learning ones, to have to comply with applicable law. The principle of transparency should apply to algorithms and it ought to be possible to check whether the law is being complied with.

II. Big data, information asymmetry and profiling

Commonly applied definitions of neither "big data" nor "profiling" are yet available, and so various definitions are in use. A simple and pragmatic approach will suffice for our purposes. "Big data" is here defined as any technology which permits unlimited quantities of data to be gathered and processed, whereby the data are accessible because users have put them into the Internet and sufficient technical capacities are available for evaluating them.[184] "Profiling" is here defined as any technology which permits conclusions to be drawn from existing data and profiles regarding individual behaviour.[185] Article 4(4) of the General Data Protection Regulation contains a legal definition:

> *"'Profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."*

1. The problem

Information asymmetry is not a new problem. The whole of existing consumer law is based on the idea that asymmetries can be eliminated using government-prescribed information rules. Despite all the criticism, above all from the behavioural sciences, consumer policy is sticking to this paradigm, not least because society rightly assumes that legal subjects act autonomously and under their own responsibility. The need to differentiate between different consumer models does not change that premise. No-one is calling the normative model of democratic societies into question.

[184] Hildebrandt/Gaakeer, (eds), *Human Law and Computer Law: Comparative Perspectives*, (Springer Verlag, 2013).
[185] Hildebrandt/Gutwirth, (eds), *Profiling the European Citizen. Cross-Disciplinary Perspectives*, (Springer Verlag, 2008).

The linking of insights gained in the behavioural sciences with big data and profiling technologies has given rise to a new kind of information asymmetry. In the analogue world the business sector knows more about products and markets. Consumer behaviour research used to be time-consuming and expensive, and its findings were only of limited use. Big data and profiling give the business world the chance to analyse consumer behaviour in a targeted manner, to better understand why a particular decision was taken and thus to get to know consumers better than they know themselves (or even want to know themselves).[186] This advantage means targeted advertising campaigns can be used in entirely new ways to drastically reduce costs and increase the efficiency of the advertising means employed.

> *Example*
> *Imagine a person with the following Google profile: male/female, aged 26–30, works from 7 a.m. to 6 p.m., buys medicines online. If that person permits localisation on their smartphone, then Google knows when they are at home and how long they sleep at night and are motionless. Google can also see when that person gets up at 3 a.m. and picks up their mobile phone. A supplier of sleeping pills could charge Google with offering its products around that time of night to those consumers who have difficulty sleeping and who browse the Internet to distract themselves. Such a transaction would not be the result of information asymmetry about the product or market, but about the manner in which, the conditions under which and the time of day when consumers take a decision. The entrepreneur knows what consumers do not know, namely that they behave as predicted by Google under the given conditions.*

2. Legal classification

Existing protective mechanisms available in applicable consumer contract law cover these situations as little as the relatively recent Unfair Commercial Practices Directive does, which the German legislature has incorporated into the Act against Unfair Competition. As far as the situation upstream of the conclusion of a contract is concerned, under applicable law it is already doubtful whether consumers actually have a right to information. The prevailing opinion is that the prohibition of misleading advertising or of a misleading omission is not equal to the consumer's right to objective information about the qualities of a product or service. In our example the problem does not revolve around information about the product or service. In any case, stricter requirements are applied in the law of medicines to limit the scope of advertising much more than in other fields. The suppliers of sleeping pills are only interested in the consumer's behaviour. It is specifically that knowledge about the consumer's behaviour which opens up new sales methods to them.

The extremely wide definition of advertising applied in the Directive and thus also in German law permits marketing oriented to consumer behaviour to be subsumed under the requirements of fair trading law. Only, under applicable law consumers ought to have no right to the offer to buy sleeping pills at 3 a.m. in the morning being based on a sophisticated analysis of their behaviour profile.[187] The question also remains of whether, even if they were aware of that when making their purchase, consumers would behave differently or whether they would be happy to take up the offer. Consumers may take a different decision if they are able to find out beforehand what kind of profile Google has of them, knowing that they can influence their data by deleting or changing data, for instance.

Articles 13 and 15 of the General Data Protection Regulation give consumers rights to information and rights of access which specifically also cover profiling. In the light of the

[186] Lunn, Regulatory Policy and Behavioural Economics, (Organisation for Economic Co-operation and Development, 2014), <http://www.oecd-ilibrary.org/content/book/9789264207851-en> (last retrieved 28 Nov. 2016).
[187] Brownsword, *The E-Commerce Directive, Consumer Transactions, and the Digital Single Market: Questions of Regulatory Fitness, Regulatory Disconnection and Rule Redirection*, lecture given on 18 June 2016 at the SECOLA conference in Tartu, Estonia.

Federal Data Protection Act, it seems reasonable to interpret the General Data Protection Regulation such that consumers are at least to be informed about the basic assumptions applied in the algorithm logic on which the profiling is based.[188] EU law trusts in the power and assertiveness of each individual. Individuals first need to be aware of the problem, they need to assert their claim and possibly apply to a court. What we need is not just one *Schrems,* but many *Schrems*. It is more than doubtful whether it would be possible to get a grip on information asymmetry even if bundling were possible. In addition, the General Data Protection Regulation does not provide for data protection authorities to intervene instead of the Regulation. Since data processing is not linked to binding general requirements, the data protection authorities entrusted with their implementation also appear to lack the competence to measure the algorithms applied against a standard benchmark and, where applicable, to demand that corrections be made.

III. Potential solutions as regards regulating algorithms and big data

The use of algorithms and the prospects opened up by self-learning algorithms which update the source code raises questions of an altogether different dimension than when one takes the micro perspective of digital services. The issue here is not only one of maintaining the *autonomy* of consumers, which was to be the driver behind potential solutions as regards the law of digital services, but of *human dignity* in the age of artificial intelligence (AI). The political challenge is to answer the question of how to ensure that self-learning algorithms "act" in an ethically responsible manner. Can politics trust in business, in competition, in independent ethical behaviour on the part of those who are responsible for driving forward developments when it comes to AI? And, even more difficult, what will happen when AI takes on a life of its own? How can a self-controlling process be politically, ethically and legally mainstreamed?

The Advisory Council believes that it is the political realm which is called to act. The question is no longer whether political action is necessary, but what type of action that could be. A normative component needs to be incorporated into the algorithms. Under the lofty rubric of "human dignity" and the autonomy of human beings, the issue when it comes to consumer law would be compliance with the prohibition of discrimination, fair advertising, consumer data protection law and fair terms and conditions. Once this basic issue has been solved – and the Advisory Council is convinced that political action is what is needed – we will find a series of obstacles strewn across the path towards implementation of that goal which have their origin in the different rationality behind law and technology.[189]

1. Requirements under the Federal Data Protection Act

The 20th century legislative model requires that the government create a legal framework for technology within the context of which business itself develops its own technical standards. The manufacturers of technical products are obliged by the legislature to comply with the state of technology and the state of scientific knowledge. Standardisation bodies have a key role to play in this, since it is they which flesh out the framework provided by the legislature. In Germany, consumers are involved in the process of standardisation through the DIN Consumer Advisory Board. Once adopted, standards enjoy privileged status. Once the manufacturer has certified that its products meet these standards, either itself or via independent third-party institutions (e.g. TÜV), products can be put on the market without further governmental control. In the event of a claim, it is assumed until the opposite is proven that the manufacturer has met any legal obligations. The EU took over this model cum grano salis in the mid-1980s and applied it to technical regulation in Europe.

[188] See Schmechel, (op. cit., fn. 16), who cites Paal, *Beck'sche Kompakt Kommentare Datenschutz-Grundverordnung*, Paal/Pauly (eds), C.H. Beck Verlag 2017, margin no. 31 re Article 13 of the General Data Protection Regulation.
[189] Boer, *Legal Theory, Sources of Law, and the Semantic Web,* (IOS Press, 2009).

The German legislature took a different path in section 28b of the Federal Data Protection Act. In that provision it obliged loan agencies in particular to comply with scientifically-mathematically recognised standards and did not allow them to process especially sensitive data within the meaning of section 3 no. 9 of the Federal Data Protection Act. The provisions read as follows.

Federal Data Protection Act
Section 28b
Scoring

For the purpose of deciding on the creation, execution or termination of a contractual relationship with the data subject, a probability value for certain future action by the data subject may be calculated or used if

1. the data used to calculate the probability value are demonstrably essential ***for calculating the probability of the action on the basis of a scientifically recognised mathematical-statistical procedure*** *[emphasis added],*

2. in case the probability value is calculated by a credit inquiry agency, the conditions for transferring the data used under section 29 and in all other cases the conditions of admissible use of data under section 28 are met,

3. (...)

4. (...)

Section 3
Further definitions

(...)
(9) "Special categories of personal data" means information on a person's racial or ethnic origin, political opinions, religious or philosophical convictions, union membership, health or sex life.
(...)

A case is pending before the Federal Constitutional Court against the Schufa credit agency concerning the matter of whether Schufa should have to disclose its scoring algorithms. The Federal Court of Justice negated just that.[190] The Federal Constitutional Court has not yet declared whether it will accept the constitutional complaint for decision. Germany's highest court has therefore not yet clarified which requirements are to be made of a *scientifically recognised mathematical-statistical procedure*. As regards sensitive data, section 28 (8) read in conjunction with subsection (6) of the Federal Data Protection Act at any rate sets limits when it comes to those criteria which may be applied when determining the score value. What has not yet been clarified is the extent to which the boundaries set in section 19 and section 20 of the General Equal Treatment Act (*Allgemeines Gleichbehandlungsgesetz*, AGG) have an impact on data capture. The US Equal Access Opportunity Act is clearer in that respect.[191] Monitoring compliance with statutory requirements is the responsibility of the data protection authorities. In view of the relatively low mathematical/technical complexity of scoring and the possibility of assigning responsibilities, competent monitoring ought to be safeguarded.[192]

The Advisory Council notes that the existing rule in section 28b of the Federal Data Protection Act represents a useful starting point when it comes to regulating self-learning algorithms.

[190] See Federal Court of Justice, judgment of 28 Jan. 2014, file no. VI ZR 156/13 (Gießen Regional Court, Gießen Local Court). A constitutional complaint has been filed against the Federal Court of Justice's ruling (file no. 1 BvR 756/14).
[191] See Metz, "Scoring: New Legislation in Germany", (2012), *35 Journal of Consumer Policy*, p. 297–305.
[192] See Part IV, III. 1. above.

2. Requirements under the General Data Protection Regulation

Nevertheless, the provision in section 28b of the Federal Data Protection Act cannot be transferred to self-learning algorithms which *autonomously* update and change programs and network among themselves. The US Federal Trade Commission has taken up this problem and is investigating the need to increase and options for increasing transparency.[193] Concrete results are not yet available.

The General Data Protection Regulation only addresses algorithms in the form of an individual entitlement to information and access. This regulatory technique is well-known, as it was used in Directive 2008/48/EC, where the obligation to issue credit responsibly is conceived merely as information.[194]

General Data Protection Regulation
Article 13
Information to be provided where personal data are collected from the data subject

(...)
*(2) In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide **the data subject** [emphasis added] with the following further information necessary to ensure fair and transparent processing:*
(...)

*(f) the existence of **automated decision-making** [emphasis added], including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.*
(...)

Article 15
Right of access by the data subject

*(1) The **data subject** [emphasis added] shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:*
(...)

*(h) the existence of **automated decision-making** [emphasis added], including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. (…)*

Article 9
Processing of special categories of personal data

(1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
(…)

[193] See Part V, II. below, Foreign models.
[194] See also Directive 2014/17/EU on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 (OJ L 60, 28.2.2014, p. 34).

However, unlike section 28b of the German Federal Data Protection Act, the General Data Protection Regulation does *not* make any legally binding requirements in respect of scoring, apart from in Recital 71, according to which "*the controller should use* ***appropriate mathematical or statistical procedures*** *for the profiling*". Unlike section 28b of the Federal Data Protection Act, requirements made of business under the Regulation are subject to a threefold restriction:

- the requirements made under Recital 71 ***should*** be complied with, not "are to be" or "must be" complied with,
- the procedures must be ***appropriate*** and not necessarily "***scientific***",
- the procedure should be ***mathematical or statistical*** and not ***mathematical-statistical***.

Normally, matters on which no political agreement can be reached are moved into the recitals. Ultimately, it is then up to the European Court of Justice to decide to what extent enterprises must use mathematical-statistical procedures, what that means, what standards are to be applied to the mathematical or statistical procedures or what happens if enterprises do not comply with the requirements set in Recital 71. What concrete impact this lowering of standards will have on the distribution of competencies and what scope the German legislature actually retains in view of full harmonisation will need to be discussed elsewhere.[195] At least Article 9(1) of the General Data Protection Regulation, like the Federal Data Protection Act, prohibits the processing of sensitive data. The restrictions imposed on this prohibition will not be addressed here.

Opening up Recital 71 of the General Data Protection Regulation by, in a way, generally binding business in the same way as in section 28b of the Federal Data Protection Act cannot hide the fact that the primary addressees of the EU requirements are citizens who want to assert their right to information and access. However, under the provision of Recital 63, that right "*should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software*". In the light of the Federal Data Protection Act, it is obvious that the General Data Protection Regulation should be interpreted to mean that consumers should at least be informed about the basic assumptions made in the algorithm logic.[196] Depending on the outcome of the proceedings pending before the Federal Constitutional Court, the question of the relationship between EU law and Germany's Basic Law could also be raised. Even if it were possible to push through the German legal position across Europe – perhaps after it is underpinned by constitutional law – we are still left, in regard to this complex issue, with requirements under EU law which do not go very far because they are entirely guided by the power of individuals and their ability to assert their rights.

There are considerable consequences as regards official legal redress. Profiling also has to be measured against the provisions of the General Data Protection Regulation on the admissibility of personal data processing. However, under Article 58(1a) of the Regulation, the data protection authorities are also tasked with monitoring and implementing application of the Regulation. This concerns the principles applied to data processing as set out in Chapter II (Articles 5 to 11) of the Regulation. It is not entirely clear whether the monitoring obligation also applies to the algorithms used, which are only referred to in regard to the rights of the data subject in Chapter III, and then only in the recitals, which have no legal force. Even if there were such an obligation, there are no uniform standards to which the authorities could gear their activities.

[195] See Part V, III. 4.

[196] Schmechel (op. cit., fn. 16), who cites Paal, *Beck'sche Kompakt Kommentare Datenschutz-Grundverordnung*, Paal/Pauly (eds), C.H. Beck Verlag 2017, margin no. 31 re Article 13 of the General Data Protection Regulation.

The Advisory Council notes that the rudimentary approaches to regulating algorithms set out in the General Data Protection Regulation are insufficient and fall below even the standard applied in section 28b of the Federal Data Protection Act.

3. Re the three possible options for a regulatory approach

The Advisory Council notes that there are theoretically three possible options for regulating this matter:

- ***proactive* (legality by design): the legislature could oblige enterprises to incorporate binding legal requirements into algorithm development;**
- ***reactive*: the legislature could restrict itself to obliging enterprises to comply with the law when developing algorithms (which actually goes without saying) and then focus on ex-post monitoring;**
- ***the happy medium:* the legislature could set a regulatory framework which combines binding governmental requirements with self-regulation.**

These options will be outlined and analysed in the following.

4. Re lack of transferability of technical regulation

If the legislature decides to take the *proactive* approach, in the light of a century's worth of experience, it would make sense to oblige industry to comply with the rules of technology. The following triad has become established both legislatively and constitutionally[197] when it comes to regulating product safety:[198] the generally recognised rules of technology; the state of the art; and the current state of science and technology. It is obvious even at first glance that the German legislature has set the bar high in section 28b of the Federal Data Protection Act. Credit institutions must apply scientifically validated methods, that is not only those which are generally recognised and generally applied but those which stand up to being measured against scientifically validated standards. One of these three standards has taken root, namely the generally recognised rules of technology in the field of consumer goods and the current state of science and technology for medicinal products. Where products are subject to pre-market control exercised by government authorities, these are obliged to examine compatibility with binding government requirements when licensing products. Where no such pre-market controls are conducted, which – for good reason – is the case for all technical consumer goods, either the manufacturers themselves or authorised certification agencies establish whether the product meets the generally recognised rules of technology. The point of reference when conducting this assessment is generally the technical standards drawn up by German standardisation bodies or by EU standardisation institutions. Within the EU, self-certification or third-party certification guarantees manufacturers (or importers) access to the Single Market. However, manufacturers are not obliged to abide by technical standards. They can also apply other methods to ensure they are complying with the statutory safety requirements. Corrective measures are taken under labiality law. Where products give rise to damage despite standards being complied with, the courts can hold manufacturers liable in so far as this proves justified.

Transferring the above approach to digitalisation, the legislature could set binding standards as regards developing algorithms. One conceivable option would be, for example, to reformulate Article 9 of the General Data Protection Regulation (the prohibition of processing sensitive data and its exceptions) in this way. As simple and convincing as such a rule may

[197] Federal Constitutional Court, order of 8 August 1978, file no. 2 BvL 8/77.
[198] Marburger, *Die Regeln der Technik im Recht*, (Heymanns Verlag, 1982); Joerges/Falke/Micklitz/Brüggemeier, "Die Sicherheit von Konsumgütern und die Entwicklung der Europäischen Gemeinschaft", (1988), *Schriftenreihe des Zentrums für Europäische Rechtspolitik*, Vol. 2, p. 523.

appear, it would at best solve questions concerning *automated* programming by software agents, but not programming by *autonomous* software agents. Compliance with legal requirements can, therefore, only be guaranteed if they are not only incorporated into the source code but if they are also automatically taken into account whenever an autonomous change is made. To be able to do that, legal rules would have to be made compatible with the logic of the "code", which only understands "yes" and "no" and cannot cope with vaguely formulated general legal clauses (e.g. "good faith" or "good morals").

Across the world research teams are working on the options which *legality by design* opens up. Opinions differ as to their feasibility. Thinking this through to the end, full compatibility would mean reducing the law down to a "yes" or a "no" and incorporating legal reality into this "yes/no" logic. Legality by design would have to be shaped in such a way that all possible cases could be broken down into "yes/no". It would also be worth thinking about incorporating an option into an algorithm in which a competent human being would have to be called in where uncertainty arises as to how to handle reality. It is clear that a great deal more research needs to be done here. It is currently still unclear whether such compatibility can actually be created by technical means.

In fact, the trend when it comes to standard-setting in consumer law is towards general clauses. It is not least the adoption of the idea of social protection (the protection of the weakest under law) which has meant that the number of legal rules which bind the contracting parties to the principles of good faith, good morals and, less spectacularly, compliance with sensible and adequate rules has increased exponentially. The politically desired greater level of protection in private-law relationships contrasts with a loss of legal certainty. At any rate, the functional logic of algorithms could have positive consequences if the legislature were forced to differentiate more strictly than before between prohibitions which are absolute and those which are linked to sensible benchmarks. The development of black lists in fair trading law and the law of general terms and conditions, as well as the prohibitions of discrimination, which are absolute, bear witness to the possible developments which modern consumer legislation might undergo.[199] Even if it were possible to shift the focus of consumer law, we would still be left with many rules where the standards themselves leave considerable scope for interpretation on account of being formulated in the style of general clauses. As well as considerable doubts as to how complex legal realities can be processed, the criticism raised against the feasibility of implementing the law in algorithms is above all directed against the fact that it is hardly conceivable how general clauses are to be translated into a mathematical programming language.

The Advisory Council notes that it will not be possible to regulate algorithms using the means and technologies available for regulating industrial products.

5. Re the deficits and consequences of a reactive approach

In reality, control is currently being exercised purely *reactively*. Enterprises in the digital economy use the freedom afforded by liberal market economies to define algorithms independently. To what extent existing algorithms comply with the requirements of applicable consumer law and of anti-discrimination law, to name just two legal fields, is currently largely not subject to any ex post factum control of whatever shape or form. The reason is simple: Potential illegal results can only be identified by the respective addressee, and that only theoretically.

If one nevertheless wanted to advocate purely ex-post controls, then there would be two prerequisites: (1) a digital agency which has the requisite technical and legal resources to be able to check whether the technology is compatible with the law and (2) an obligation to disclose the algorithm with all its autonomous modifications to a closed circle of government controllers.

[199] The report commissioned by the Advisory Council and submitted by Rott (op. cit., fn. 157) adopts the same approach.

The need for a digital agency entirely independently of the existence of a law of algorithms is addressed elsewhere.[200] Letting things go on as before and trusting in the self-responsibility of business and the self-regulatory power of competition without an obligation to register and without the obligation to disclose algorithms is at any rate not a serious option. In view of the current pace of social change, not only in the world of business, and its potential impact on human beings, a purely reactive political approach is not an option.

The Advisory Council is convinced that sticking to "business as usual" is, politically speaking, not a serious option. The political realm is called to drop the option of ex-post controls, the de facto approach, and to look for a regulation which does justice to the specific features of algorithms.

6. Re the limited possibilities of co-regulation

Attempts to link governmental and private regulation can be found along the spectrum between the two extremes of pre-market and post-market controls. All these considerations are, tacitly, based on the idea that it will be possible to get a handle on algorithms in the same was as it was possible to get a grip on the health and safety risks posed by consumer goods on the one hand and the machines and technology used in the production of goods on the other.

Gerald Spindler and Christian Thorun put forward a carefully elaborated proposal for co-regulation in a report they submitted to the registered society *Selbstregulierung Informationswirtschaft*.[201] The basic idea is that the (German) legislature should adopt framework legislation which sets out the minimum requirements as regards standard-setting (clear targets, participatory approach, decision-making, transparency, financing, standardisation organisation gets no copyright) as well as regarding enforcing those standards (binding commitment, monitoring, complaints mechanism, sanctions).[202]

Spindler/Thorun do not themselves address co-regulation so as to pick up on the risks of automated and self-learning algorithms by software agents. They test their proposal in four areas: data protection; unfair competition; IT security; liability law and telemedia law with civil law and ancillary areas (in particular consumer protection law). Without calling the potential of co-regulation in regard to the four areas into question from the outset, scepticism as to how the model proposed by *Spindler/Thorun* could be transferred to the regulation of algorithms nevertheless predominates.

Even the EU's attempts to take advantage of the tried and tested system of governmental framework-setting and private standard-setting for services by and large miss the mark. One could raise the objection that there is as yet no European legislation available for standardising services;[203] in addition, when it comes to the digital world, it is hard to see why the digital economy should agree to set voluntary standards which could go beyond general guidelines or even codes of practice. The digital economy is dynamic; new business models are constantly evolving which generally involve algorithms. However, standard-setting is a rather more static process. Private standard-setting tends to codify the past, at any rate in so far as standards describe products. If one takes the example of health apps,[204] the question arises of why companies providing these services should cooperate with each other, given

---

[200] See Part V.

[201] See <https://sriw.de/images/pdf/Spindler_Thorun-Eckpunkte_digitale_Ordnungspolitik_final.pdf> (last retrieved 28 Nov. 2016), since published as Spindler/Thorun, "Die Rolle der Ko-Regulierung in der Informationsgesellschaft: Handlungsempfehlung für eine digitale Ordnungspolitik", (2016), *MultiMedia und Recht Beilage*, Vol. 6, p.1–28.

[202] Busch's editorial in "Towards a 'New Approach' in European Consumer Law: Standardisation and Co-Regulation in the Digital Single Market", (2016), *Journal of European Consumer and Market Law*, Vol. 5, p. 197–232, p. 197 takes the same approach.

[203] Van Leeuwen, *European Standardisation of Services and its Impact on Private Law Paradoxes of Convergence*, (Bloomsbury 2017).

[204] Adam/Micklitz (op. cit., fn. 78).

that their main business purpose is to set themselves apart from potential competitors. The world of industrial products, by comparison, is reliant on standard-setting, because products would otherwise not be compatible with each other. This applies all the more since translating the law into the language of codes goes hand in hand with a very considerable level of investment in which there is above all a public interest.

The Advisory Council notes that the widely touted co-regulation in the form of government procedural framework-setting to regulate algorithms needs to be modified.

7. Re the need for an Algorithm Act

The Advisory Council feels there is an urgent need for political action in order to maintain consumers' autonomy and dignity in a digital world. The use of algorithms and the foreseeable developments as regards self-learning algorithms in a world which is becoming increasingly interconnected all affect deep-seated ethical principles of our communal life. It is up to politics in Germany to face up to this challenge. Leaving things to business as in the past is not a serious option, especially since the most innovative sectors of the economy are not based in Germany. That action needs to be taken now. In an ideal world, the forum in which an adequate solution would be sought would be the European Union or, perhaps better still, the OECD and the United Nations. The need to act cannot be postponed indefinitely.

The Advisory Council recommends

(1) putting in place the legal requirements to ensure that algorithms take account of the requirements of consumer law, data protection law, anti-discrimination law and digital security. In the case of algorithms which enter into direct contact with consumers, the underlying parameters need to be made transparent. Legal responsibility also needs to be assignable in the case of self-learning algorithms and applicable consumer protection regulations need to be complied with;

(2) ensuring that, based on standardised disclosure requirements, algorithms are disclosed to a circle of experts in the digital agency who carry out spot checks to see whether they are legally sound. Standardised software engineering procedures need to be developed to that end;

(3) that enterprises should also be called on to draw up a code of conduct on the use of personal data, AI systems and big data analysis.

8. Re the problem of competence

One conflict with the EU which is likely foreseeable is inherent to the General Data Protection Regulation, whose objective is full harmonisation. The above-cited rights to information and access under Articles 9, 13 and 15 of the Regulation do not justify a line of argument which the European Commission may put forward, namely that the Regulation leaves no room for enacting national legislation on algorithms. Article 40 of the Regulation and the concomitant Recital 72 go much further:

General Data Protection Regulation
Article 40
Codes of conduct

> *(1) The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.*

(2) Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:
(a) fair and transparent processing;

(…)
(5) Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.
(…)

(9) The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).
(…)

Recital 72: Profiling is subject to the rules of this Regulation governing the processing of personal data, such as ***the legal grounds for processing or data protection principles*** *[emphasis added]. The European Data Protection Board established by this Regulation (the 'Board') should be able to issue guidance in that context.*

In view of the general wording of Article 40 of the Regulation and of Recital 72, combined with the fact that the Regulation also covers mathematical and statistical profiling procedures, it does not seem so far-fetched that the Member States might have handed over competence for regulating legal matters relating to algorithms to the EU. That is, at any rate, true as regards the field of data protection. An Algorithm Act would, however, go way beyond formulating mere data protection principles. At its core, it has to address the economic and social order in a digital world, for which the EU does not have a mandate. The EU cannot interfere so far into the future of the Member States' economic and social order via the "backdoor" of data protection regulations and claim such wide-ranging competencies for itself.

Subject to more in-depth investigation, the Advisory Council believes that competence for drawing up an Algorithm Act has remained with the Member States, despite the objective of full harmonisation set out in the General Data Protection Regulation.

Part V Digital agency – institutional embedding, remit and competencies

The law of digital services has shortcomings which cannot be overcome using the existing institutional structure. The first problem is the legislature's lack of trust in consumers themselves, the second its lack of trust in the associations which are to rely on contract law, the law of general terms and conditions, and fair trading law to meet the challenges the digital world poses. The 2016 Consumer Law Conference[205] strongly substantiated the need to add a second pillar to the current system which relies on associations. The digital

205
<http://www.bmjv.de/DE/Ministerium/Veranstaltungen/Verbraucherrechtstage/Verbraucherrechtstage_node.html> (last retrieved 28 Nov. 2016).

economy was not the topic of the Conference, which instead dealt with possible shortcomings as regards the enforcement of rights and conclusions to be drawn from them. Given the current situation, it appears that consumer rights enforcement may be delegated to the Federal Cartel Office.[206]

Shortcomings as regards the enforcement of rights are exacerbated in the digital world, providing further justification for expanding the Federal Cartel Office. In the light of the role of software agents, regulation by code, big data and profiling, the focus will in the future above all be on what scientific skills shortages there are on the part of the government and which skills are needed to meet the challenges posed by AI.

I. Skills shortages and shortcomings as regards legal redress

Skills shortages and shortcomings as regards legal redress should be kept strictly separate. The government lacks experts with specific skills because there is no body in which the diverse activities of German ministries are pooled and systemised. Shortcomings as regards legal redress indicate the difficulties inherent to the digital world when it comes to asserting applicable law. From the consumer's perspective this above all concerns fair trading law, the law of general terms and conditions, and anti-discrimination law.

The scientific skills shortages which exist in this new world inhabited by software agents, self-learning algorithms, big data and profiling are obvious.[207] Essentially, it is necessary to build technical capacities by and with governmental agencies in order to put policy-makers in the position where they can be proactively involved in shaping further developments in the digital world. This will only succeed if they cooperate with the academic and business worlds. Drafting a law of algorithms is perhaps one of the biggest challenges of the next few years. However, there is still great uncertainty regarding developments in the world of AI and, above all, regarding the question of whether and possibly how programming languages and legal language can be dovetailed. The Advisory Council believes that policy-makers urgently need to act to overcome these shortcomings. There are foreign models which can be drawn upon. The Grand Coalition Government is recognisably willing to expand the Federal Cartel Office, and not only to restructure it into a consumer authority but also to incorporate legal issues raised in the digital world. This task will only succeed if the Federal Cartel Office addresses both the enforcement of rights and those questions which research has not yet been able to answer and also provides scientifically sound policy advice. The resources needed to do that must be made available.

Problems around rights enforcement make up the second big set of issues which are further exacerbated in the digital economy. The key points in question here are: circumventing existing rules, difficulties linked to rights enforcement in the digital world, individualisation of rights enforcement, the time lag between court decisions and problems which require an immediate remedy, and the often cross-border dimension of consumer problems which necessitates cooperation with institutions in other Member States.

Some business models in the digital world work are particularly successful online because they (can) circumvent analogue law. Robo-advisers evade the oversight of the Federal Financial Supervisory Authority; health apps do not provide the visual structures needed to check whether they comply with consumer protection law; and telemedicine projects often operate in a legal grey area. Wide-ranging competence for addressing such matters would help to close the regulatory gap. Rights enforcement in the digital world has become difficult: firstly, due to the deterritorialisation of law in the (globalised) Internet and, secondly, due to the possibility of using algorithms to seemingly individualise advertising, offers, prices and, ultimately, contracts – although that individualisation may be based on discrimination. This discrimination is not necessarily focused on any specific individual, but on a group of individuals with certain features defined by algorithms. These phenomena can only be

[206] *Frankfurter Allgemeine Zeitung*, 21 Nov. 2016.
[207] See Part IV.

brought to light (if at all) by a governmental body which can oblige enterprises to disclose data and supply information.

In view of the scale of the problems which the digital world raises, it will not be sufficient to place one's trust in consumers as before, that is consumers who individually assert their rights and sometimes spend many years fighting for their rights in court. The political weight of individual claims, even if they do lead to such spectacular successes as in the case of *Schrems*,[208] is of only limited relevance in specific instances and will not help consumers as a whole. Time lag is another issue. No courts have ever solved any burning issues.[209] Only very few of the platform business models have so far come into contact with governmental enforcement bodies (courts or authorities). One need only consider personalised advertising and/or personalised information.

Private consumer protection associations are not in a position to act as the sole bodies entitled to enforce rights in the same way as governmental authorities are, to whom enterprises are required to disclose information as part of these authorities' remits. Another difficulty is that, in the transnational context, governmental authorities are typically tasked with rights enforcement, they share information and cooperate.[210] The whole of EU law is tailored to consumer rights being enforced by authorities. Not only the sectoral authorities forcefully promoted by the EU in regulated markets but also the orientation to the cross-border enforcement of rights has led to the successive shifting of balance within existing competencies.

Conversely, involving platforms in alternative dispute resolution opens up legal redress options which only an authority can implement. As, in the medium term, all disputes will be handled via platforms, it is relatively easy to filter out who has filed a complaint, where they are from, what they are complaining about, the subject matter of and the reason for the dispute, whether it concerns incorrect information, incorrect education or incorrect advice, and who the opposing party is. This creates a data pool in which it would be possible to find out precisely and within seconds which bank, for example, receives the most complaints in which country generated by which consumers. Not only the competent institutions' dispute resolution mechanisms but their complaints mechanisms and complaints management can be digitalised. The Federal Financial Supervisory Authority can already generate electronic consumer complaints which can then be analysed in that way.[211] The Brazilian Ministry of Justice generates an electronic database based on complaints. Each year it publishes a ranking list of enterprises which react most swiftly or in the most consumer friendly manner.[212] In Germany and in Europe such models require compliance with data protection regulations, as well as with strict limits within which the responsibilities of "leading" enterprises can be listed. Data protection conflicts with efficient consumer protection. Although this is nothing new, in the age of digitalisation the problem takes on hitherto inconceivable dimensions.

A governmental authority which has the required digital skills and is actively involved in protecting collective consumer interests would be a decisive, key step which is well overdue in Germany. Two things need to be guaranteed: The availability of scientific expertise to answer the questions raised in the digital world, and the availability of sufficient powers which enable the governmental agency to prohibit certain practices and help consumers claim compensation. The EU's proposal for amending Regulation 2006/2004/EC offers key suggestions as regards the list of competencies required.

---

[208] Case C-362/14, Maximilian Schrems v. Data Protection Officer, EU:C:2015:650.
[209] Adam/Micklitz (op. cit., fn. 78).
[210] References for foreign models are cited in Part V, II.
[211] As regards banks, see <https://www.bafin.buergerservice-bund.de/bank.aspx> (last retrieved 20 Oct. 2016).
[212] <www.consumidor.gov.br> (last retrieved 20 Oct. 2016).

II. Foreign models

As far as can be seen, quite a few examples are available in the western world of what a digital agency could look like. Developments seem to have progressed furthest in the United States and in the United Kingdom.[213] What both countries have in common is that the matter was incorporated into existing supervisory bodies. As far as is known, no country has a digital agency which is an autonomous and separate authority.

In the United States, the matter falls within the remit of the Federal Trade Commission (FTC), which comprises three parts: the Bureau of Competition, the Bureau of Consumer Protection and the Bureau of Economics. The FTC is an independent authority with far-reaching investigatory and regulatory powers. Originally entrusted with overseeing competition, the FTC was also tasked with consumer protection issues as consumer policy has gained increasing importance over the past 60 years. The Bureau of Consumer Protection has eight divisions: the Division of Privacy and Identity Protection (which oversees the Children's Online Privacy Protection Act, among other legislation), the Division of Advertising Practices, the Division of Consumer and Business Education, the Division of Enforcement, the Division on Marketing Practices (which combats high-tech/Internet fraud, for example), the Division of Consumer Response and Operation, the Division of Financial Services and the Division of Litigation Technology and Analysis. The latter is relevant for our concerns, as it has a key role when it comes to investigating and dealing with consumer issues when the focus is on new technologies.[214] The department comprises seven units: the Digital Forensic Unit, the E-Discovery Unit, Forensic Accountants, Honors Paralegals, Mobile/Internet Lab, Office of Technology Research and Investigation, and Technology Planning.

The Office of Technology Research and Investigation (OTech) was created in 2015 as the successor to the FTC's Mobile Technology Unit (MTU), which dealt with consumer issues against the backdrop of the explosive growth in mobile phone use. The MTU launched a number of studies, including ones on mobile shopping,[215] health apps[216] and "mobile cramming", that is the practice of charging services to mobile phone bills which have not been ordered.[217] OTech has been placed on a broader footing and is to be used to raise the FTC's consumer profile. That is to be achieved by providing expertise on data security, smart cars, smart homes, transparency of algorithms, new payment methods, big data and the Internet of Things.[218] OTech provides the FTC with technical expertise, it identifies and structures relevant research projects, and develops new consumer research methods.[219] Thus, OTech acts in an advisory capacity within the FTC. It supports the FTC in regard to its remit of investigating relevant issues and preparing measures for regulating the digital economy. So far, OTech has restricted itself to the scientific treatment of relevant fields of digitalisation.

---

[213] For a basic analysis of tasks, see Rott, *Rechtsvergleichende Aspekte der behördlichen Durchsetzung von Verbraucherschutz*, Report commissioned by the Federal Ministry of Justice and Consumer Protection, file no. V B1-7008-3-3-52 24/2016.

[214] <https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-litigation-technology> (last retrieved 24 Nov. 2016).

[215] <https://www.ftc.gov/system/files/documents/reports/whats-deal-federal-trade-commission-study-mobile-shopping-apps-august-2014/140801mobileshoppingapps.pdf> (last retrieved 24 Nov. 2016).

[216] The most recent guidelines were adopted by the FTC's OTech together with the Department of Health and Human Services' Office of National Coordinator for Health Information Technology, Office for Civil Rights, and the Food and Drug Administration <https://www.ftc.gov/news-events/press-releases/2016/04/ftc-releases-new-guidance-developers-mobile-health-apps> (last retrieved 24 Nov. 2016).

[217] <https://www.ftc.gov/news-events/press-releases/2014/07/ftc-recommends-mobile-industry-changes-combat-mobile-cramming> (last retrieved 24 Nov. 2016).

[218] <https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/office-technology-research-investigation> (last retrieved 24 Nov. 2016).

[219] <https://www.ftc.gov/news-events/blogs/techftc/2015/03/booting-new-research-office-ftc> (last retrieved 24 Nov. 2016).

In the UK the issue falls within the remit of the Competitions and Markets Authority (CMA), which was established in 2014 following the merger of two previously separate institutions, the Office of Fair Trading (which was responsible for monitoring unfair advertising and terms and conditions) and the Competition Commission. The CMA employs 700 people and has offices in Scotland, Wales and Northern Ireland. It has six divisions: the Corporate Services Directorate, the Market and Mergers Directorate, the Enforcement Directorate, Legal Service, Policy and International, and Economic Adviser. Just like the FTC, the CMA also has wide-ranging investigatory and regulatory powers. The focus is less on regulation than on what is known as its policy of the "light touch", which means that interference with the business world is to be restricted to the absolute minimum where possible.[220] In this spirit, the CMA has drawn up a series of guidelines, commentaries and opinions on the digital economy. The current focus is on what is known as open banking, based on the revised EU Payment Services Directive. The aim of open banking is to enable customers to share their data with new service providers so as to make it easier and simpler for customers to administer their accounts.[221] The CMA is planning projects on online interviews, data use and price comparison websites in 2016 and 2017, all guided by the attempt to bring the advantages for consumers into line with those for enterprises.[222]

In 2013 the Netherlands combined three previously independent authorities into one: the Competition Authority (NMA), the Post und Telecommunication Authority (OPTA) and the Consumer Authority (CA). The newly established Authority for Consumers & Markets (ACM) is an independent authority with wide-ranging investigatory and control powers. It employs more than 500 people and comprises seven departments which essentially still strongly reflect the originally independent authorities: the Consumer Department, Energy Department, Telecommunication, Transport and Postal Services Department, Competition Department, Legal Department, Corporate Services Department and the Health Care Taskforce. Factual and legal issues are allocated on the basis of institutional linkages to the former OPTA. The equivalent in Germany would be if it were decided to combine the Federal Network Agency with the Federal Cartel Office. The Transport und Postal Services Department deals with all the issues around the Internet, mobile phones, TV, radio and postal services, especially including what is defined in this report as the law of digital services.[223]

What conclusions can be drawn from these foreign models when it comes to establishing a digital agency in Germany? Basically, a model developed in one country cannot readily be transferred to another. Each country has its very own history and has developed its very own understanding of what role and function governmental authorities have when it comes to regulating the economy. After the Second World War, Germany created a cartel office in the course of restructuring its economy and – unlike in the three countries mentioned in the above – its remit was not expanded to include consumer protection. The necessary consequence of the decision to have associations in charge of controlling advertising practices and terms and conditions was that it is only they which are responsible for legal redress. Since they are private civil-society organisations, consumer associations cannot be assigned investigatory powers.

By expanding the Federal Cartel Office into a consumer authority, Germany would be taking a long-overdue step, at any rate if one takes the other EU Member States or the United States as the benchmark. That would, in particular, apply to the institutional linking of cartel law and consumer law. However, as far as the digital economy is concerned, it is even more

[220] See Rott, *Rechtsvergleichende Aspekte der behördlichen Durchsetzung von Verbraucherschutz*, Report commissioned by the Federal Ministry of Justice and Consumer Protection, file no. V B1-7008-3-3-52 24/2016.
[221] For details, see Oehler, *Digitale Welt und Finanzen. Formen des Crowdfunding: Handlungsbedarf für die Verbraucherpolitik*, SVRV report, http://www.svr-verbraucherfragen.de/wp-content/uploads/2016/10/Digitale-Welt-und-Finanzen_Crowdfunding.pdf.
[222] <https://www.gov.uk/government/consultations/competition-and-markets-authority-annual-plan-2016-to-2017> (last retrieved 24 Nov. 2016).
[223] <http://wetten.overheid.nl/BWBR0020586/2016-08-11#Hoofdstuk1> (last retrieved 24 Nov. 2016).

important than in the analogue economy to note that shortcomings are divided into skills shortages and shortcomings as regards legal redress, as diagnosed in the above. Compared to the United States, the UK and the Netherlands, Germany and German authorities have not evolved any comparable practice of drawing up scientifically founded opinions, commentaries and recommendations on individual consumer law issues. This appears to be changing in the course of the spread of digital technology in particular, as the cooperation between the Federal Ministry for Economic Affairs and Energy and the Federal Ministry of Justice and Consumer Protection on platforms shows. The market watchdog for the digital world and the watchdog for the financial market, which are funded by the Federal Ministry of Justice and Consumer Protection, also suggest this is the case. The watchdogs monitor the market, record and empirically evaluate consumer complaints, analyse them and point out systemic errors in the market by means of targeted scientifically based studies, for example. They inform the competent supervisory authorities – such as the Federal Financial Supervisory Authority and the Federal Network Agency – as well as the general public of their results at an early stage.[224] However, the market watchdogs will not be able to remedy those shortcomings which have been described in detail here on their own.

Should the Federal Cartel Office be restructured, then it must above all be ensured that the required expertise about the digital world is available, not only in order to be able to assert consumer rights in the digital economy, but also so as to be able to draw up expert reports on new issues and problems to support policy-makers in their decision-making. Much speaks in favour of creating a third pillar within the Federal Cartel Office or at any rate of creating a separate department. This would also have the advantage of it being possible to deal with questions concerning the digital economy in an interdisciplinary manner. At any rate, however, based on the US example a separate department should be created which can operate independently of the other two pillars (cartel law and consumer law). The UK and the Netherlands fall behind the United States in this regard. Beyond formal institutional independence, the comparison opens up the possibility of a further, noteworthy phenomenon which has less to do with the digitalisation of the economy and more to do with i-government. It is particularly noteworthy that in the Netherlands and the UK the CMA and the ACM respectively present themselves on the Internet less by means of organisational charts and competences as through people and their professional skills, especially when it comes to digitalisation.

III. Potential solutions as regards the need for a digital agency

The law of digital services contains a *problem as regards legal redress*. In the world of software agents, of regulation by code and big data, the primary problem is that competence is not concentrated in governmental agencies. The problems as regards legal redress when it comes to digital services can be countered by improving individual redress and restructuring the Federal Cartel Office into a consumer protection authority so as to strengthen collective redress. The Advisory Council has made proposals in this regard (see II. 7. re individual redress and II. 8. re collective redress). In order to be able to tackle the really big challenges posed by the digital world, AI, autonomous algorithms, regulation through the code, big data and profiling, a further, decisive political step needs to be taken, namely the establishment of a digital agency which is sufficiently equipped so that it can be expanded into a digital competence centre where discourses are channelled, bundled and actioned.

[224] For further information (in German) about these market watchdogs, see <http://www.marktwaechter.de/>.

The Federal Ministry of Justice and Consumer Protection and the Federal Ministry for Economic Affairs and Energy have adopted a clear position:[225]

> *Digital agency: Pooling consumer protection, competition and market rules. Economic and consumer policy need to keep pace both with digitalisation and with the dynamics of change. One important step is strong monitoring competence. The current fragmentation of competencies within supervisory authorities and above all the lack of competencies is of no help to any of the market players. When it comes to competition, market and consumer issues which concern digitalisation, we not only need a digital agenda but also a "digital agency". At least, though, the remits of existing authorities need to more precisely defined.*

The focus must be on expanding technical competence. Without competence there can be no regulation and no monitoring. Germany does not yet have such a competence centre. According to media reports, technical and regulatory competence is spread across several different ministries. The following questions thus arise as regards the establishment of a digital agency:

- Should the digital agency be institutionally independent or part of an existing institution? Should the tasks arising in the digital world be assigned to the Federal Cartel Office or should an independent authority be created into which data protection would be integrated? Is bundling competencies in a single ministry an option (based on the example of the European Commission, which has a separate ministry dedicated to the digital world and largely independent of business and consumers)?

- What competencies should the digital agency have? Investigative and advisory or regulatory too? If the latter is the case, should it also be given the competence to issue bans, impose sanctions, to itself set standards (like in the US) and to claim collective damages (like in the UK)?

- What should cooperation with consumer organisations look like when it comes to legal redress? Should the digital agency pass the results of its own investigations on to consumer associations upon their request if the agency does not itself plan to take any further steps? Should there be any cooperation with the market watchdog for the digital world and if so what form should it take?

- How can it be guaranteed that the digital agency exercises its powers independently, possibly based on the example of the Federal Commissioner for Data Protection and Freedom of Information?

1. Re the need for immediate political action

The Netherlands, the United Kingdom and the United States have already acted. They have incorporated digital competence centres into their available governmental competition and consumer protection monitoring agencies. A series of reports on dealing with current or long-term problems published after consulting with business and consumer representatives bear witness to the growing political commitment of these bodies. Depending on how they are structured, these authorities propose governmental measures, recommend relevant measures to the government and parliament, or adopt measures themselves. Germany is lagging behind in this regard. The disadvantages for the economy and for consumers are obvious and have been variously documented.

---

225 <https://www.bmjv.de/SharedDocs/Downloads/DE/Artikel/Ma%C3%9Fnahmenprogramm_BMJV_BMWi.pdf?__blob=publicationFile&v=2> (last retrieved 24 Nov. 2016).

It is obvious that political action is necessary. The decision to establish a digital agency, in whatever form, cannot be postponed. No ministry, no authority likes to relinquish competence. But that is exactly what needs to happen so as to first be able to join all forces and then find out what skills shortages exist. Some fundamental re-thinking is needed and a new administrative legal culture needs to be developed in which it is understood that the current fragmentation of competencies across the ministries and the lack of legal instruments for effective regulation is a matter which urgently needs remedying.

The Advisory Council recommends establishing a digital agency in which previous competencies linked to digital services are pooled and expanded.

2. Re institutional embedding of the digital agency

From the point of view of consumer protection, there are three options as far as the institutional embedding or integration of a digital agency is concerned: the Federal Cartel Office, the Federal Commissioner for Data Protection and Freedom of Information, or a separate, new authority.

In the course of liberalising its markets, the EU has massively promoted the establishment of authorities – to control and monitor telecommunications, energy and finances and to control consumer law only when it comes to cross-border redress. Germany created the Federal Network Agency and the Federal Financial Supervisory Authority, two authorities which, under pressure from EU law, incorporated the protection of collective consumer interests into their remit. Germany only acted to the extent that the EU imposed requirements. That is why the Federal Office for Motor Vehicles is under no obligation to protect consumer interests. Not even the scandal engulfing VW was sufficient to politically confirm a change to its remit. Should the German Government's plan, namely to assign the Federal Cartel Office competence for consumer protection, come to fruition, this would provide the option, for the first time, of firmly establishing official control of consumer protection law horizontally and not sectorally.

Taking such a perspective it at any rate from the point of view of consumer protection appears plausible that the entire complex of issues surrounding the digital economy should be assigned to the Federal Cartel Office. That would make it possible to tap into considerable synergies between the individual fields which would be lost if a separate authority were to be established for each task. In that case it would have to be ensured that as well as monitoring unfair advertising and terms and conditions the Federal Cartel Office would also be able to pursue infringements of the General Equal Treatment Act. Examples taken from the digital world show that this is a key problem area.

The other options appear more problematical by comparison. Establishing a separate authority may be easier to achieve, because that way all the ministries have to relinquish competencies in equal measure and these are then bundled in the new agency. However, this option could prove dysfunctional, because there would be no links to anti-trust law, to consumer law and to anti-discrimination law. The other option, blending data protection and digital tasks, appears even more difficult to implement politically, because the *Länder* are also involved in monitoring data protection. One option worth considering would be upgrading the Federal Network Agency, though in view of its broad-based competence for electricity, gas, telecommunications, post and railways this appears problematical.

The Advisory Council is in favour of assigning the Federal Cartel Office those tasks which are being considered as part of the digital agency's remit. This will ensure that those legal issues which the digital economy raises and which go together are not pulled apart on extraneous grounds.

3. Re the tasks and competencies of the digital agency

Assigning these tasks to the Federal Cartel Office would ensure that the available monitoring and control mechanisms could also be available to the digital economy. In the first instance that would mean redress mechanisms, to which the list of proposals for the reformed Regulation 2006/2004 would need to be added (see II. 8.).

There are skills shortages as regards those tasks which are upstream of legal redress. The digital agency must be given the possibility of investigating relevant sub-issues itself, of financing third-party research, drawing up proposals, discussing these with the involved sectors of the economy and consumers, drawing up codes of conduct and introducing concrete measures into the legislative process.

The Advisory Council recommends assigning all the necessary tasks to the digital agency and guaranteeing it the necessary resources so that it is in a position to proactively investigate technical and legal issues raised in the digital economy, to draw up proposals, discuss these in the public domain, develop codes of conduct with business and consumers, and to develop recommendations and proposals for the legislature.

4. Re the problem of competence

The Member States are *in principle* free to organise and shape legal redress as they see fit. That goes both for the question of whether enforcement of consumer law is to be placed in the hands of associations and the extent and reach of the competencies. But the scope for action is not unlimited. Legal redress must be based on the principle of effectiveness and equivalence developed by the ECJ. The diverse EU directives and regulations set institutional and procedural requirements which the Member States must comply with in their implementation.

More specifically, amalgamating the government agencies involved in regulating sectoral markets raises a problem which has now reached the ECJ: EU law obliges the Member States to establish independent agencies to control regulated markets (telecommunications, energy, finance and cross-border consumer protection). What exactly “independent” is supposed to mean and to what extent the independence required under the EU regulations and directives could be endangered as a consequence of authorities being amalgamated or tasks being merged will be based entirely on how that agency is institutionally embedded.

The Advisory Council recommends commissioning a legal expert opinion which addresses the question of the merging of German authorities to the extent that these are also required to implement tasks for which EU law sets legally binding institutional and procedural requirements.

SVRV Sachverständigenrat für Verbraucherfragen