



Protecting Consumer Protection Values in the Fourth Industrial Revolution

G. Howells^{1,2} 

Received: 2 May 2019 / Accepted: 2 September 2019 / Published online: 10 December 2019
© The Author(s) 2019

Abstract

We are entering into an era of new technological possibilities. Many benefits will be derived for consumers from the development of data and computer-driven innovation. We will have new products and services and new ways of making and supplying goods and services. Without wanting to inhibit innovation, this article calls for the legal system to remain committed to an ideology and legal framework that supports consumer protection. It will counsel against assuming that the law should give way unduly to the technology agenda, whilst accepting that adaptations should be made and also that there should be a critical review of whether traditional forms of regulation are needed in the Fourth Industrial Age.

Keywords Digitalization · Blockchain · Smart contract · Data · Consumer · Automated vehicles

Impact of Digitalization on Consumers

The Fourth Industrial Revolution

Digitalization is affecting the consumer market in ways that could not have been imagined a generation ago. We are in the midst of the Fourth Industrial Revolution that builds on the electronic and information technology of the Third Industrial Revolution in a way that combines technologies and blurs the distinctions between the physical, digital, and biological (Schwab 2016). The results are often positive. Products are being replaced by digital content: Vinyl records were loved by many and even retain a (growing) niche market, but most consumers take advantage of subscriptions to cloud services offering access to catalogues of music on demand on a scale that they could never afford to purchase. Traditional maps are increasingly being replaced by online App services available immediately via mobile phones. We use “free” messaging services such as Facebook and Instagram whose business model is

✉ G. Howells
Geraint.howells@manchester.ac.uk

¹ City University of Hong Kong, Kowloon, Hong Kong

² University of Manchester, Manchester, United Kingdom

driven by access to and exploitation of our personal data. The contractual process is even becoming smarter (i.e., automated). For instance, delivery of shopping may be triggered by a certain event such as stock running low in the refrigerator. Products are being reinvented: Autonomous vehicles may one day replace traditional manually controlled cars, but in the meantime, aspects of vehicles are becoming increasingly automated even if the driver retains ultimate control. The internet of things is upon us: One product can talk to another, so a mobile phone app may be able to control the thermostat on your central heating system. Even, the way products are made may be changing with consumers able to buy a disc containing the design instructions that is used to print a product at home using a 3D printer. The internet has allowed new platforms to develop to sell products and services. Potentially, these open up markets to global competition and allow small enterprises easier market access. Online platforms have also spawned new services, or more accurately new providers of services, which form part of the so-called sharing or gig-economy. These often involve new ways of doing traditional offline services (like taxis and renting rooms), but they are made possible by digital platforms that connect potential consumers with suppliers. It is even suggested that big data can allow for personalized contracts or even personalized legal rules that match individual needs and preferences and promote more efficient outcomes. Even legal tender is being supplemented by crypto-currencies – though it will be noted later that this is one development about which there may be reason to be sceptical.

Alongside all these positive developments, digitalization is provoking major disruptive effects in the consumer marketplace. This has impacted on traditional business models. Consumers are embracing the new opportunities, but some may also be feeling less secure as they grapple with new products and ways of purchasing. The important contribution of this article is to stress that technological innovation need not necessarily disrupt the extant legal regime of consumer protection (Twigg-Flesner 2016). There is a danger that lawyers play up the dramatic impact changes may have on the law to induce their clients to seek their legal services. It is also not unknown for academics to do the same in order to excite the interest of the academic community in their work. Nobody gets famous by saying things are not going to change much. Just think of the consultancy hours and papers written on the millennium bug and yet the clocked ticked over the millennium hour with almost no disturbance to the digital world.¹ Of course, the millennium might have triggered a major computing meltdown and so there was good reason to prepare for and consider the legal consequences. Equally, those who point to all the possible legal issues arising from the new consumer marketplace are performing a valuable service. There will certainly be the need for some adaptations to meet the needs of the digital environment. However, the argument is that it should not be necessary to undermine the gains made in consumer protection in order to have a vibrant and dynamic digital consumer marketplace. Many of the traditional consumer rules seem to be flexible enough to adapt to the innovation; at least, their core values can be maintained even if some technical adaptations are required. In some areas, the impact of digitalization may indeed throw a light on an aspect of the law that needs clarification. Equally, there may be a few areas where significant changes may be needed if the new business models are to flourish. The situations where the gains from digitalization justify sacrificing core consumer values are likely to be fairly limited, as enhancements can often be made that align with traditional core values. This is evident from the REFIT project and the reforms in the anticipated Consumer Law Enforcement and

¹ One rare example of a problem is said to be a radiation equipment failure in the Ishikawa nuclear energy facility in Japan, but backup procedures were effective.

Modernisation Directive.² In any event, technology is evolving and it may not be wise to meet every demand for legal reform or deregulation as it arises before the technology settles down or the law develops solutions. There should be a high threshold premised on consumer welfare gains if consumer law protection is to be sacrificed as core consumer values are accepted as self-evident conditions within Europe for a healthy market economy.

There are other areas of the Fourth Industrial Revolution, especially where bio-technology is involved, that impact on consumers and undoubtedly will pose new ethical challenges to society. Many of these developments will challenge traditional regulation and legal rules and may require different regulatory solutions (Brownsword 2008; Brownsword and Yeung 2008). Digital means of communication and distribution might make protection of intellectual property rights and enforcement of obscenity laws more challenging. Admittedly, there may also be data protection issues that need specific regulation for the digital era (see Swire and Litan 1998), but even with data protection, it should in many instances be possible to use the general principles in a way that achieves acceptable outcomes. The regulation of cookies is one example of a novel issue thrown up by digitalization that the law has addressed.

Particularly when health or ethical issues are at stake, a difficult balance may need to be struck between exercising the precautionary principle so that consumers are not exposed unduly to risks when there remains uncertainty about technological developments and the desire to promote innovation. In some instances, regulatory sandpits may be needed to provide for experimentation: Though these are more justified in relation to financial product innovation than when health or moral ethical issues are at stake.

Maintaining Core Consumer Values

My thesis is simple and yet surprisingly to some people it may be controversial. The Fourth Industrial Revolution is unlikely to require radical regulatory and legal overhaul for the majority of mainstream consumer transactions. Consumer protection in the Fourth Industrial Revolution poses less significant risks or ethical challenges than in fields such as bio-technology. Enforcement may be more complex, especially where pure digital content is involved, but there are usually means to enforce rules as the digital and bricks and mortar need to interface and in particular payment methods can be used as a gatekeeper. In the mainstream consumer market, the same types of transactions are taking place online and offline. The same fundamental issues are at stake and the same responses are justified. Core consumer values should be maintained.

Europe has developed an extensive range of consumer protection measures based on some core values (Howells et al. 2017a) As the consumer market evolves in the Fourth Industrial Age, consumers will have the same basic needs that have influenced the development within Europe of core consumer protection values. These include informing consumers in a transparent manner, fairness in marketing practices and contractual terms, protecting reasonable expectations of quality and safety, effective market surveillance and enforcement, and providing clear accessible routes to redress. Indeed, the conclusion of the REFIT Fitness Check report was that the core horizontal consumer law directives remained essentially fit for purpose even in the era of digitalization (Commission Staff Working Document 2017), whilst the

² A compromise text was agreed between the Council and Parliament, which was subsequently endorsed by Parliament by plenary vote in April 2019. At the time of finalizing this paper, the Council had yet to schedule its vote.

evaluation of the Consumer Rights Directive suggested extending it to digital services contracts, clarifying how it applied to digital content contracts and introducing new transparency requirements for online intermediaries (European Commission 2017a). Transparency has become a key core value. Consumers have been granted rights to information and expect not to be misled, including by omissions. Consumers will continue to expect to be well informed and technology may even enhance the capacity to achieve this. New actors such as platforms may need new solutions, but these can be in line with the traditional core values. The transparency requirement has been strengthened by the Unfair Contract Terms Directive being interpreted to require that consumers can understand the terms.³ Any moves to smart digitalized contracts should not be allowed to undermine this core value of transparency. Consumers will still not want to be subjected to unfair commercial practices – which may take new forms in the digital environment. Both the Consumer Rights Directive and Unfair Commercial Practices Directives are due to be amended to take the digital environment into account. Both the particular rights, such as the right of withdrawal, and more general controls can be adapted to the digital environment. There will be the same demand for assurances that unfair contractual terms that create a significant imbalance in their rights cannot be imposed on them. This may be even more important if digital contract terms become longer and harder to find online. In addition to transparency, fair marketing practices, and contract terms, consumer law has created the expectation that goods are guaranteed to meet some basic quality and safety standards. The legal baseline quality standards have been fairly easily adapted to cover digital content and services. Also, whilst new forms of products relying on artificial intelligence (AI) or new 3D printing techniques may test the rules of product liability, it is believed that there are the tools for resolving the challenges thrown up within the existing law. It may be that some concepts need to be clarified, but these have already been subject to discussion even before the advent of the Fourth Industrial Age. Issues that come to mind are whether software should be treated as a product and who should be excluded from liability as they are only hobbyists. The digital revolution might focus attention on these issues, but in truth, they were crying out for review in any event. What should not be permitted is a blanket exemption from traditional consumer law just to aid innovation. Innovative industries have been able to prosper notwithstanding product liability. It is true that the advent of platforms creates a new actor that has to be factored into the legal regime, but often the traditional rules can be applied or extensions made in line with core values. The sharing economy does challenge some forms of public regulation. Again, these might in any event have been worthy of review. They should not, however, be deregulation simply to facilitate new trading models unless there is convincing evidence of consumer welfare gains. Access to justice will remain a priority and there will be increased anxiety that traders should be accountable even if they are less easily physically detectable. This paper seeks to isolate the impact of digitalization on this area of consumer protection law and be a calm voice promoting the need to maintain as far as possible the consumer protection regime that in Europe has been hard won over the last half century.

A distinction in the literature has been drawn between “coherentism” (that seeks to promote consistency by clarifying concepts, removing inconsistency and filling gaps whilst remaining loyal to the existing regimes) and “regulatory instrumentalism” that seeks to achieve specific policy goals and is therefore less concerned with preserving the coherency of the existing law

³ *RWE Vertrieb AG v Verbraucherzentrale Nordrhein-Westfalen eV*, Case 92/11, EU:C:2013:180;[2013] 3 WLUK 596;[2013] 3 C.M.L.R. 10 and *Kásler v OTP Jelzálogbank Zrt* EU:C:2014:282;[2014] 2 All E.R. (Comm) 443.

(Brownsword 2017; Rubin 2017). As the same consumer policy goals remain valid, it is not surprising that someone concerned with maintaining consumer protection would naturally be inclined towards coherentism (Twigg-Flesner 2018). These rules provide an island of certainty for consumers that gives them the confidence to engage in a dynamic consumer digital market. Consumer law is thus a means of strengthening the market.

This support for the existing regime is not intended to suggest the current consumer law regime is perfect. The EU probably represents the most protective regime, but it could still be improved. This belief that for the most part the existing regime should be retained and its core values applied to the digital marketplace does not ignore the need for possible adaptation to ensure the laws can apply in a technologically neutral way. Measures such as the E-Commerce Directive⁴ and the UNCITRAL Model Law on Electronic Contracting⁵ and Convention on the Use of Electronic Communications in International Contracts 2005 show how simple adaptations can make the law fit for technologically neutral applications. It also does not mean that there might not be some areas where new market factors call for new regulatory-instrumentalist solutions – platform liability comes to mind. Likewise, when it comes to the public regulation of contracts in particular sectors, it has already been noted that there may be cases in which the sharing economy should prompt a review of existing regulatory policy.⁶ Such a review will often be required because the traditional regulation is outdated. Indeed, it is the poor unreformed rules that cause the digital world to be used as a means of avoid them: Often, these are instances where the rules have lost the support of the community (Murray 2011).

However, the core values of consumer protection remain relevant. In any event, many of the consumer law principles are sufficiently flexible to be capable of being applied sensitively to meet the needs of the new digital environment. This allows oversight by the law without rushing with undue haste to provide specific regulation when regulators may lack the necessary expertise. Equally, as technology moves at speed, regulating for specific problems may produce solutions that soon become dated. For example, to adapt contract law models to the blockchain may not make sense if the blockchain is itself replaced or evolves to take on new forms. History teaches us that industry and law normally manage to come to an accommodation that facilitates healthy societal developments, whilst retaining traditional legal principles.

Relationship Between Law and Technology

The assumption of some technologists is that because something is technologically possible it should be allowed. This view is challenged: the law cannot just be wished away (Zetzsche et al. 2018). Technologists tend to dislike law and lawyers: the law is seen as an obstacle preventing them doing what they see as valuable. Lawyers are thought not to understand their technology clients sufficiently, to over-lawyer to rack up large numbers of expensive billable

⁴ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market: OJ 2000 L178/1.

⁵ UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998.

⁶ In similar fashion, Grundmann and Hacker distinguish the regulatory framework from the private law rules governing digital content as the object of the contract or the use of digital technology in various procedures during the life-cycle of the contract (Grundmann and Hacker 2018).

hours and be deal-breakers rather than the providers of creative solutions (Walker 2010). Many of the early internet pioneers had a distrust of the establishment and the state that was exacerbated with the financial crisis. The early suggestions that cyberspace was a potentially lawless “wild west” space incapable of being governed by traditional legal means (Johnson and Post 1996) has given way to an appreciation that as the digital world needs to interact with the bricks and mortar world it is capable of regulation (Goldsmith 1998; Goldsmith and Wu 2006); even if locating businesses and securing enforcement across borders might be more complex. It remains, however, fashionable to suggest that the law may need to accommodate other forms of technology driven regulation more suited to the digital world (Lessig 2006; Reidenberg 1998). For instance, privacy might be best protected by programmes that ensure sites' policies match consumer preferences (i.e., Riverbed, Privacy Badger, uBlock Origin and Ghostery and the early example of P3P). Reviews on websites are increasingly viewed as being particularly powerful forms of reputational signalling (Busch 2016).

These forms of “code” and soft law may be a form of regulation (Lessig 2006), but they are not the law. Law must always trump Code; just as law must also trump the market or societal norms. Even if Code can be used to mitigate the impact of legal rules it cannot change the fundamental legal rules (Wu 2003). There are legal limits to what can be done by Code. Just because something can be commanded to be done by Code does not make it legal. There are lots of things that are done that are illegal in both the online and offline world. They remain illegal in both. If over time the law is too removed from societal values and market choices, this may undermine its strength and lead participants to find ways to avoid it (Murray 2011; Wu 2003). Code may, at a practical level, influence the choices open to consumers. It has the potential to enhance consumer choice by helping ensure consumer preferences are met, as with the privacy programmes that check sites accord with consumer preferences. Equally, it can limit the options available to consumers as traders will be able to use Code to guide the consumers towards a contract that accords with the trader's interests. This really differs only in degree to the limited choices offered consumers by standard form contracting. As the subject matter will rarely touch on sensitive issues, there is perhaps less need to be concerned by the lack of active choice in the consumer market than in other areas of life where legal regulation raises more ethical issues (Brownword 2008).

It should also be remembered that consumer protection legislation only imposed obligations on those acting in a commercial or professional capacity. Consumer laws rarely affect individuals who simply want to share ideas. It is the conduct of commercial activities that brings innovators within the scope of the regulatory regime. Once technologists have a profit-seeking motive, they can no longer disregard regulatory obligations (even if they are unprofitable in their early days). However, profit seeking can be a great incentive to innovation and so there remains a public interest in convincing technologists that law is good for them and their businesses. Here, one only has to go back to the famous example of Akerlof's market for lemons, to show how having basic consumer protection rules can give consumer's confidence to pay higher prices for assurances of quality (Akerlof 1970).

In any event, private law rules in contract and tort will, unless one wants to rewrite the basic tenets of the common law, continue to govern the supply of goods and services in the digital environment – even if specific rules are amended to facilitate the digital agenda (Katz 2015). We will not dwell on all these general principles beyond noting that they remain a kind of jack-in-the-box, which digital and technology firms may need to confront even if they manage to exclude themselves from specific consumer rules. For instance, it

would be hard to imagine a legal regime excluding negligence liability for digital suppliers or exempting online contracts from rules on undue influence or mistake.

Structure

A first point to consider is how the basic obligations and remedies under sales law have been reframed to apply to the supply of digital content. The United Kingdom's (UK) Consumer Rights Act 2015 and the EU Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services⁷ demonstrate how the same basic underlying core principles can be fairly easily adapted to the digital environment. There has been some adaptations to meet the digital environment and to adapt to the "life-time" nature of some digital contracts, but the same core values protecting reasonable expectations of quality and redress are found in the new regimes. Next, the use of data to access digital content and services is shown to have become widely accepted.

The examples of smart contracts, product liability and autonomous vehicles, and 3D printing are then used to illustrate how the core values of consumer protection law can and should be maintained. Certain adaptations may be necessary, but for the most part, this can be achieved by court made law developing the general principles in line with the digital context. These may bring disruption to the consumer marketplace, but the law seems capable of adapting to meet the changes.

One of the most important developments has been the development of platforms. This is an area in which a regulatory-instrumentalist approach may be justified. The platform is a new actor that has the potential to become a strategic gatekeeper offering the opportunity for new forms of protection. Platforms may be viewed as part of a connected network with those using the platform to supply goods and services. This may justify the platforms having some responsibility for what is supplied or at least their information obligations and the review and feedback services may need attention.

Platforms are often linked also to the rise of the "sharing" or "gig-economy." Developments such as the growth of Uber and AirBnB might cause us to question whether the traditional rules continue to serve an appropriate function. Very often, these debates will be at the level of public regulation rather than private law. However, any removal of regulation should be because we are convinced the rules are no longer needed to fulfil core consumer protection (or other social) values. The new actors may throw light on the existing regulatory rules being outdated. Some existing rules may even encourage anti-competitive behaviour. Societal conditions may have changed. The technology itself may remove the need for some regulation or allow its modification. However, what must be resisted is any suggestion that the law should change just in order to accommodate what is technologically possible where this risks undermining genuine consumer protection concerns.

We conclude by looking at two aspects about which the author is sceptical. The personalization of laws and contracts is seen as possible by embracing the power of big data, but seems to ignore the value of simplification in the field of consumer law and the limitations on the consumer's ability to value consumer rights when faced with attractive inducements – like lower prices. Digitalization of the supply of goods and services has been accompanied by the

⁷ OJ 2019 L136/1 (hereafter Digital Content Directive).

digitalization of payment methods with the development of crypto-currencies. These are discussed, but with some scepticism about their long term value in the consumer marketplace.

Digital Content

Digital content and digital services are ubiquitous. Many offline products are being replaced by digital products. Think of the demise of the CD or DVD in favour of streaming services giving a licence to access digital content. New markets like the gaming market have become multi-billion dollar global industries. However, there is a functional equivalence between these online and offline worlds.

The UK's Consumer Rights Act 2015 was innovative in seeking to create a distinct regime for digital contracts. These new rules were closely modelled on the rules for sale of goods. The EU has now adopted its Digital Content Directive, which is more tailored to the needs of digital content than the corresponding provisions of the Consumer Rights Act 2015, but is still based on traditional sales law principles. (Howells 2016; Lehmann 2016; Schulze 2016). This is a good example of the law seeking to maintain traditional consumer core values whilst adapting them to the digital context. Indeed, with the adoption of Directive 2019/771 on certain aspects concerning contracts for the sale of goods,⁸ there have been moves to make the rules on non-conformity similar for goods and digital content and services. Non-conformity in both cases, for example, is framed in terms of similar subjective and objective requirements, with some variations to reflect the particular features of physical goods and digital content. Also, the directives attempt to resolve the issue of which set of rules should apply when the supply involves both goods and digital content and services. Essentially, sale of goods law will apply when the digital content or service is incorporated or interconnected with the goods even if supplied by a third party. Where the digital goods are provided independently they are covered by the Digital Content and Services Directive. Any tangible medium serving exclusively as a carrier of the digital content is also covered by those rules. The Consumer Rights Act 2015 has had some bearing on the development of the Digital Content Directive, demonstrating how the interplay between UK and EU reforms has allowed member states the freedom to experiment so that experience can inform horizontal European legislation.

The Digital Content Directive would maintain the norm of conformity with the contract. It includes traditional matters such as quantity and quality, but adds on elements important in the digital environment. Thus, digital content and services should possess the functionality, interoperability, and other features as required by the supply contract and be supplied with updates as stipulated in the contract.⁹ In addition to these subjective requirements, they should also possess the qualities and performance features, including in relation to functionality, compatibility, accessibility, continuity, and security that are normal for digital content or services of the same type that the consumer could reasonably expect.¹⁰ Whereas goods need to comply with a sample or model, the same principle is adapted to the digital environment by making reference to compliance with a trial version or preview. Equally, just as goods can be non-conforming due to incorrect installation by a supplier, so in the digital context, lack of conformity can result from incorrect integration into the consumer's digital environment

⁸ OJ 2019 L136/28.

⁹ Art. 7.

¹⁰ Art. 8.

carried out by the supplier or due to shortcomings in the integration instructions provided to the consumer.¹¹ For goods, conformity is assessed at the time of supply. This is the same for digital content or services, where there is a single act of supply or series of individual acts of supply, but where the contract specifies the digital content or services will be supplied over a period of time the content must be in conformity throughout that period.¹² For digital content and services, the primary remedy is always cure. This is necessary because it is recognized that all digital goods may contain bugs that should not render them non-conforming so long as they are fixed. On the other hand, the obligations are made more extensive. The spot contract nature of goods contracts is replaced by a more relational contract that exists for the “life-time” of the goods (Nogler and Reifner 2014). Also, the burden of proof is reversed for 12 months for one off supplies of digital content and services, as is the case of goods under the new Directive,¹³ but for continuous supplies over a period of time, the burden of proving conformity is firmly placed on the supplier, unless the consumer fails to cooperate by providing necessary details about their digital environment.¹⁴ The life-time nature of the contract is also reflected in the rules that provide a balance by allowing the trader to modify the digital content or services, subject to certain conditions, but also allowing the consumer to terminate if the modification has more than a minor impact on their access to or use of the digital content or service.¹⁵

The remedies are also attuned to the digital context. The primary remedy is cure.¹⁶ However, unlike for goods, the specific remedies of repair and replacement are not mentioned. The trader has the freedom to decide how to do this and the recital mentions possible means being the issuing of updates or the making of a new copy.¹⁷

Price reduction or termination are allowed if cure is impossible or disproportionate, has failed, the defect reappears after cure, the trader refuses cure, or where the lack of conformity is of a serious nature. When termination is allowed, the consequences take account of the digital environment.¹⁸ Suppliers should stop using any content provided or created by the consumer, subject to certain exceptions for content with no utility outside the trader’s digital content or services or which only relates to the consumer’s use of such, or where it has been aggregated with other data and it would be require disproportionate efforts to disaggregate it or it was generated jointly with others who continue to use the service.¹⁹ Consumers should normally be able to retrieve any content provided other than their personal data after termination.²⁰ Traders may prevent further access to the digital content and service. Consumers should return digital content supplied on durable medium or when not supplied on a durable medium must refrain from using content or making it available to third parties.²¹

Sales law certainly needed some adaptation to apply to digital content. However, both the UK and EU reforms are consistent with the core consumer protection values established in the traditional consumer sale of goods context. The EU approach is to go into more detail and seems to represent the outcome of a dialogue that built on the UK reform. In fact, the result is a

¹¹ Art.9.

¹² Art. 11.

¹³ Directive 1999/44/EC on certain aspects of the sale of consumer goods and associated guarantees: art. 5(3).

¹⁴ Art.12.

¹⁵ Art. 19.

¹⁶ Art.14(1).

¹⁷ Recital 63.

¹⁸ Proposal, Art.13.

¹⁹ Art. 16(3).

²⁰ Art. 16(4).

²¹ Art. 17.

reinforcement of core consumer protection values as protection of reasonable expectations is now assured for digital content and services, and in particular, there is a welcome recognition of the life-time nature of some digital content and service contracts.

Data in Return for Access to Digital Content and Digital Services

Many important contracts nowadays involve consumers providing their data, rather than money, in return for access to digital content and digital services. Facebook is such a contract with which many people will be familiar. There is a tension between human rights concerns that personal data should not be a tradeable commodity based on moral arguments and an appreciation of the reality that many commercial services can only operate because of the value of the data collected (De Franceschi and Lehman 2015; Langhanke and Schmidt-Kessel 2015). This is so even if it is noted that personal data is a fundamental right that cannot be considered a commodity (Recital 24 of Digital Content Directive). It is nevertheless to be welcomed that in the common situation where consumers are given “free” access to digital content or services as long as they share their personal data, problems with that content or service should be governed by the same rights and remedies which apply where a consumer has paid for the digital content/service. The recognition of practical limits to the human rights argument against recognizing such arrangements supports the argument that consumer contracts raise less acute ethical issues than some other areas of technological development.

The UK Consumer Rights Act 2015 (CRA) introduced rules on contracts for digital content, but linked this to payment of a price (s.33(1) CRA). This excludes contracts where the consideration was the provision of data. Of course, analogous rights might be implied at common law, but it would certainly seem better to keep the law updated with social practice. Indeed, there is a power for the Secretary of State to extend the scope to other contracts for the supply of digital content to a consumer if satisfied there is significant detriment to the consumer (s.33(5) CRA). The Digital Content Directive seems better in this respect. It provides in Art. 3(1) that it shall apply where the supplier supplies digital content to the consumer who “provides or undertakes to provide personal data to the trader” except where the data is exclusively processed to supply the digital content or service or to comply with legal requirements. The recitals also make it clear that the collection of meta data and simply exposing the consumer to advertisements are not covered (Recital 25) (De Franceschi and Lehman 2015; Metzger 2017; Zech 2016). The Consumer Rights Directive has been amended in a similar way to include supplies of digital content or services in return for the consumer providing data (Art. 3 (a)) The law has been easily extended to cover situations where the consumer supplies data in order to access digital content and services. What was seen as a major issue by some, in reality has become a non-problem.

Smart Contracts

What Are They?

There is much discussion about smart contracts. But what are they? How are they smart? Are they even contracts at all? This term typically refers to automated systems where the contract is executed automatically on the system being informed that a predetermined condition has been met. This might be because the other party indicates fulfilment of a condition such as by

providing proof of delivery or receipt of payment. Sometimes, there may be the need for third party input to prove that a condition has been fulfilled by an external event. A courier might indicate the goods have been received or there may be the need for proof of an external event, such as a change in stock market prices that triggers some set response. Blockchains use oracles to interact with the internet to determine these circumstances. Software is written so that when specific conditions are fulfilled a party will perform a contractual obligation. It is not just that the contract will be performed; in fact, the parties have no choice as to whether to perform: the contract will be performed automatically without human intervention. Unless pre-programmed to allow correction, the parties have bound themselves to fulfil their prior agreement.

A common platform for smart contracts is the Ethereum blockchain, but there is no need for blockchain to be used. A vending machine operates in the same way. A smart contract is actually a familiar concept to anyone who has bought a can of coke from a vending machine (Szabo 1997). The use of blockchain technology and distributed ledgers allows this concept to be used on a more complex scale without the need to involve intermediaries.

Thus, a lot of what is commonly referred to as smart contracts is in fact about the smart execution of the contract. Beyond using technology to automate performance, it is possible to use the blockchain to make an offer that is automatically accepted and executed when the required payment is made using digital currency (Durovic and Janssen 2019).

How Useful Are Smart Contracts?

Simple vs Complex Terms

There is nothing essentially different about such “smart contracts” (see Giancaspro 2017; Raskin 2017). Indeed, their adoption may be restricted due to some inherent limitations. They may not in practice be all that smart as they follow simple commands based on the if/then logic of computer programming. The utility of such systems (and presumably therefore the scale of their adoption) may be limited by the inability of computer programmes to deal with the complexity of sophisticated legal terms and concepts (such as reasonable commercial practices, good faith or standards relating to the quality of goods or services) that need to be assessed against rich and diverse factual scenarios (Savelyev 2016; Sklaroff 2017). Automated actions may be best restricted to simple parts of contracts where specific clearly identifiable tasks can be executed by computer commands. In many consumer contracts, this may comprise the bulk of the issues. Payment might, for instance, be made conditional on signing acceptance of delivery from a courier. More futuristically, a groceries delivery might be triggered from a “smart” refrigerator noticing supplies have been exhausted. Some consider blockchain collapses the distinction between agreement and execution (Diedrich 2016). However, all these actions can be viewed in many cases as merely the technical means to fulfil the contract, which is in fact based on a legal agreement distinct from the computer programme that executes the contract (Cheng 2016).

Automatic Enforcement vs Efficient Breach and Selective Enforcement

Automatic execution is seen by many as having the advantage of certainty and technologists in particular can be frustrated by the legal regulation surrounding their technological developments. Automatic execution challenges traditional legal practice. Normally, a contracting party

is free not to perform but will be liable to provide a remedy. Efficient breach is most common in commercial settings, but there may be circumstances when consumers would rather not perform the contract and pay damages instead. Could it be argued terms permitting self-execution are indicatively unfair as they are “excluding or hindering the consumer’s right to take legal action or exercise any other legal remedy?”²² Probably not as such terms could be considered justified in the overall analysis of the contract as not being contrary to good faith. They are essential if that type of contract is to be permitted. Moreover, the only right being removed is the right to break the contract. The freedom to breach contract efficiently is viewed as more important in common than civil law systems, but it hardly seems a serious risk to your freedom. You are only binding yourself in practice to perform what you have already agreed to perform in theory. However, the inability to exercise efficient breach is a potential practical disadvantage. Automatic execution means that the parties may be stuck with a non-economically efficient outcome where breaking a contract and paying damages would have increased overall welfare. Adjustment may be the best commercial solution when parties face a situation where one party might potentially breach the contract, but may not be possible or as attractive once a contract has been executed. This restriction may be a limiting factor on the commercial value of smart contracts (Savelyev 2016; Sklaroff 2017).

Application of Traditional Legal Rules

The normal rules of contract apply to smart contracts and can be relatively easily adapted to such contracts. For example, as regards formation, offer and acceptance must accord, consideration can be found, if necessary, in an act of performance (as under unilateral contracts) and it would be wrong to say there is no intention to create legal relations from the mere fact the contracts are premised on there being no need to call on the courts because the contract is self-executing (Durovic and Janssen 2019). Whether a smart contract can generate legally binding follow-on contracts is perhaps a more moot matter (Giancaspro 2017). Likewise, the law can handle questions of capacity. Minors may manage to enter into smart self-executing contracts, but the regulatory and private law controls will still kick in. Businesses not selling necessities will have to put in place age checking mechanisms. If an agreement is secured by duress or undue influence the fact performance is executed automatically cannot exclude the law. As emphasized before, the law cannot just be wished away (Zetsche et al. 2018).

Moreover, technologists misunderstand contract law if they believe that just because a contract is executed that means it is not susceptible to intervention by the law and courts. The ability to do something does not make it legal anymore in the online world that it does in the offline world. The law has long been used to dealing with the problems caused by executed contracts and unilateral contracts. Means will be found to achieve justice even when contracts have been illegally executed. Raskin differentiates between strong and soft smart contracts with the former having prohibitive costs of (Clack et al. 2016; Raskin 2017, p.310). Some transactions can easily be undone, such as money transfers, whereas if the goods have been used, altered, or modified this may be more difficult. However, this does not mean that redress is impossible. It may just be that the court remedy needs to be varied or made more flexible. Though, it is clear that correcting errors may be more difficult where contracts are not reversible and injunctions may not work if a programme is self-executing and unable to be

²² Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, annex 1(q): OJ 1993 L 95/29.

turned off (Giancaspro 2017). However, the law can find ways to do justice and damages are always the remedy of last resort to achieve a fair outcome. Damages (money) is the ultimate flexible remedy.

Raskin also gives the rather chilling example of how car loan companies are installing immobilisers and GPS systems so that if you are in default the car can be programmed not to start and can be easily recovered. There are clear risks to safety should the car stop automatically without warning, but there seems to be adequate safeguards to avoid this risk. It might be seen as heavy handed enforcement. Debtor protection laws should not be circumvented, but more effective enforcement procedures should not be objected to per se as ultimately this may help consumers if collection costs are reduced.

Do Smart Contracts Make the Environment More Unfair to Consumers?

It has been argued that the online world is more dangerous for consumers as they are placed at the mercy of technology that can be used to direct consumers to strike deals that impose detailed standard form contracts in a way that is not normal in the offline world (Brownsword 2018 citing Calo 2014; Lemley 2006). This risk is even more exaggerated with smart contracts where humans have less control. In making the case for more protection for online consumers, Brownsword also shows how the existing case law may not be not very protective in the offline world. In fact there are mixed signals. In *Aziz*,²³ the Court of Justice of the European Union said that a significant imbalance would lead to a finding of an unfair term if the seller or supplier could not have reasonably assumed the consumer would have agreed to the term in individual contract negotiations. This seems pro-consumer. But, dicta of Advocate-General Kokott²⁴ in *Aziz* and the decision of the majority of the UK's Supreme Court in *ParkingEye*²⁵ seem to suggest a more pro-business attitude of accepting that even significantly imbalanced terms can be rendered fair if the party imposing them has a legitimate interest in doing so. This tension between the consumer and the business approach to consumer protection seems to be the core struggle. Whilst some elements of online contracting may make it less likely that consumers actually read terms, this is irrelevant to the question of whether the consumer would have agreed to the terms if they had read them or whether the trader's perceived legitimate interests are relevant. In truth, unfair terms law proceed on the assumption that few consumers will read the terms. Terms may be more likely to be held unfair if they are not properly disclosed, but disclosure by and of itself should not save a term. Efforts seem better directed at securing an understanding of the consumer's need for protection in both the online and offline world rather than creating a bifurcated standard. The same unfairness standards can apply to smart contractual terms with due recognition being given to the circumstances of online contracting. The application of the rule rather than the anything inherent within the rule itself seems to be the barrier to improving consumer rights. The rule itself seems applicable to smart contracts like any other.

²³ *Aziz v Caixa d'Estalvis de Catalunya* (2013) Case C-415/11 EU:C:2013:164; [2013] 3 C.M.L.R. 5 Judgment para 68.

²⁴ *Ibid.*, Opinion Para 73.

²⁵ *Parking-Eye Ltd. v Beavis*, [2015] UKSC 67, [2016] AC 117.

Some of the rules on unfair terms will, however, be hard to apply if the contract is made up of purely computer code. How can code be plain and intelligible language for consumers, especially given the strict interpretation the Court of Justice of the European Union places on this requirement?²⁶ Technology should not undermine the fundamental consumer right to be properly informed. If traders want to develop ways of selling that rely on communications between computers, for instance, then the technology should be required to ensure that the code be interpreted and presented to the consumer in a textual form that can be the basis of an informed contract (Durovic and Janssen 2019). The natural language code had been said to be “preparatory to the actual contract” (Giancaspro 2017). The Code should be the servant of the contracting process. There are a number of programmes such as Qbit and Convert Binary that allow code to be translated into language and vice versa but the question is whether the translation meets the high standards of transparency and plain and intelligible language requirements normally imposed on consumer contracts. Any translation needs to be built into the contracting process in a manner that is easy for the consumer to access. Transparency is a core value of consumer law and should not be sacrificed, but it seems technology can be developed to ensure that elements of the contract that rely on code are converted to text consumers can understand. Smart execution of a contract need not in any event prevent the original contract meeting traditional standards.

Smart contracts may become more common and can facilitate contracting processes and contractual enforcement. However, they do not seem to require any fundamental change in the law. Whether they will become widely used remains to be seen. They may not suit all situations. There may be commercial advantage to allowing efficient breach and the ability selectively to enforce breaches may be commercially desirable. Smart contracts are only suitable when the terms are uncomplicated. Compliance with open textured statutory standards, such as satisfactory quality, cannot be coded. Moreover, leaving some discretion based on linguistic ambiguity by using terms like “reasonable efforts” and “good faith” may be desirable. Smart contracts also require a great deal of upfront costs for legal drafting, which may limit their take-up.

Product Liability, Autonomous Vehicles, Internet of Things and Artificial Intelligence

Product Liability

The EU introduced strict product liability to ensure a “fair apportionment of the risks inherent in modern technological production.”²⁷ There would seem therefore to be no better arena to play out that need to apportion risk than in the brave new world of automated cars, the internet of things (where products communicate instructions to one another) and robots with artificial intelligence potentially self-learning how best to perform their tasks. Moreover, as products like automated vehicles have strong network

²⁶ *RWE Vertrieb AG v Verbraucherzentrale Nordrhein-Westfalen eV*, Case 92/11, EU:C:2013:180; [2013] 3 WLUK 596; [2013] 3 C.M.L.R. 10 and *Kásler v OTP Jelzálogbank Zrt* EU:C:2014:282; [2014] 2 All E.R. (Comm) 443.

²⁷ Recital 2.

effects, as they need to be widely taken up, suppliers might be tempted to rush to the market to gain a dominant position. Product liability can serve as a counterbalance promoting responsible trading. Many innovative and high risk industries have lobbied for special treatment under product liability laws, but all have managed to work within the product liability rules without undue hindrance. There may be some difficult cases thrown up by the new generation of AI and interconnected products, but the general core value of European product liability law seems as relevant to them as to other complex products like cutting edge pharmaceuticals.

The EU appears relaxed about the need to update its laws and believes its product liability law is capable of adapting to the new challenges (European Commission 2018a, 2018b). That does not mean some concepts might not need to be reconsidered. For instance, clarification might be necessary as to whether “product” covers software and whether services are included if provided with a product (on which the laws of member states differ). The trend seems to favour including software and treating packages of goods and services in a way that promotes consumer protection. The concept of producer may be challenged by developments like 3D printing and emerging new actors, such as platforms.

There are also questions around the concept of defect. As computer programmes always have bugs, this might impact on the expectations consumers have. Potentially, knowledge of the presence of bugs could dampen safety expectations, though whilst one might accept bugs as an annoying inevitable feature of programmes there might still be a reluctance to accept those that threaten personal safety. In any event the inevitability of bugs might bring into question the need for the EU Product Liability Directive to be revised to take account of post-marketing behaviour.

Are autonomously learned behaviours defects? Presumably the argument will be run that they are not defects as they were not present at the time of sale. The counter argument would be that the defect was the potential for risky behaviour to develop. This risk was known of when the choice was made to use AI and responsibility should be taken for what you place outside your control. It is like releasing a substance when you do not know how it will react. Any defect could be premised on the fact that such a scenario should have been taken into account in the design if liability was to be avoided by programming the AI device to avoid dangerous choices. EU Guidelines talk of building in procedures for humans to retain oversight and also having fall back plans as a safeguard (High-Level Expert Group on Artificial Intelligence 2019). Equally the risk of hackers intercepting communications between products in the world of the internet of things is a known risk. Adequate precautions should be taken to protect the product against hacking if it is not to be found defective.

The development risks defence would not seem to apply to unforeseen risks generated by AI. The defence only applies where the knowledge was not available to predict these evolutions. Although the particular choices as to future conduct made by AI may not have been contemplated, it should be sufficient to remove the defence that the risk of AI making wrong choices was known. Even if the particular risks were not known, the source of them was. The Court of Justice of the European Union (CJEU) approach suggests that once the means to discover a potential defect is known about it is for the producer to decide whether to continue marketing, do more research into the risk or accept any liability for the risk and perhaps use insurance to mitigate the impact. The risks of AI creating new risks seems one that should be internalised by the producer.²⁸

²⁸ *Commission v United Kingdom*, C-300/95 [1997] ECR I-2649.

There may also be a need to consider the scope of damages. Product liability is about safety and so mere breach of cybersecurity might not be enough, but if that breach had potential safety effects these should be considered. It is surprising that some regulators considered the doll, *My friend Cayla*, might not infringe the Toy Safety Directive (and in this context one might also consider the product liability directive) because security was not the same as safety.²⁹ The child was potentially endangered because you did not need physical contact with the doll to talk with it and a stranger in the street could therefore seek to entice the child outside by speaking through the doll. This lack of security does not seem to offer the safety expected. It could be rendered safe by adding a feature requiring the person communicating to have physical contact with the doll. The wording of the Directive seems capable of being interpreted in a way that allows for such a solution.

The above interpretations may be over optimistic. That may be why consumer groups are the ones favouring reforms, whilst the business community is more content to wait to see how the existing rules can be applied (European Commission 2018b). There may eventually be the need for some rule tweaking, but in many cases the wording of the Directive is open textured enough to allow appropriate solutions to be found in the context of concrete examples. However, the core value of protecting reasonable expectations of safety should not be forgotten. It is about apportioning risks caused by technological development. In fact, the Directive seems to have been prescient and to have been sufficiently future proof to allow it to be used as the basis for addressing the dynamic technological changes we are seeing to-day.

Automated Cars

Of all the developments in the consumer market, the rise of the automated car is perhaps the most discussed and futuristic. It offers the prospect of safer and cleaner driving, but also has raised the spectre of increased product liability litigation. The automated vehicle is more likely to be seen as the cause of accidents, whereas previously with traditional cars the driver was usually blamed for accidents (Anderson et al. 2018; Marchant and Lindor 2012; Villasenor 2014, 2012). It is inevitable that autonomous vehicles will be involved in accidents and at least some will be associated with errors related to the vehicle. Some manufacturers may be so confident in their products or want to stand behind their innovation that they will voluntarily accept liability. Volvo has taken this stance and Mercedes and Google have followed suit (Webb 2017, p. 45). The UK has also tried to deflect liability away from product liability to traditional motor insurance by making the insurer liable for harm caused by automated vehicles under the Automated and Electric Vehicles Act 2018 (Butcher and Edmonds 2018). However, this still leaves open the question of what liability, if any, the car should have. The UK Automated and Electric Vehicles Act 2018 allows the insurer to take a subrogation action against the driver or vehicle manufacturer. The expectation is that commercial practice will determine how liability is handled between insurer and manufacturer as manufacturers will have an incentive to reach a commercially sound practice in order to avoid their products becoming difficult to insure. No-fault solutions may be developed in order to promote confidence in this innovative form of transport that offers considerable potential benefits if it can become widely accepted (Evas 2018).

²⁹ For criticism of the doll from the Norwegian Consumer Council see <https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/>.

Even if traditional product liability rules apply, the results need not be revolutionary and the European Parliamentary Research Service has even recommended no change be made at this time (Evas 2018). The level of automation is ranked on a scale from No automation–driver assistance–partial automation–high automation–conditional automation–full automation (European Commission 2017b; SAE 2014). In the short term, the most likely use of automation is in features like automated warning and breaking systems when hazards are detected, parallel parking systems, and predictive maintenance. In many of these situations, the driver will remain responsible, just as a pilot is even when auto-pilot is engaged.³⁰ If the device malfunctions, the manufacturer may be responsible for the defect as with any other component. If liability can be traced back to the software component developer, their liability will turn on whether the software is a product. Regardless of whether software is currently to be treated as a product, in any event, a good case can be made out for including software within the product liability regime, just as digital content has been equated to goods (Howells et al. 2017b). This is an example of technology forcing us to modernise our laws to ensure the core values the law represents can best be reflected in the light of technological developments. However, it is at most an adaption of traditional rules which may already encompass software being viewed as a product, at least in some contexts.

Under the product liability directive, a product is defective “when it does not provide the safety which a person is entitled to expect.” The presentation of the product is a relevant factor. So, the liability may well turn on what the vehicle manufacturer claims for his product and in particular the extent to which it guarantees safety or expects the driver to retain responsibility.

If in the future, cars become fully automated, the liability of the manufacturer may become more important, and indeed the manufacturer may become a more natural target for litigation. If we ever get to the stage where children, the disabled or drunk persons can reasonably be transported alone in cars they cannot control, then, the car (and realistically that means its producer or seller) may be the natural defendant if an accident is caused by the vehicle (Gurney 2013). There will then be complex questions about what standard of safety is expected of the vehicle (Evas 2018). It should probably be at least as safe as a car driven by a human, but as it is claimed to promote safety a higher safety expectation might be reasonable. In assessing any higher standard, of course, the claims made by the manufacturer will be relevant. These are hard questions, but no more so than arise for many other products such as pharmaceuticals and medical devices where trade-offs between efficacy and side-effects have to be made regularly. The present definition of defect can be applied with as much ease (and as much difficulty) for autonomous cars as for many other products.

Currently, the time for assessing safety is when the product is put into circulation. In this context (as we noted for digital content), there may need to be an ongoing obligation to update materials and monitor the product. However, as there is currently no such ongoing duty (beyond negligence) it might be argued that, where the defect was caused by a change made by AI intelligence post-sale, the original product was not defective, but only became unsafe when the product morphed and created the risk due to the choices of the artificial intelligence. However, we have noted above why such products are likely to be held defective and the development risks defence is unlikely to be being available. Ultimately, if you put a potentially dangerous product into the environment, this seems a reasonable basis for imposing strict liability should that harm materialise.

³⁰ *Brouse v US*, 83 F. Supp. 373, 374 (N.D. Ohio 1949).

If the car is run by artificial intelligence tricky ethical questions might arise. Choices will need to be made as to how to engage with risks and programmes will be forced to make choices between potential victims. The classic example used is the dilemma posed by a runaway trolley and whether it should be diverted to save five lives at the expense of one person who would be certainly killed if the diverting action was taken (Huang 2015; Moolayil 2018). However, as absolute safety cannot be guaranteed, the best that can be expected is that the programme is based on a reasonable choice. It is a benefit to be able to make these choices rationally in advance, but that also makes us nervous as we have to face the sad consequences of conscious choices. Legal procedures might provide a framework for making these choices acceptable. Standardization might assist in determining whether the right assessment was made. The programming rules could then be subject to safe harbour rules so that there would be no criticism if the programme had been built according to societally agreed choices about rules of the road.

Whether there should still be liability in such circumstances depends upon the function of strict liability. The product would probably not be defective. However, the traditional rules provide the framework to resolve these challenging issues. It is not clear though that all the issues in play in relation to automated cars relate solely to product liability. The policy concern is really to deal with the effects of traffic accidents. Some countries like France already have no fault liability. The solution may be eventually to have a system of no-fault liability for autonomous vehicles and this has been floated in a policy document at the European level (Evas 2018).

3-D Printing

Technology may not only affect the nature of the things sold in the consumer market. 3-D printing can also affect how they are produced. This may in the long term lead to a revolution in the consumer market if goods can be printed on demand in the consumer's home and customised to meet their needs (Anderson 2014). It is likely to be a positive development, even if issues like printing of firearms raise matters of social concern (Curtis 2015).

The issues raised by 3-D printing are familiar ones (Engstrom 2013; Howells et al. 2019). If the 3-D printer is simply defective and produces rogue products or the defect lies in the substances used then liability is straightforward. It is more complicated if the defect originates in the CAD file. This engages the debate about whether software is a product so as to fall within the strict product liability regime. Whilst this may currently be a moot point, the trend is certainly to favour equating software with products at least, where it does more than merely provide information and affects actions (Ahleit 2001; Howells et al. 2019). As digital content is placed on the same footing as goods in the sales context, so this should be the case in product liability law. If considered necessary the law should be amended to clarify this point. This is an issue which has been uncertain for some time and increased digitalization has just made its clarification more urgent.

There are a separate set of issues relating to whom should be potentially liable. Where the consumer uses a commercial printer to print off products, the question is whether the printing company is merely providing a service or is supplying and taking responsibility for the final product. This is simply a modern variation on the old challenge of differentiating goods, work and materials and services contracts. Where printing services host a platform providing CAD files and printing service options the question of platform liability is again raised. This is discussed below.

There is one more legal conundrum posed by 3D printing that arises from the democratization of the manufacturing process. Those who post CAD files may well consider themselves hobbyists. The same might be said for small scale producers who print off products for a small circle of friends or members of a club. The divide between hobbyist and business can be a fine one, but in any event the EU strict product liability rules liability can only be avoided if no charge is made. This may cause us to reflect on these rules. A first reaction might be to promote the circulation of ideas and innovative products by restricting liability. But, equally, one should not forget the rationales that led to strict liability rules protecting consumers when products harm their physical well-being. The justification for channeling liability to an enterprise is based on its ability to absorb the loss. This is plainly not the position for most hobbyists. However, EU law rejected excluding artisan craftsmen from the scope of strict product liability. It is very hard to define where the line should be drawn between hobbyist and business. This is especially true online because if a product becomes popular it can quickly go viral. It may therefore be easier to have a bright line rule such as exists in the EU Product Liability Directive. Those seeking financial compensation must expect to face potential liability. This is part of a broader debate about the status of those participating in the sharing economy, discussed below. In any event, it should be remembered that anyone in the production process from CAD file designer to printer might be potentially liable in negligence.

However, it is not ideal for consumers to have to rely on hobbyist CAD file producers as they will frequently not have the resources or insurance cover to meet serious liabilities. Using platforms as a vehicle for channeling liability is a potentially attractive option. Platforms that are not involved in production themselves would like to equate themselves to a catalogue or shopping mall. However, they can be viewed as the element that provides commercial flavour to the sharing economy, which in an ideal world might be a more liberated social activity free from traditional commercial motives. This might be the justification for making platforms liable for problems encountered and this is discussed in more detail below.

Platforms and the Sharing Economy

The growth of the internet as a sales medium illustrates how the digital age has affected marketing and selling networks. A key development has been the growth of the platform economy, where a digital platform brings suppliers and consumers together. This is often associated with the growth of the “sharing” or “gig-economy.” Well-known examples relate to taxi rides (Uber), short-term accommodation (Airbnb), and handyman tasks (Taskrabbit).

A school of thought advocates these operators should be left free from pre-emptive regulation (Koopman et al. 2015). No one would want to strangle innovation unnecessarily at birth. However, if the need for good regulation is accepted, even innovative developments need to respect consumer protection values. Courts and regulators need to find practical solutions to ensure core consumer values are maintained. Only a few novel issues will require consideration of radical change at the level of core consumer protection rules, though in some sectors, public policy choices may need to be reconsidered.

Applying Traditional Rules

Core consumer rules will often be flexible enough to accommodate the new platform context; though occasionally, the rules may need to be tweaked in a technologically neutral manner.

The rules on information provision apply equally in the online world as in the offline world and in some ways technology makes it easier to provide the information. Indeed criticism can be heard about information overload and in particular about excessively long on-line contracts (Ben-Shahar 2009; Ben-Shahar and Schneider 2014). The challenge is often to make the information sufficiently prominent and litigation has ensued about the use of links to comply with information duties.³¹ Likewise, unfair commercial practices law has simply to be taken on board by platforms and applied appropriately (European Commission 2016, Section 5). One of the crucial issues is to decide whether the platform is only liable for the services it provides as an intermediary or if it becomes involved in and responsible for the provision of the underlying contract for goods or services supplied (European Commission 2016, Section 5.2; Hatzopoulous and Roma 2017). Data protection rules apply as in the offline world, although there is a need for particular rules to deal with cookies. The anticipated Consumer Law Enforcement and Modernisation Directive tries to clarify some of the information aspects related to platforms. For instance the platform should state whether the supplier is a trader and, if not, explain that EU consumer law rights do not apply. Also, it should explain how obligations are shared between the third party offering the goods, services or digital content and the provider of the online market place. Information should also be shared on the main parameters for any ranking and their relative importance. It will also be misleading to state reviews are submitted by consumers without taking reasonable and proportionate steps to check they originate from such consumers. One might quibble as to whether all the solutions are ideal: Should traders be able to rely on third party statements about their trader status? But the point is that general rules can apply and can be adapted as necessary without undermining the core values.

One particular challenge posed by platforms is that they facilitate the rise of a new category of actors who are individuals and become engaged in trade on an ad hoc basis. Just as “prosumers” are consumers who use technology to become more knowledgeable and influential in ensuring goods and services meet their need (Toffler 1980), so ironically, the platform allows people with less expertise than traditional traders to engage in production and selling – we might call them “conducers.” This new category has been said to raise a new regulatory challenge. In truth though there has always been a borderline between C-2-C and B-2-C contracts. Tests for drawing the borderline turn on the frequency of deals, the sophistication of the supplier, the size of the turnover, and any profit motivation. Many individuals may have inadvertently crossed the line and become a trader in the past—think of someone who collects and sells stamps regularly at collectors markets. It is just that more people may be dragged into the world of regulated trade via platforms. Indeed they may not be able easily to regulate how many sales are made once their digital content is posted on platforms. This may cause us to stop and reflect whether the right line has been drawn as to when suppliers become subject to consumer protection laws. However, we may ultimately decide the mere fact the digital environment is used is no reason by itself to amend the scope of protection. The consumer protection needs of someone seeking a ride in a taxi seem to be little different whether they called for the cab or found it on an app. Neither should lower standards be accepted because someone is part of the gig economy and only offering their services for a few hours a week. There is a clash between the desire to promote entrepreneurship (or for the more socially minded the sharing of resources in a responsible manner) and the need to ensure

³¹ Providing information by hypertext link was not found sufficient to comply with Distance Selling Directive: see *Content Services Ltd v. Bundesarbeitskammer*, EU:C:2012:419; [2012] 3 C.M.L.R. 34.

consumer protection. There may be legitimate questions asked (and discussed below) about the public policy choices made, but for now the point is that just because technology allows new entrants this should not *alone* be an excuse for lowering standards.

New Rules for Platforms?

The importance of online platforms has even made the EU consider a rare foray into the world of B-2-B contracts given the important gatekeeper role they have in providing access to the market (Twiggs-Flesner 2018, discussing Proposal for a Regulation on promoting fairness and transparency for business users of online intermediation services³²). The question of platform liability towards consumers also needs attention.

We have noted the recent reform would require the platform to explain the allocations of obligations. Should the law go further and impose substantive obligations on the platform? From the consumer protection perspective, platforms could be viewed as merely the equivalent to a shopping mall: one never expects the landlord to be liable for the goods sold in the shops. However, as platforms are the catalyst for commercialising the sharing economy, it might be questioned whether platforms should burden some responsibility. Platforms can go beyond brokering transactions and in some cases set down standards and impose prices; often, they are involved in collecting payment, arranging delivery, and complaints handling facilities. These features might lead one to question whether they should share liability. This would be a bold example of regulatory instrumentalism to achieve the specific policy goal of enhancing consumer protection. By promoting consumer confidence in the platforms, this can also engender consumer confidence in the smaller less well known businesses they might host.

Some analogies might be drawn with other situations in which third parties have to bear liability towards consumers. A comparison might be made with credit card provider's joint liability for the quality of goods and services bought using the card. Such financial service providers might be considered potentially liable as they are expected to check the quality of those recruited to the networks. They stand behind the traders that have access to their facilities. This is unrealistic though for some providers who are nevertheless subject to joint liability. Consider the complex international networks behind systems like Mastercard and Visa. The network member that issued the card may be many miles away from the supplier of the goods of whom it is unaware. It is the fact the creditors profit from the transaction and can spread the cost of liability that makes them an effective target. Chargeback is now a familiar consumer protection mechanism. The rationale for imposing "platform liability" could also be the same as for retailers under package travel contracts. They are responsible for the parties they coordinate (Busch et al. 2016). They may have deep pockets to spread the loss, but the justification for imposing liability is that by working with companies in a network situation they will be taken by consumers as providing an endorsement of the supplier. Platforms are well placed to spread the loss and also will have recruited those who sell through their platform. They can be the gatekeepers who have an incentive to ensure consumer protection is complied with (Murray 2011).

A blanket policy of making platforms liable for the suppliers they host may be too extreme for some. Perhaps platforms should be required to disclose whether they take any

³² COM(2018) 238 final.

responsibility for the suppliers they host? Nudging theory might suggest they be liable unless they prominently disclaim liability. Equally, even if joint liability is not accepted, platforms should have some responsibilities. For instance, information duties might be imposed or they might be placed under a duty to pass messages on between consumers and suppliers (Busch et al. 2016). At least, it seems reasonable they should be responsible for ensuring their review mechanisms are fair and transparent. They might also be expected to introduce complaints handling mechanisms.

Regulatory Choice and the Sharing Economy

Perhaps the most significant challenges for society related to the Fourth Industrial Revolution concern how to respond in public policy terms to the disruption brought about by the sharing economy. This is not so much concerned with the private law, but rather the regulatory framework surrounding the contract (Grundmann and Hacker 2018). There is a need to consider carefully whether the sharing economy requires and justifies changes to be made to the external public regulation. Deregulation just for the sake of promoting the sharing economy and platform providers does not seem justified. A business's desire to operate with a new model as part of the sharing economy obviously cannot by itself be a sufficient reason to dismantle regulation with legitimate policy objectives. On the other hand, some of the public regulation may strangle the attempts to develop sharing economy models that are seen as beneficial. The platform economy may in some sectors be a response to inappropriate and unwelcome regulation – what Wu describes as avoision of regulation (Wu 2003). This is most obviously alleged to be the case with taxis, where licencing systems have created markets that exclude competitors and impose high charges on consumers.

Generally, the new providers should be treated no differently from existing providers. Rules that simply frustrate their purpose for no good reason should be avoided. A rule simply banning taxi services using apps would not be defensible. Laws can be over-regulatory. One might recall the red flag rule that required a person to walk 60 yards in front of a locomotive vehicle carrying a flag.³³ This may have had a purpose: It was feared that horses might be scared by the new vehicles. However, it soon came to be seen as a hindrance to the valuable activity of driving a car at reasonable speed. It took 31 years to repeal the “red flag” law in the UK. Though the precautionary principle has a lot to commend it, in modern times it is unlikely that innovation will face such extreme barriers. The danger is actually in the opposite direction. The technology lobby and financial entrepreneurs will push for deregulation. Their voices will be heard by governments fighting to attract technology business in a globally competitive market for investment.

A choice may have to be made in each sector as to whether to maintain the existing public regulation and make the new platform providers comply with the traditional rules (which in some cases may affectively kill them off) or to adopt a new regulatory policy. Regulation should be reviewed to ensure it is as innovation-friendly as possible so long as the core values of consumer protection policy are respected. Reform might be desirable because the old regulation truly is outdated and can be dispensed with. A limit on the number of taxi licences might be one example of such a rule that might no longer be

³³ Locomotive Act 1865.

justifiable. It might be that technology fulfils a function previously met by regulation. An app might, for instance, enable tracking of who picked customers up on the street avoiding the need for a booking to be made through an office. In some cases the consumer benefit from new services provided by platforms may be so great that even some consumer protection norms might be justifiably sacrificed. This last situation is unlikely to arise every often. Even perceived benefits, such as the breaking of traditional markets by new entrants like Uber, may be short-lived if new dominant platforms emerge and mimic the previously preferred actors.

It is noticeable that in some areas, like crowdfunding, the need to adopt a regulatory framework for the new way of doing business has been readily accepted. The questions have been about the form it should take (Estevan de Quesada 2018). This may be because the commercial nature of crowdfunding is apparent; as are the risks of abuse. In “softer” more overtly consumer areas, like ride sharing and short term accommodation, regulation is more often portrayed as a barrier to innovation that threatens cheaper access to goods and services. This is sometimes wrapped up in a concern to promote a more social sharing dimension to the market.

However, there is a risk of underestimating the very real consumer concerns that exist. Two areas that have been affected greatly are taxis (by Uber) and short-term rentals (by Airbnb). There may be advantages in allowing individuals to rent out their spare room or allowing new entrants to challenge licenced taxi monopolies. However, there are also social implications. Taxi licencing may serve valuable functions to ensure cars are roadworthy and insured and drivers pose no risk to the public. Planning laws may ensure that residential neighbourhoods are distinct from those where commercial activity, including the letting out of rooms, takes place. One should be careful about relaxing rules unduly and losing legitimate forms of protection (Sundararajan 2016). This is particularly so as much of the sharing economy is in reality commercial in nature. There are models closer to a true sharing ideal, like Couchsurfing, where individuals may just want to share their facilities or some ride sharing firms that may genuinely only want to make more productive use of assets. However, many participants in the sharing economy are driven by similar profit motives to the traditional businesses models they compete with. Their existence may show the need to review existing controls, but they should not be able simply to avoid regulation that traditionally controls those activities.

National regulation has been protected by the CJEU decision³⁴ that Uber was a transport provider and therefore not allowed the market access freedom provided to intermediaries under the E-Commerce Directive.³⁵ In working out new models of regulation, there may be a need for a framework law, but account also needs to be taken of the fact the nature of goods and services offered by platforms varies dramatically (Katz 2015) and it will intrude into diverse national regulatory regimes (taxi regulations provide a good example of this). Therefore, there may be a need to allow for some variation between sectors and legal systems. Co-regulation is an option that might be used and has been popular with the EU (Finck 2017). However, the technology driven stakeholders should not be allowed to dominate the agenda and debates.

³⁴ *Asociación Profesional Élite Taxi v Uber Systems Spain SL*, C-434/15 EU:C:2017:981:[2018] Q.B. 854.

³⁵ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’).

Personalised (Consumer) Laws?

The last two topics to be covered address areas where the author believes technology is overstretching itself – the personalization of consumer law and crypto-currencies. The latter are a reality, but their long-term viability is doubted, at least, as a means of payment by consumers. Discussion of the former currently derives from the musings of law professors intrigued by the way in which technology might be used to personalize the law by adapting mandatory rules or even contract terms. Concerning mandatory rules, the discussion is based on a simple law and economics model that acknowledges people have different preferences as regards the level of their legal protection and that it costs traders more to offer that protection to different consumers (essentially because some are more likely to use their rights). It might seem straightforward therefore to match consumer preferences with the cost of providing the rights to ensure the market maximizes consumer welfare (Ben-Shahar and Porat 2019). There is also a broader debate about the use of big data to provide micro-directives on how the law should apply in particular circumstances (Casey and Niblett 2017). Casey and Niblett also suggest big data can be used to fill gaps in contracts and ensure the performance of contracts fits initial expectations, but they point out this may not be suitable for consumer contracts where businesses have advantages as they will have access to the data, will be able to control the algorithms used and better understand the legal rights and obligations. However, this is the world of law reviews (mainly in North America) and they often do not match reality. This personalized model seems so unrealistic that it will only be discussed briefly here, though as it is catching the imagination of scholars it will probably need to be refuted in more detail.

The popular topic of behavioural economics gives us some important insights into why we should be cautious about this personalized approach. One of the important insights it provides is that consumers do not have good self-awareness. For example, they will underestimate how a risk applies to them or be too optimistic about their chance of avoiding a risk (Howells 2005). If they make these mistakes about factors that pose a risk to their health and life (such as smoking), just consider how much more likely it is that they will misjudge the value of rather technical legal rights. It might be argued that personalization should be limited to private law rights and public law controls will remain to ensure things cannot go too badly wrong. However, private law rules also have an indirect effect on markets and behaviours within them. Ben-Sharar and Porat in a leading article on the topic focus on mandatory cooling-off periods (Ben-Shahar and Porat 2019). Most consumers might well, if asked, prefer a lower price in return for a shorter cooling-off period. If empirically proven this might suggest the law is currently over-protective. However, it might also simply reflect the difficulty many consumers have in valuing legal rights.

Of course some consumers will have more protection than they need and others less. There will be some cross-subsidization. However, the costs of legal protection are often modest in relation to the total cost and therefore the fine tuning will only marginally affect costs. Indeed, the costs involved in working out such fine tuning may well wipe out any gains. A frequent request from business is simply that it be given clear rules to follow. Even with the help of big data, algorithms and hi-tech computers (which all cost money) personalizing mandatory law will be a complex problem and businesses will likely make mistakes they will be blamed for. Are they to rely on consumers' self-declarations or decide/suggest for consumers based on algorithms what their default level of protection should be? Is a business going to want to force a consumer to take a higher priced package with higher levels of protection because that is what the computer predicts? If not we are surely not in the land of personalized mandatory

protection, but rather a more informed free market where all protections become optional. It must be doubted whether many businesses would want to enter into this quagmire.

Consumers too benefit from simplicity. One of the major problems for consumers is to understand their rights and this is one factor in the under use of consumer rights (Howells and Twigg-Flesner 2010). Even the famous blue-button example which would have allowed consumers to choose between national law or a European consumer law regime (with potentially different prices) (Schulte-Nölke 2000) was subject to the criticism that consumers were not well placed to make the choice as they would not understand the comparative value of the competing legal regimes. The present ideas seem far messier. Will consumers be required to have a preference for every mandatory consumer rule? Take the example of cooling-off periods – in the EU (and elsewhere to a lesser extent) these apply in many situations – sales on the doorstep and over the internet – and also with special rules for some such products such as timeshare or life insurance. Do consumers have to have preferences for each situation? Can they opt in and out of product liability rules? For instance, would we allow pharmaceutical prices to vary depending upon whether the development risks defence was available to producers? Would different sale of goods rights apply to different consumers? Could consumers opt out of any mandatory protection as regards non-conformity or might some choose to opt out of the EU law providing for a reversal of the burden of proof? Is the remedies regime up for negotiation? Should consumers be able to waive their rights to consumer information? The list could go on and even law professors may find it hard to calculate the benefits for themselves.

It should also be remembered that consumer transactions are also impacted by other laws than purely consumer law. One prime example is data protection law (Busch 2019). In fact, this is one area where personalization might have a role to play. This is because even relatively strict data protection regimes like that in the EU have at their core a model of transparency and consent (Solove 2013). Therefore, programmes such as the Platform for Privacy Preferences (P3P) and other more recently developed programmes have a role in matching preferences to website policies. However, these reflect preferences within the sphere of what is allowed under the mandatory regime. Personalizing mandatory choice sounds like a means to enhance preferences, but is more likely to be a back door to reduced protection. Consumer protection has been hard fought for. As it is a mass product, it is cost-efficient and applies to all preventing anti-competitive practices. The lure of technology driven models should not undermine core consumer values. At best personalization is likely to lead to only paper gains in autonomy.

Crypto-currency

Finally, cryptocurrencies are considered (Campbell-Verduyn 2016; McJohn and McJohn 2016; Narayanan et al. 2016). These might turn out to be to the twenty-first century what the tulip bulb was to Dutch investors of the seventeenth century: Albeit, the mathematical equation you pay for when purchasing a crypto-currency has even less intrinsic value than a tulip. Many in the financial services sector see their value as “driven by speculation and exuberance and not by rationality” (Witzig and Salomon 2018). They appear to be an example of doing something because it is technologically feasible without regard to the traditional role of the state as the backer of currency.

These crypto-currencies have an appeal to some who mistrust the financial services sector and government regulation in the wake of the 2008 Global Financial Crisis. Practical advantages are that they can potentially reduce costs by missing out intermediaries; they offer a secure means of payment and anonymity (though the anonymity is not watertight, Kaplanov 2012). The system is not, however, entirely costless as there is a need to pay the “miners” who use high powered computers to authenticate transactions. The ecological effects of using so much high-powered computers has also not been factored into their cost. Moreover, their functional advantages need to be weighed against the risk of crypto-currencies being used for moneylaundering, tax evasion, and nefarious purchases, as highlighted by its use by the Silk Road black internet marketplace. Moreover, even if the blockchain technology is safe (at least until someone finds a way to break its code), the wallets in which consumers keep the currency are a potential weak point. The Mt Gox bitcoin exchange went into bankruptcy in 2014 in Japan, announcing it had lost 750 000 of its customers’ bitcoins, and around 100 000 of its own bitcoins. This equated to 7% of all bitcoins that were worth around \$473 million at the time. The example of DAO (“distributed autonomous organization”) is also salutary (Werbach 2018). It grew to hold \$150 million in cryptocurrency, but then participants began to siphon off funds. What they did was permitted according to the self-executing software and the funds were only able to be returned after the fund was split into two by a so called “hard fork.” One group disagreed with this alteration of the rules and maintained a duplicate currency under which the “thief” kept his or her currency.

It is not even clear that crypto-currencies should be classified as currencies. “Money” has three broad characteristics: it is a store of value, a unit of account, and a medium of exchange (Blundell-Wignall 2014). Although, it might be claimed crypto-currencies can meet these criteria there are some issues. As a store of value, its weakness is its unstable value. This instability probably affects its ability to perform the other functions too. As a unit of account, it is not widely used and most people relate to prices fixed in national currencies whose value is more stable. Bitcoin is also not easy to express in small units. As a medium of exchange, the price volatility is again a problem and transaction times can be slow and not energy-efficient. A final concern is that it cannot be guaranteed to be converted back into legal tender. It is also possible that bitcoins might be considered a commodity so that contracts paid for with crypto-currencies will be barter contracts. They have de facto become an investment product that carries a high risk and some argue they are best viewed as securities that ought to be subject to security regulation. However, it is probably hard to pigeon-hole them easily into any existing category (Grinberg 2011).

Some states, like China, have prohibited cryptocurrencies. Others, such as the UK, have discouraged them. Several, often smaller states, are seeking to embrace them as a driver for their economies – see Estonia, Switzerland, Singapore, and Hong Kong (De Filippi 2014; Witzig and Salomon 2018). It is not unusual for small economies to see exploiting new financial products and technology as a potential windfall, but one only has to look at the collapse of Icelandic banking sector during the Global Financial Crisis to see that if the fundamentals do not make sense then caution should be exercised.

In the coming years, it is just possible that we may all be using cryptocurrencies to make regular payments. However, this is doubtful. Particularly, as alternative electronic payment systems become more convenient (loaded on apps in phones) and lower their costs, it is hard to imagine the demand will be sustained for complex and high-risk crypto-currencies. If they are

simply investments they are high risk; many should probably be regulated as securities. Blockchain technology and timestamping of digital documents undoubtedly have further potential to be exploited, but cryptocurrencies may just turn out to be a short lived phenomenon.

Conclusion

The message of this paper is undramatic, but hopefully valuable and timely. The digital era is bringing about many changes for the better in the consumer environment. We should be cautious though about accepting that just because something is technologically possible it should be done – cryptocurrencies are a good example. Advances in technology should not in themselves be an excuse for deregulation – as is often advocated, for instance, with regard to the sharing economy. Though, if new business models demonstrate the need to re-evaluate traditional rules, this should be embraced for all actors. New actors, like platforms, may cause us to consider their place in the regulatory environment. Many of the factors that are considered in need of review due to developments in the Fourth Industrial Age are in fact old chestnuts that have been debated for sometime, such as the status of software or the line between a trader and a hobbyist. But, fundamentally, the traditional core values of consumer protection law seem capable of applying to the digital environment with appropriate modification. This is not surprising. Consumers are likely to continue to have similar expectations in the online digital world. The need for new regulatory models to meet the challenges of an increasingly technological society may call for some new regulatory practices, but consumer protection seems able to retain its traditional values and in many instances its traditional form. It is in fact a positive conclusion, for it means the law, carefully applied or modified, is unlikely to be a brake on the development of innovation in the digital consumer market. Law can be a positive driver to ensure consumers have confidence in the goods and services and business models developed in the Fourth Industrial Revolution.

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

- Ahleit, K. (2001). The applicability of the EU product liability directive to software. *Comparative and International Law Journal of Southern Africa*, 34(2), 188–209.
- Akerlof, G. (1970). The market for 'lemons': Quality, uncertainty and the market mechanism. *The Quarterly Journal of Economics*, 84, 488–500.
- Anderson, C. (2014). *Makers: The new industrial revolution*. New York, NY: Crown Business.
- Anderson, J., Morikawa, J., Nidhi, K., & Stanley, K. (2018). *Rethinking insurance and liability in the transformative age of autonomous vehicles*. Santa Monica, CA: Rand Corporation.
- Ben-Shahar, O. (2009). The myth of 'opportunity to read' in contract law. *European Review of Contract Law*, 5, 1–28.
- Ben-Shahar, O. & Porat, A. (2019). Personalizing mandatory rules in contract law. *University of Chicago Law Review*, 86.
- Ben-Shahar, O., & Schneider, C. (2014). *More than you wanted to know: The failure of mandated disclosure*. Princeton, NJ: Princeton University Press.
- Blundell-Wignall, A. (2014). *The Bitcoin question: Currency versus trust-less transfer technology (No. 37)*. Paris: OECD Publishing.

- Brownsword, R. (2008). *Rights, regulation, and the technological revolution*. Oxford: Oxford University Press.
- Brownsword, R. (2017). After Brexit: Regulatory-instrumentalism, coherentism and the English law of contract. *Journal of Contract Law*, 34, 139.
- Brownsword, R. (2018). The E-commerce directive, consumer transactions, and the digital single market—Questions of regulatory fitness, regulatory disconnection and rule redirection. In S. Grundmann (Ed.), *European contract law in the digital age* (pp. 165–204). Cambridge: Intersentia.
- Brownsword, R., & Yeung, K. (Eds.). (2008). *Regulating technologies*. Oxford: Hart Publishing.
- Busch, C. (2016). Crowdsourcing consumer confidence: How to regulate online rating and review systems in the collaborative economy. In A. De Franceschi (Ed.), *European contract law and the digital single market* (pp. 223–243). Cambridge: Intersentia.
- Busch, C. (2019). Implementing personalized law: Personalized disclosures in consumer and privacy law. *University of Chicago Law Review*, 86, 309–331.
- Busch, C., Shulte-Nölke, H., Wiewiórska-Domagalska, A., & Zoll, F. (2016). The rise of the platform economy: A new challenge for EU consumer law? *Journal of European Consumer and Market Law*, 5(1), 3–7.
- Butcher, L., & Edmonds, T. (2018). *House of commons briefing paper no. CBP 8118 of 15 August 2018 on the automated and electric vehicles act 2018*. London: House of Commons Library.
- Calo, R. (2014). Digital market manipulation. *George Washington Law Review*, 82(4), 995–1051.
- Campbell-Verduyn, M. (Ed.). (2016). *Bitcoin and beyond*. Oxford: Routledge Taylor and Francis Group.
- Casey, A., & Niblett, A. (2017). The death of rules and standards. *Indiana Law Journal (Bloomington, Indiana)*, 92(4), 1401–1447.
- Cheng, L., Saw, T. J., & Sargeant C. (2016). Smart contracts, bridging the gap between expectations and reality. *Oxford Business Law Blog* 11 July 2016.
- Clack, C., Vikram, B., & Braine, L. (2016) Smart contract templates: Foundations, design landscape and research directions. *Arxiv:1608.0071v3* 15 March 2017.
- Commission Staff Working Document. (2017) *Report of the Fitness Check* (SWD(2017) 209 final).
- Curtis, K. (2015). A wiki weapon solution: Firearm regulation for the management of 3D printing in the American household. *Rutgers Computer and Technology Law Journal*, 41(1), 74–107.
- De Filippi, P. (2014). Bitcoin: A regulatory nightmare to a libertarian dream. *Internet Policy Review Journal on Internet Regulation*, 3(2).
- De Franceschi, A., & Lehman, M. (2015). Data as tradeable commodity and new measures for their protection. *Italian Law Journal*, 1(1), 51–72.
- Diedrich, H. (2016). *Ethereum: Blockchains, digital assets, smart contracts, decentralized autonomous organizations*. New South Wales: Wildfire Publishing.
- Durovic, M., & Janssen, A. (2019). The formation of smart contracts and beyond: Shaking the fundamentals of contract law? In L. DiMatteo, M. Cannarsa, & C. Poncibo (Eds.), *Smart contracts and blockchain technology: Role of contract law*. Cambridge: Cambridge University Press.
- Engstrom, N. (2013). 3-D printing and product liability: Identifying the obstacles. *University of Pennsylvania Law Review Online*, 162(35), 35–41.
- Estevan de Quesada, C. (2018). Crowdfunding in Europe. In S. Grundmann (Ed.), *European contract law in the digital age* (pp. 103–134). Cambridge: Intersentia.
- European Commission. (2016). *Guidance on the implementation/application of Directive 2005/29/EC on unfair commercial practices*. Brussels: Commission Staff Working Document SWD(2016) 163 final.
- European Commission. (2017a). *Report on the application of Directive 2011/83/EU* (COM (2017) 259).
- European Commission. (2017b). Autonomous cars: A big opportunity for European industry. *Digital Transformation Monitor*, January 2017.
- European Commission. (2018a). *Report on the application of Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC; COM/2018/246 final)*. Brussels: European Commission.
- European Commission. (2018b). *Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC; Commission Staff Working Document SWD/2018/157 final)*. Brussels: European Commission.
- Evas, T. (2018). *A common EU approach to liability rules and insurance for connected and autonomous vehicles*. Brussels: European Parliamentary Research Service.
- Finck M. (2017). *Digital regulation: Designing a supranational legal framework for the platform economy*. LSE Law, Society and Economy Working Papers 15/2017.
- Giancaspro, M. (2017). Is a ‘smart contract’ really a smart idea? Insights from a legal perspective. *Computer Law and Security Review*, 33, 826–835.
- Goldsmith, J. (1998). Against cyberanarchy. *Chicago Law Review*, 65, 1199–1250.
- Goldsmith, J., & Wu, T. (2006). *Who controls the internet?* Oxford: Oxford University Press.

- Grinberg, R. (2011). Bitcoin: An innovative alternative digital currency. *Hastings Science & Technology Law Journal*, 4(1), 159–208.
- Grundmann, S., & Hacker, P. (2018). The digital dimension as a challenge to European contract law—The architecture. In S. Grundmann (Ed.), *European contract law in the digital age* (pp. 3–45). Cambridge: Intersentia.
- Gurney, J. (2013). *Sue my car not me: Products liability and accidents involving autonomous vehicles* (pp. 247–278). Technology and Policy: University of Illinois Journal of Law.
- Hatzopoulous, V., & Roma, S. (2017). Caring for sharing? Collaborative economy under EU Law. *Common Market Law Review*, 54, 81–128.
- High-Level Expert Group on Artificial Intelligence. (2019). *Ethics guidelines for trustworthy AI*.
- Howells, G. (2005). The potential and limits of consumer empowerment by information. *Journal of Law and Society*, 32, 349–370.
- Howells, G. (2016). Reflection on remedies for lack of conformity in light of the proposals of the EU Commission on supply of digital content and online and other distance sales of goods. In A. De Franceschi (Ed.), *European contract law and the digital single market* (pp. 145–161). Cambridge: Intersentia.
- Howells, G., & Twigg-Flesner, C. (2010). *Consolidation and simplification of UK consumer law*. London: Department of Business, Innovation and Skills.
- Howells, G., Twigg-Flesner, C., & Wilhelmsson, T. (2017a). *Rethinking EU consumer law*. Abingdon: Routledge.
- Howells, G., Twigg-Flesner, C., & Willett, C. (2017b). Product liability and digital products. In Synodinou, T-E., Jogleux, P. Markou C., & Prastitou, T. (Eds.), *EU Internet Law*, (pp. 183–195). New York, NY: Springer International Publishing.
- Howells, G., Twigg-Flesner, C., & Willett, C. (2019). Innovation, 3D printing and the values and rules of consumer law. In A. De Franceschi & R. Schulze (Eds.), *Digital revolution—New challenges for law* (pp. 217–246). Munich: Beck International.
- Huang, B. J. (2015). Law and moral dilemmas, book review of the trolley problem mysteries by F.M. Kamm. *Harvard Law Review*, 130, 659–699.
- Johnson, D., & Post, D. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review*, 48, 1367–1573.
- Kaplanov, N. (2012). Nerdy money: Bitcoin, the private digital currency, and the case against its regulation. *Loyola Consumer Law Review*, 25, 111–174.
- Katz, V. (2015). Regulating the sharing economy. *Berkeley Technology Law Journal*, 30, 1067–1126.
- Koopman, C., Mitchell, M., & Thierer, A. (2015). The sharing economy and consumer protection regulation: The case for policy change. *Journal of Business, Entrepreneurship and The Law*, 8(2), 529–546.
- Langhanke, C., & Schmidt-Kessel, M. (2015). Consumer data as consideration. *Journal of European Consumer and Market Law*, 5(6), 218–223.
- Lehmann, A. (2016). A European market for digital goods. In A. De Franceschi (Ed.), *European contract law and the digital single market*. Cambridge: Intersentia.
- Lemley, M. (2006). Terms of use. *Minnesota Law Review*, 91(2), 459–483.
- Lessig, L. (2006). *Code 2.0*. New York, NY: Basic Books.
- Marchant, G., & Lindor, R. (2012). The coming collision between autonomous vehicles and the liability system. *Santa Clara Law Review*, 52(4), 1321–1340.
- McJohn, S., & McJohn, I. (2016). The commercial law of bitcoin and blockchain transactions. *Uniform Commercial Code Law Journal*, 47(2), 187–222.
- Metzger, A. (2017). Data as counter-performance: What rights and duties do parties have? *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 1, 2–8.
- Moolayil, A. (2018). The modern trolley problem: Ethical and economically-sound liability schemes for autonomous vehicles. *Case Western Reserve Journal of Law, Technology and the Internet*, 9(1).
- Murray, A. (2011). Nodes and gravity in virtual space. *Legisprudence*, 5(2), 195–222.
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfelder, S. (2016). *Bitcoin and cryptocurrency technologies*. Princeton, NJ: Princeton University Press.
- Nogler, L., & Reifner, U. (2014). *Life time contracts*. The Hague: Eleven International Publishing.
- Raskin, M. (2017). The law and legality of smart contracts. *Georgetown Law and Technology Review*, 1(2), 305–341.
- Reidenberg, J. (1998). Lex informatica: The formation of information policy rules through technology. *Texas Law Review*, 76(3), 553–593.
- Rubin, E. (2017). From coherence to effectiveness. In R. Van Gestel, H.-W. Micklitz, & E. Rubin (Eds.), *Rethinking legal scholarship*. Cambridge: Cambridge University Press.
- Savelyev, A. (2016). Contract law 2.0: Smart contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, 26(2), 115–134.
- Schulte-Nölke, H. (2000). EC law on the formation of contract—From the common frame of reference to the ‘blue button’. *European Review of Contract Law*, 3(3), 332–349.

- Schulze, R. (2016). "Supply of digital contract" A new challenge for European contract law. In A. De Franceschi (Ed.), *European contract law and the digital single market*. Cambridge: Intersentia.
- Schwab, K. (2016). *The fourth industrial revolution*. Cologne/Geneva: World Economic Forum.
- Sklaroff, J. (2017). Smart contracts and the cost of inflexibility. *University of Pennsylvania Law Review*, 166(5), 263–303.
- Society of Automobile Engineers. (2014). *Taxonomy and definition for terms related to on-Road motor vehicle automated driving systems* (Standard J 3016_201401).
- Solove, D. (2013). Privacy self-management and the consent dilemma. *Harvard Law Review*, 126(7), 1880–1903.
- Sundararajan, A. (2016). *The sharing economy: The end of employment and the rise of crowd-based capitalism*. Cambridge, MA: The Michigan Institute of Technology Press.
- Swire, P., & Litan, R. (1998). None of your business: World data flows, electronic commerce and the European privacy directive. *Harvard Journal of Law & Technology*, 12(3), 693–702.
- Szabo, N. (1997). *The idea of smart contracts*. Retrieved from <https://nakamotoinstitute.org/the-idea-of-smart-contracts/>. Accessed 18 Nov 2019.
- Toffler, A. (1980). *The third wave: The classic study of tomorrow*. New York, NY: Bantam Books.
- Twigg-Flesner, C. (2016). Disruptive technology—Disrupted law? How the digital revolution affects (contract) law. In A. De Franceschi (Ed.), *European contract law and the digital single market* (pp. 21–48). Cambridge: Intersentia.
- Twigg-Flesner, C. (2018). The EU's proposals for regulating B2B relationships on online platforms - transparency fairness and beyond. *Journal of European Consumer and Market Law*, 7(6), 222–233.
- Villasenor, J. (2014). *Products liability and driverless cars*. Washington DC: Brookings Institution.
- Walker, S. (2010). *Top 10 reasons why entrepreneurs hate lawyers*. Retrieved from: <https://venturehacks.com/articles/hate-lawyers>. Accessed 29 Apr 2019.
- Webb, K. (2017). Products liability and autonomous vehicles: Who's driving whom. *University of Richmond Journal of Law and Technology*, 23(4), 1–52.
- Werbach, K. (2018). Trust but verify: Why the blockchain needs the law. *Berkeley Technology Law Journal*, 33(2), 487–550.
- Witzig, P. & Salomon, V. (2018). *Cutting out the middleman: A case study of blockchain- induced reconfigurations in the Swiss Financial Services Industry* Working Paper 1. Université de Neuchâtel.
- Wu, T. (2003). When code isn't law. *Virginia Law Review (Charlottesville, Virginia)*, 89(4), 670–751.
- Zech, H. (2016). Data as a tradeable commodity. In A. De Franceschi (Ed.), *European contract law and the digital single market*. Cambridge: Intersentia.
- Zetsche, D., Buckley, R., & Arner, D. (2018). The distributed liability of distributed ledgers: Legal risks of blockchain. *University of Illinois Law Review*, 4, 1361–1406.

Cases

European Union

- Asociación Profesional Élite Taxi v Uber Systems Spain SL*, C-434/15 EU:C:2017:981;[2018] Q.B. 854
- Aziz v Caixa d'Estalvis de Catalunya* (2013) Case C-415/11 EU:C:2013:164; [2013] 3 C.M.L.R. 5
- Commission v United Kingdom*, C-300/95 [1997] ECR I-264
- Kásler v OTP Jelzálogbank Zrt* EU:C:2014:282;[2014] 2 All E.R. (Comm) 443
- RWE Vertrieb AG v Verbraucherzentrale Nordrhein-Westfalen eV*, Case 92/11, EU:C:2013:180;[2013] 3 WLUK 59

United States

- Brouse v US*, 83 F. Supp. 373, 374 (N.D. Ohio 1949)

United Kingdom

- Parking-Eye Ltd. v Beavis*, [2015] UKSC 67, [2016] AC 117

Legislation

European Union

- Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, annex 1(q): OJ 1993 L 95/29
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market: OJ 2000 L178/1

United Kingdom

Consumer Rights Act 2015

Locomotive Act 1865

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.