INTERCONNECTIVITY AND LIABILITY: AI AND THE INTERNET OF THINGS

Geraint Howells, Professor of Law and Dean of the College of Business, Public Policy and Law, National University of Ireland, Galway, Ireland, Visiting Professor University of Manchester.

Christian Twigg-Flesner, Professor of International Commercial Law, University of Warwick, UK.

1 INTRODUCTION

In this chapter, we deal with the role of artificial intelligence (AI) in the context of the Internet of Things (IoT). We will focus in particular on the question of liability in circumstances where an IoT system has not performed as expected and where this has resulted in loss or damage of some kind. We will argue that the combination of AI and the IoT raises several novel aspects concerning the basis for assessing responsibility and of allocating liability for loss or damage, and that this will necessitate the development of a more creative approach to liability than generally followed in many legal systems. Most legal systems combine linear liability based on contractual relationships and fault-based or strict liability on a wrongdoer in tort law. We seek to demonstrate that this approach is no longer sufficient to deal with the complex issues associated with the interaction of AI and the IoT, and to offer possible solutions. Our discussion will address this from the perspective of both consumer and commercial transactions.

Our discussion will proceed as follows: first, we will explain the nature of an IoT system in general terms, drawing on case studies from both the consumer and commercial sphere to illustrate this. We will then focus on the role of AI in the operation of an IoT system. Secondly, we will analyse the particular issues that arise in the circumstances where an AI-driven IoT system malfunctions and causes loss or damage, and the specific legal questions this raises. Third, we will examine to what extent legal systems (particularly the UK and the EU) are currently able to address these questions, and identify aspects that require action, whether in the form of legislation or some other intervention. Finally, we will propose an alternative for addressing the liability challenges arising in this particular context.

Our discussion rests on two inter-related points: first, the values underpinning established liability systems, particularly in the field of consumer protection law, should be maintained in the context of new
digital technology applications. Secondly, and by way of corollary, the adoption of new digital technology applications cannot be a basis for imposing a lower threshold of liability than the level of liability established in other contexts. In other words, the particular features of new digital technologies such as AI should not allow a “producer” of an AI-system to claim that it should not be held to the same standard as a producer of a physical item. The same principles of promoting consumer protection and confidence in the market informing the choice of existing liability standard should inform the decisions about liability in the novel context of AI where goods and services are interconnected, need to be updated and autonomous decisions can be made without human intervention.

One way of preserving established values in the context of new digital technology applications is to either apply existing laws where this is already possible or achievable through light amendments to existing laws. This might suffice in some instances, but it might also be necessary to be more creative in developing novel solutions which target novel issues of new digital technology applications. In the latter instance, aligning new laws with established underpinning values ought to be a key guiding criterion.

2 IOT AND AI

We start by considering what the Internet of Things (IoT) is. There are various definitions of the IoT in use. For instance, the European Union Agency for Cybersecurity (ENISA) has defined IoT as “a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making”. In contrast, the IERC-European Research Cluster on the Internet of Things defines it as “a dynamic global network infrastructure with self-configuring capabilities based

---


2 The tension between extending the reach of existing laws and limited reforms where needed on the one hand, and the development of new laws specifically targeted at novel issues created by new digital technology applications on the other hand, is a feature of much of the scholarly writings on the digital economy. This tension has been discussed in depth by Roger Brownsword, e.g., in “Law Disrupted, Law Re-Imagined, Law Re-Invented” (2019) Technology and Regulation 10.

on standard and interoperable communication protocols where physical and virtual “things” have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.4 The European Commission has explained that the IoT is where “all objects and people can be interconnected through communication networks, in and across private, public and industrial spaces, and report about their status and/or about the status of the surrounding environment.”5 In short, there is no consistent definition of the IoT,6 but there are common features to these definitions. First, the IoT involves the connection of devices through communication networks (primarily the internet). IoT devices therefore need to be equipped with the functionality required to access and communicate via the internet. Secondly, such devices may also be able to generate data about their own performance or about their environmental surroundings, usually through sensors which are part of such devices. The devices may also be linked to external data sources. The interconnection of such devices therefore provides for the exchange of data and can determine the actions taken by them. It also allows for them to be controlled remotely, e.g., via a smartphone app. A common consumer application of the IoT is the creation of so-called “smart homes”,7 where various domestic devices (kitchen appliances, central heating systems, lights and home security systems) are communication-enabled and can be programmed to take set actions in response to data received by each device, as well as being controlled remotely by the home-owner.8 In the commercial arena, common applications include both “smart manufacturing” to optimise supply chain logistics and production line management as well as enabling products to communicate performance data to facilitate predictive maintenance (i.e., identifying maintenance needs before they manifest).9 A further commercial utilisation is “smart farming” to improve the efficiency of farming operations, optimisation of the agri-

---

7 Staff Working Document, pp.31-2. A second example given by the Commission is personal wellness and wearables, i.e., devices a consumer can use to provide monitoring data about their health.
8 A home-owner can also use one of the various personal voice assistants to control their smart homes by speaking an instruction to the system.
9 Staff Working Document, p.33. The possibility of continuous monitoring could even lead to the extension of the current liability of seller and producer respectively: Bryant Walker Smith, “Proximity Driven Liability” (2014) 102 Georgetown Law Journal 1777.
food chain and food safety management. There are other examples, such as smart cities, autonomous vehicles and so on. A shared feature is that they involve devices connected to a communications network generating and exchanging data, and acting in response to data received, as well as being controlled remotely.

As the technology advances, the operation of many IoT systems can be further enhanced by the introduction of artificial intelligence (AI) into the operation of such systems. The European High Level Expert Group has adopted a complex definition of AI systems: “Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.”

In the European Commission’s April 2021 proposal for the Artificial Intelligence Act, an “artificial intelligence system” is defined as “software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.” In short, AI involves algorithmic decision-making based on data received and processed by the algorithm, in order to pursue a specific objective (e.g., energy-efficient operation of a consumer’s home; optimal supply chain operation for a production line, etc.). A crucial feature of AI is machine-learning capability, i.e., the possibility to “learn” from data and adapt both its processing rules and outputs accordingly.

---

13 Annex I refers to “(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; (c) Statistical approaches, Bayesian estimation, search and optimization methods.”
14 Art.3(1) of the proposed Regulation.
Taken together, an AI-driven IoT system therefore comprises the following key components: multiple devices, many equipped with sensors; devices connected via communication networks to exchange data and receive instructions; and an AI algorithm to operate the IoT system based on data received from data sources both internal and external to the IoT system. Each device will rely on software to perform its operations and to interact with the AI algorithm controlling the system.

Within such AI-controlled IoT systems, internet connectivity and heavy reliance on data raise significant concerns over cybersecurity. An IoT system could be hacked and interfered with, e.g., by manipulating the parameters for its operation. Data could be accessed without authorisation and “stolen”. However, for the purposes of this chapter, we are not directly concerned with cybersecurity issues. Rather, we focus on “system malfunctions” within AI-controlled IoT systems and the particular liability issues this raises, especially when such malfunction results in economic loss, damage, or personal injury. Questions of insufficient cybersecurity would, of course, be relevant to determining whether the system, or its components, meet the legally-mandated quality standards. In the next section, we identify the main causes of relevant IoT system malfunctions which could give rise to liability issues.

3 SYSTEM MALFUNCTION AND LEGAL ISSUES

An IoT system can malfunction for all sorts of reasons. We refer to “malfunction” as an umbrella term for any failure of an IoT system to work as intended or expected by the user. There can be many reasons for such a malfunction, and the more complex the IoT system is, the greater the number of possible points of failure. For the purpose of our discussion, we identify a number of possible malfunctions. One type of malfunction arises where one of the physical devices in an IoT system has failed. This would be a hardware failure and this type of problem would be covered by the legal rules dealing with the quality

---

16 See e.g., Joachim Scherer and Caroline Heinickel, “Regulating Machine-to-Machine Applications and Services in the Internet of Things” (2014) 2 European Networks Law and Regulation Quarterly 141, pp.150-151.
17 See also Jean-Sebastien Borghetti, “How can Artificial Intelligence be defective?” in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmeyer (eds.), Liability for Artificial Intelligence and the Internet of Things (Nomos, 2019).
and fitness for purpose of goods. As such, this would not raise any novel legal issues. However, it is in the nature of an IoT system that the various physical devices comprising that system interact and are able to exchange data. This requires devices within a system to be interoperable, i.e., to be linked together and to exchange data in a format that each device can understand. A lack of interoperability, e.g., because data is not understood in the same way by each component device, could cause the system to malfunction or fail altogether.

Secondly, some of the devices may have embedded software that allows them to operate. A malfunction within an IoT system could be the result of a software flaw, whether due to a coding error or, where enabled, an update to the software resulting in an error. This possibility raises two related issues: first, the software might have contained a coding error from the outset. Here, the question is whether the software is treated as an integral feature of the physical device and therefore covered by the legislation on the sale and supply of goods, as well as product liability, or whether the software is subject to a separate contract between end-user and the supplier of the software. Secondly, an error might have been introduced into the software as a result of an update. This raises a novel issue insofar as legal rules regarding the quality and fitness for purpose of goods usually focuses on the moment of delivery as the point at which the goods’ compliance with the relevant rules is assessed. By their very nature, software updates are made after this point, and so there will be a question of whether the fact that such updates occur periodically means that this falls outside existing legal rules on the supply of goods (which usually have a fixed point around the time of supply at which the supplier’s obligations are determined) and requires new provisions. In particular, it may need to be considered whether, if the update contains a flaw, this flaw should be treated as having existed at the point of initial supply (if liability were to fall on the supplier), or instead the point at which the update was supplied. The latter might be pertinent where updates occur for several years after supply, or where such updates are supplied by a third party under a separate agreement. A complication is that assessment of conformity or defectiveness should be judged against the expectations of the original contract or supply.

In addition to the problems associated with faulty updates, a further question arises whether a failure to provide updates could give rise to

---

18 There is also a debate in many jurisdictions as to whether a contract for the supply software should be classified as one for the supply of goods or services, with a further distinction drawn between standard and customised software.
liability. This issue may become pertinent in a variety of situations, in particular where there are errors in the software code which need to be corrected in order to ensure that the software performs as expected (a conformity problem), as well as where there is a problem with the software which might cause the goods to operate in an unsafe manner. A possible solution might be a legal duty to provide updates or to arrange for the provision of updates by a third-party. 19

Indeed, the role of software extends beyond device-specific operating software. An IoT system can often be controlled remotely by using an “app” installed on a smartphone. This app could have a problem which could, in turn, disrupt the operation of the IoT system and trigger a malfunction resulting in loss or damage. As the legal treatment of software varies between jurisdictions, and also between consumer and commercial transactions, the legal rules regarding software might need to be clarified.

Matters are further complicated once an IoT system is operated with the use of AI and the decisions made by an AI algorithm result in a malfunction of the IoT system itself. Such an AI-based malfunction could be due to a variety of reasons. First, this might be due to the way in which the AI algorithm was coded at the outset. Secondly, where the AI algorithm has “self-learning” capacity, the decision-making pattern it has evolved might result in IoT system malfunctions. Third, the source of the problem might not be the AI algorithm itself, but rather the data received and processed by the algorithm in order to determine the operation of the IoT system. This data might have been provided by one of the devices within the IoT system, or from an external source. A problem with such data could be due to a variety of reasons, including a fault with a sensor on one of the IoT system’s devices, resulting in inaccurate, incomplete or missing data; also, data might have been supplied from an external source based on a unit of measurement which differs from that used by the AI algorithm. This complexity will create challenges for both establishing the actual cause of the problem and the consequent attribution of liability.

This discussion shows that the interaction of physical and digital elements within an AI-controlled IoT system means that there are multiple points of failure, some of which are external to the IoT system

19 This question resembles a long-running debate in sales law regarding a legal obligation to make available spare parts to ensure that goods can be repaired and their lifetime be extended. In the EU and the UK, some steps towards this have now been taken in respect of some categories of goods in the context of Ecodesign and Energy Labelling.
itself. A user who has encountered an IoT system malfunction will therefore face the evidentiary hurdle of identifying the cause(s) of such a malfunction first. This will be necessary to identify both the potential counter-party against whom a claim might be made and the legal basis of such a claim (bearing in mind that, aside from legal rules regarding quality-issues and damage caused by goods, not every legal system will necessarily provide clear legal rules in this regard). It will be necessary to identify the correct counter-party because most IoT systems will comprise a number of physical devices, software and other digital elements, an AI algorithm, and internal and external data, and it is likely that this will involve a plurality of counter-parties. There might be situations where an IoT system was acquired as a package from one supplier, but even there, multiple parties might be involved because of the combination of physical and digital elements. The end-user of any IoT system will therefore commonly have to deal with several counter-parties. This will usually be through separate contracts based on different contract terms.20

The legal basis of any claim to be brought will depend on how the relevant legal system deals with liability issues in respect of goods incorporating software, stand-alone software, AI algorithms, and the supply of data. At present, legal systems vary in respect of the extent to which these issues are addressed at all, and insofar as they are, in the scope of the relevant legal rules both with regard to their substance and as between consumer and commercial situations. Proposals for law reform are discussed at national, regional, and international levels. In the next section, we will examine these issues more closely, identify what should be addressed in legal rules, and consider existing measures and reform discussions.

4 KEY LEGAL ISSUES AND CURRENT STATE OF THE LAW

In this part of our paper, we will examine current and proposed approaches for addressing the legal issues which arise in AI-operated IoT systems. In the previous section, we identified a number of questions, to which we now turn.

20 Guido Noto la Diega and Ian Walden, “Contracting for the ‘Internet of Things’: looking into the Nest” (2016) 7 European Journal of Law and Technology (no page numbers).
4.1 Goods with digital elements

As IoT systems comprises various devices, which connect and interact with one another based on integrated software. We first consider goods containing digital elements. With goods containing digital elements, it is often necessary to consider whether both the goods and the digital elements are treated as goods, or whether a different regime applies. In some jurisdiction, such as the UK and the EU, distinct legal regimes for the supply of goods and digital content and digital services have been adopted, particularly in the EU (directives on the sale of goods (2019/771/EU; “SGD”) and on digital contents and digital services (2019/770/EU; “DCDSD”)) and in the UK (Consumer Rights Act 2015). These technical rules on the scope of the various regimes go to the question of whether the supplier of the goods should also take responsibility for defects in the digital elements and how the physical and the digital elements interact. Behind this lies more policy orientated questions about whether the rules for goods or digital content are more appropriate; though in many instances the rules are approximated.21

The UK Consumer Rights Act 2015 was one of the first pieces of legislation to regulate digital content. This gave consumers a claim against a trader where digital content had been supplied in return for a price. It does not cover the situation where the counter-performance is data, but the Secretary of State has the power to extend this to other contracts such as where the consumer provides data instead of paying a price.22 EU law adopts a broader approach including any supply of digital content or services. In the case of goods with digital elements where the digital content is not in conformity with the contract, UK law treats this as a non-conformity of the goods themselves.23 Effectively, this may give the consumer the option of either suing the supplier for the paid-for digital service (if paid for separately), or the supplier of the goods incorporating the digital content.

The EU takes a more systematic approach to allocating liability between the Sale of Goods Directive and the Digital Content and Services Directive. Digital content covered by the Dis broadly defined to encompass “data which are produced and supplied in digital

21 There is also the question as to whether the relevant time for assessing conformity should be the traditional time of supply, or whether the supplier should have responsibility for both updating the software and for any defects that result from such updates. This also raises the question of updates which even the supplier may have no control over as they are made autonomously.
22 S.33.
form”. The DCDSD also applies to any tangible medium which serves exclusively as a carrier of digital content. Accordingly, such carriers are excluded from the SGD. By contrast, the Consumer Rights Directive had treated such tangible mediums as goods. As Staudenmeyer notes, the solution in the DCDSD was chosen for simplicity as devices such as discs and DVDS are simply providing the mechanisms for delivering the digital content. It might have been more logical to apply the DCDSD to the digital content/service and SGD to the carrier, but it was considered that would have been confusing. Applying the SGD would not have made much sense if the real complaint was about the digital content. However, the DCDSD only brings within its scope tangible media that serve exclusively as a carrier of the digital content. There is a question mark as to whether this applies subjectively in the particular contract or objectively based on the use the carrier could be put to. Take, for instance, a USB stick or a portable hard drive. Both can be used for adding extra data, so does that mean they are not covered? Or does the fact that under the digital content contract, they are simply intended to be the carrier of the digital content mean that they fall within the scope of the DCDSD? Staudenmeyer suggests it should be assessed based on the circumstances of the case. This can be problematic though. Increasingly, conference papers for example are supplied on USB sticks. Some sticks may be so full that they can realistically only be used for storing the papers, but if they have a lot of spare capacity, attendees might store other files on them or even delete conference files and place their own on them. But it seems clear the intention was only to use them as a carrier for the digital content supplied. They are different from USBs that might be supplied as a souvenir for visiting the event.

However, the main rule is to place digital content/services supplied with goods under the SGD. The DCDSD provides that its rules shall not apply to digital content or digital services which satisfy both functional and contractual criteria. To be excluded and hence covered by the SGD, the digital content/service must firstly be incorporated in or interconnected with goods in a manner that affects the functioning

24 Art.2 no 11.
25 Art.3(3) DCDSD.
26 Art.3(4)(a) SGD.
of the goods. This will only be the case if the absence of that digital content or digital service would prevent the goods from performing their functions.\textsuperscript{30} This applies irrespective of whether such digital content or digital service is supplied by the seller or by a third party. The supplier of the goods will be responsible for non-conformity resulting from the digital content/service.\textsuperscript{31} However, this will only be the case if the digital content/service has been provided under a sales contract concerning those goods. If they are not provided under the same contract, there will be a bundle of separate contracts with the DCDSD applying to the digital content/service element and the SGD applying to the goods. There may be incentives on the part of the supplier of goods to draft the contract to make it appear as if the digital content/service are not supplied under the same contract so as to avoid liability for the digital content/service. This separation is expressly permitted.\textsuperscript{32} Such clauses will have to pass the transparency test of the Unfair Contract Terms Directive though. One can imagine the courts will scrutinise such terms carefully, given that there is a presumption that the digital content or digital service constituting the digital element of goods is presumed to be covered by the sales contract.\textsuperscript{33}

The DCDSD and SGD achieved their purpose of providing a separation between their spheres of operation, but precisely in the area of related contracts the interactions of liability regimes between digital content/services and goods remain obscure. Indeed, the effect of termination of one element of a contract bundle may have on another element is left to national law.\textsuperscript{34} The rules on contract bundles only apply when the elements are supplied under a single contract. The whole question of linked or ancillary contracts is also left to national law.

As regards strict product liability, it is generally assumed the final product producer will be responsible for all harm (personal injury and damage to property) caused by the product including any harm caused by the software incorporated.\textsuperscript{35} Such software will be seen as a component part and whether there is liability for the producer of the component part will be determined by whether software is treated as a product in its own right, as discussed below. The producer of the

\textsuperscript{30} Art. 2(3) SGD.
\textsuperscript{31} Art.10 SGD
\textsuperscript{32} Recital 21 DCSD and 15 SGD.
\textsuperscript{33} Art. 3(4) DCSD.
\textsuperscript{34} Art.3(6). Recital 34.
component may be able to rely on a defence if the defect resulted from their following instructions or due to how the component was incorporated into the final product. The producer has been found to be under a duty to survey the market for accessories used with its product and to take steps to ensure consumers are warned about any that are unsafe even if not produced with the permission of the producer of the main product. This might be applied to ensure that the safety of the goods is taken to include their foreseeable interaction with independent products, i.e., where they may interact with each other in the IoT. It could also cover their safety where the goods are used with a digital service that manages the goods in a smart environment.

Thus, the area of uncertainty is in sales law where two products are bought separately but are intended to interact. Goods, digital content, and digital services may lack conformity and this lack of conformity can derive from the way the goods and digital content and services interact. There are rules requiring functionality, compatibility and interoperability if they are to be in conformity. These require that the goods can perform their function, which might include exchanging data with a product or digital service provider (functionality). This should be possible with their usual hardware (compatibility) and where provided for in the contract other alternative software and hardware (interoperability). The lack of conformity can also be derived from the trader failing correctly to integrate digital content into the digital environment or provide the consumer with adequate instructions for doing so. However, there may be gaps created especially when goods are added to existing digital environments or new digital services are added: existing products may not be at fault for how they are affected by subsequent purchases or for failures to work properly in the new

36 Art.7(f) PLD.
37 This was the view taken in a German negligence case, reported at (1986) NJW 1009.
39 Meaning “the ability of the digital content or digital service to perform its functions having regard to its purpose” Art.6 SGD/ Art.9 DCD.
40 Meaning “the ability of the digital content or digital service to function with hardware or software with which digital content or digital services of the same type are normally used, without the need to convert the digital content or digital service” Art.7 SGD/ Art.10 DCSD.
41 Meaning “the ability of the digital content or digital service to function with hardware or software different from those with which digital content or digital services of the same type are normally used” SGD Art.8/ Art.2(11) DCD.
42 Interoperability appears in the subjective, but not the objective criteria of conformity: see EU Digital Law at 55.
43 Art.8 SGD/ Art.9 DCSD.
environment where a new digital service is added. Digital services may not be liable if they are not interoperable with existing goods unless this is expressly provided for. Even if goods and digital services are in theory liable the consumer may have problems determining which element was lacking conformity and responsible for harm. One response to this might to reverse the burden of proof; another would be bolder, to create a form of network liability (considered below).

As regards strict product liability under the PLD, goods may be defective because they incorporate digital content/services that renders them dangerous.\(^{44}\) Equally, goods may be unsafe due to how they interact with the digital environment. However, the digital content/service will not itself be subject to liability under the PLD (see discussion on software below). This also means that software developers will not be liable as producers of component parts when included in the goods. Though it might be argued that if the digital content/service is supplied on tangible goods then producers of components might be liable, drawing analogies with the position under the SGD. Even if they are covered by strict liability, there will be the same problem of allocating liability as in the sales context.

**4.2 Software, digital content and digital services**

Above, we examined goods incorporating digital content/services. However, as we explained earlier, an IoT system involves an ecosystem comprising physical elements as well as digital content (such as an app on the user’s smartphone). In this section, we turn to the problem is of how to treat software/digital content which is independent of the product. This might be because of the desire to sue the software manufacturer directly in product liability on the basis that the software was supplied separately and was the cause of harm.

The treatment of software/digital content has always challenged the law. It has not traditionally fallen within the definition of goods (though Australian and New Zealand law resolved the issue simply by extending that definition to encompass software\(^ {45}\)). An early approach to fudge the issue was to argue that software was goods only when it was supplied on a tangible medium.\(^ {46}\) That made some sense as such

\(^{44}\) Although this has not been conclusively confirmed by the CJEU, it is widely assumed to be the case.

\(^ {45}\) The Australian Consumer Law provides that goods includes software, Sched. 2 S.2. See also New Zealand s.2 Sale of Goods Act 1908.

\(^ {46}\) *St Albans DC v International Computers Ltd* [1996] 4 All ER 48.
software was normally mass produced and hence subject to the same policy arguments for liability as goods, whereas bespoke software solutions resembled services which were normally subject to negligence rather than strict liability. However, that way of side-stepping the issue has become less available as increasingly in these days of cloud computing software is simply downloaded and not supplied on a disc or other durable medium. The UK’s Supreme Court has an appeal pending on whether software is goods in the context of the Commercial Agents Directive. The Court of Appeal, overturning the High Court, held that software was not goods.\textsuperscript{47} The Supreme Court has referred the matter to the CJEU,\textsuperscript{48} and judgment is pending at the time of writing.\textsuperscript{49}

In the case of software contracts, the common law might imply terms regarding quality and fitness for purposes, as in the case with contracts outside the scope of the limited codifications in England. However, relying on the common law is uncertain, and it was welcomed when sales law was clarified in the consumer context by the Consumer Rights Act 2015 creating a separate regime for digital content. This approach was followed at the EU level in the DCDSD. That Directive created the additional category of digital service as well as digital content, but it seems that was mainly for clarificatory purposes and most digital services such as sites allowing you to upload data or share files would most probably be caught by the UK definition of digital content.\textsuperscript{50}

Whether software is a ‘product’ for the purpose of strict (tort) product liability law has long been a contested issue.\textsuperscript{51} Though sound arguments can be made for software being included on policy grounds of consumer protection,\textsuperscript{52} especially when mass produced or when supplied on tangible media, it seems most likely that it is not, given the definition refers to movable goods\textsuperscript{53} and it was felt necessary to specify include liability for electricity. This seems to be in line

\textsuperscript{47}Computer Associates UK Ltd v The Software Incubator Ltd [2018] EWCA Civ 518
\textsuperscript{48}C-410/19 The Software Incubator (pending).
\textsuperscript{49}Advocate-General Tanchev’s opinion, given on 17 December 2020, concluded that “goods” should include software for the purposes of the Commercial Agents Directive (ECLI:EU:C:2020:1061).
\textsuperscript{50}The Commission had originally proposed to use only digital content and the addition has been said to be for only clarificatory purposes: EU Digital Law at 47.
\textsuperscript{53}Art. 2 PLD.
with a recent Opinion of Advocate General Hogan that a newspaper was not a defective product because it contained incorrect advice in its health column. The exclusion of such advice from product liability is perhaps not surprising, but of potentially more relevance to us was his reference to the Dutrueux case in which the supplier of a medical service was not held to be a supplier of products just because he used products which he had not produced himself. This approach would insulate the suppliers of smart systems from liability for any products connected to the system which they had not produced. Product liability law has long remained unreformed, but the need to address issues relating to the digital age may be a spur for it to be seriously reviewed. It would therefore be desirable to clarify/extend the current product liability regime such that it clearly applies to digital content. This does not mean that liability should encompass pure information services, where human intervention is always a vital link in the chain of causality. Rather, when digital content causes an action which creates harm there should be liability. Often this will be because of a faulty instruction sent to a product that causes it to take a step without human intervention or an error in the software incorporated in the product. In the former case the policy reasons for strict liability seem to apply equally, as regards software components there seems little reason why they should be exempt rather than any other component manufacturer. It is unfortunate that there seems to be hesitancy in some places for this relatively straightforward reform to the PLD. It seems inevitable and a corollary to the DCDSD.

4.3 Lifetime contracts and the duty to update

Traditionally, the law sees the supply of goods as a point contract in which the liabilities or the parties is fixed and assessed based on the

54 Case C-65/20 VI v Krone Verlag Gesellschaft mbH & Co KG ECLI:EU:C:2021:298.
55 C-495/10 Centre hospitalier universitaire de Besançon v Thomas Dutrueux ECLI:EU:C:2011:869.
56 The European Commission has acknowledged this: see European Commission, Artificial Intelligence for Europe COM (2018) 237 final, p.15. But no reform seems imminent at the time of writing.
59 This argument has been made in Geraint Howells, Christian Twigg-Flesner and Chris Willett, “Protecting the Values of Consumer Law in the Digital Economy: The Case of 3D-Printing” in Digital Revolution – New Challenges for the Law, Alberto De Franceschi and Reiner Schulze eds, (Beck, Nomos, 2019) 214.
condition of the goods at an early stage in the supply relationship. Under sale of goods law this is normally at the time of delivery, or in strict products liability law the time when the product was supplied or in the language of the PLD “put into circulation”. Any post-supply conduct of the seller or producer, such as poor conduct of a recall must be assessed under negligence law. However, this does not work for digital products such as those used in the IoT because the link to, and dependency on, ongoing digital content and services transforms them into lifetime contracts that must involve ongoing responsibilities of the supplier to the user. For consumer contracts, this ongoing obligation has been squarely addressed in the SGD and DCDSD. In the commercial sales context, it remains a matter for contractual negotiation. The PLD does not address it directly and may need reform.

Digital content and digital services will normally be required to be updated. Often this may be for security reasons, but it can also be for reasons of maintaining functionality and interoperability. The obligation to have an ongoing update obligation has rightly been described as “a ground-breaking new development” in the DCDSD and parallel rules are also found in the SGD. The initial proposal in the DCDSD had only been for updates to be required as provided for in the contract. This subjective element remains and allows the parties to agree more extensive updating obligations, but the objective conformity requirements now include minimum updating obligations.

The duty to update needs to be framed in the context of the content, service or goods provided. Where a fixed period is set, such as a one-year cloud data storage service, then it seems obvious that the updating should last for that period and that is indeed the solution provided. For goods, the seller is in any event liable for defects that become

60 Cf. Lord Diplock in Lambert v Lewis [1981] 1 All ER 1185, p.1191: “the implied [term] relates to the goods at the time of delivery under the contract of sale in the state in which they were delivered”. It has also variously been suggested that the time when risk passes, or even when property passed, might be that time: Christian Twigg-Flesner and Rick Canavan, Atiyah and Adams’ Sale of Goods, 14th ed. (Pearson, 2020), p.115.
61 S.4(1)(d) Consumer Protection Act 1987
62 Art. 7(b) PLD.
63 Walton v British Leyland, The Times, 13 July 1978
64 Luca Nogler and Udo Reifner, Life Time Contracts: Social long term contracts in Labour, Tenancy and Consumer Credit Law (Eleven, 2014).
66 Art. 7(d) DCDCS and Art. 6(d) SGD.
67 Art. 8(2)(a) DCDSD Art. 7(3)(b) SGD.
apparent within two years. The more difficult task is to determine the length of the duty to update where there is not a fixed period specified, but rather a one-off supply or series of one-off supplies. The Directives have to fall back on a general test leading to case-by-case assessments. It will depend upon what the consumer “may reasonably expect, given the type and purpose of the digital content or digital service and taking into account the circumstances and nature of the contract” The recitals give some clues. If an app or goods are for a specific purpose such as for a sporting event or music festival, then the updates would only have to be provided for the period necessary for that event. Normally, the updating obligation should be for the period for which there would be liability for non-conformity, typically two years. However, the recitals make it clear that the obligation can extend beyond the conformity period, especially as regards the duty to provide security updates. However, the extent of this obligation and the circumstances when it will arise are uncertain. The trader must inform the consumer of the update obligations.

The extent of the update obligation is only to keep the goods, digital content or service in conformity with the contract. There is no obligation to provide the latest version. As noted, the trader may have agreed to provide upgraded services and there are separate rules with conditions that have to be met if the trader wants to modify the digital content or service. The fact the obligation is linked to the lack of conformity also impacts on the remedies. The primary remedies should be bringing the goods into conformity by providing the update. If the trader will not or cannot do that (perhaps because of their reliance on an uncooperative third-party software developer) the remedies of price reduction and termination may come into play. Price reduction should be based on the decrease in value due to lack of an update rather than the cost of the update as such. One can imagine even a relatively inexpensive update might lead to vastly reduced utility, or even cybersecurity issues. Conversely, most updates will only be minor in nature and the remedy of termination may therefore not be available.

---

68 Art. 10(2) SGD.
69 Where digital elements are supplied with goods there will normally be a one-off supply related to those goods are the drafting the SGD reflects this.
70 Art. 8 (2)(b) DCDS and Art. 7 (3)(a) SGD.
71 Recital 47 DCDS and 31 SGD.
72 Art.19 DCDS; Art.7(3) SGD.
73 Art. 14(4)(5) DCDS and Art. 14(3)(4) and 15 SGD.
74 Art. 14(6) DCDS and Art. 13(5) SGD.
The consumer holds the remedies for lack of updates against the trader. However, it is the software developer who has to make the updates and the supplier, particularly in goods contracts may have no independent ability to update. This option was preferred to making the developer directly liable to the consumer as the consumer only has at best an end user license and no contract with the developer. Indeed, the solution is not out of line with traditional sales law whereby the trader is responsible for the components. The risk is held by the trader. This is tempered by provisions which provide the trader with a right of recourse against third parties such as developers, but these rules are facilitative and depend upon the trader contracting for the assistance of the developer to provide updates. The trader also can deviate from the conformity obligation with regard to specific characteristics that are drawn to the consumer’s attention and accepted. Thus, a trader could specifically provide that updates were not guaranteed. The ability to impose such a term might depend on market forces, but one could imagine that traders might be tempted to include such exclusions in boilerplate standard form contracts. In such instances, the transparency requirement before such exemptions are excluded from review for their unfairness under the UTCD would be important in protecting consumers. Although focusing liability on the trader is a traditional approach the significance of the role of software developers and others who provide data to make such systems work should encourage us to consider alternative liability regimes.76

If a product is rendered unsafe due to an update, the PLD becomes relevant. This covers harm to person or property. Even if the definition of property is extended to cover damaged data,77 this should not mean it can be used with respect to broader cybersecurity risks. There have been calls to amend the definition of defect78 to take account of the need to provide updates.79 These rely on at least three arguments.

(i) The need to include software within the scope of liability. The importance of this has been discussed above and

76 The European Parliament has discussed extending liability to such backend operators: European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence 2020/2014 (INL). See discussion below.
78 Art.6 PLD.
including software within the scope of the PLD would be a sensible reform.

(ii) The limitation when assessing defect to the condition at the time the product was put into circulation. It is possible that if the safety of a product is linked to digital content and services then there might be an implicit expectation that they be updated to keep the product safe. There would be the same debate as in contract law about how long that expectation would extend for. Failure to undertake to update them could be seen as a risk present at the time of supply rather like a lack of durability. If the trader wanted to make it clear that updates may not be supplied this could be possible by reference in the current definition of defect to the presentation of the goods. However, it is certainly unclear whether currently a failure to update could be linked back to the condition of the product at the time of supply. Adding the expectation of appropriate updates as a relevant factor would be a sensible revision. This would link back to the expectations of safety established at the time of supply and not involve imposing post-marketing obligations. These are adequately addressed for regulatory reasons under the General Product Safety Directive.

(iii) The fact that a subsequent better product is available is irrelevant. This factor should, however, certainly remain, for as with conformity the obligation should be to maintain the expected standard and not enhance it unless that has been promised. As with the conformity rules the policy objective should be to maintain the expected levels of safety.

It is likely that risks from failure to update could be captured by the current definition of defect in PLD, but it is one aspect that could usefully be clarified.

4.4 AI algorithms

We explained above that where AI is deployed in the context of an IoT system it can result in a malfunction of the system as a whole because of the actions triggered by the AI algorithm. However, even where it is possible to identify the actions taken by the AI algorithm as the
source of the system malfunction, this does not mean that the AI algorithm itself is faulty: if the decisions taken by the AI algorithm are the result of the data received, for example, then the real source of the problem would be the data. This raises separate liability questions considered in the next sub-section.

For present purposes, we assume that the AI algorithm itself is faulty in some way and that this has caused an IoT system malfunction. This leads us to important and difficult questions about liability for an AI algorithm, in particular (i) who would be liable, and (ii) what the basis of such liability (tort, contract) might be. At the present time, the liability issues in respect of AI algorithms are a matter of intense scholarly and policy discussions, but there is as yet no legislation specifically dealing with this. Nevertheless, it may be possible to apply existing laws to at least some liability questions arising in the context of AI algorithms.

We need to distinguish between two categories of algorithm. The first is an algorithm which relies on pre-set instructions which allow the algorithm to take a range of decisions triggered by pre-determined criteria. In AI terms, this might be categorised as symbolic AI. Such an algorithm is comparable to software or digital content and can therefore be treated in the same way as software (see section above).

The second category is a “self-learning” algorithm, i.e., an algorithm developed through machine-learning. It is an inherent feature of such algorithms that they are able to revise the way in which decisions are taken based on both an initial training period during which the algorithm learns to identify acceptable and unacceptable decisions, and subsequently based on decisions taken in light of new data and (where possible) feedback give to the algorithm in response. For instance, in an AI-controlled IoT system, a user override of decisions taken by the algorithm should enable the algorithm to adjust how it will respond in the same or a similar situation in the future.

Problems with such an AI algorithm can be due to a variety of factors: first, the initial training period might have created the conditions for the AI algorithm to take decisions which cause the IoT system to perform in an unexpected manner. Secondly, the self-learning development of the AI algorithm after deployment may result in bringing about such conditions. This could be the result of the data

---

received by the algorithm or the way in which the IoT system has been monitored by the user.

Determining an appropriate approach to liability for an AI algorithm, both with regard to the legal nature of such liability and the person(s) liable, is a controversial issue. A recurring suggestion is to grant an AI algorithm legal personhood akin to that of a limited liability company, so as to side-step the need of identifying the correct defendant in case of loss caused by an AI algorithm. However, an obvious problem with such an approach is the lack of monetary resources of an AI algorithm with separate legal personality for paying compensation. It is difficult to see what would be gained by pursuing this idea.

At the outset of this chapter, we stressed that in our view, the novelty of AI algorithms does not mean that established approaches to liability already in place should be abandoned and that, consequently, there should be no scope for producers/suppliers to argue for less stringent liability standards because of the continuously evolving nature of AI.

This means that, as far as the initial provision or deployment of a pre-trained AI algorithm is concerned, the situation is best treated as akin to the supply of digital content. As discussed above, at least in respect of consumer transactions, this will mean liability will be based on strict contractual liability, and liability would arise if the AI algorithm were not in conformity with the contract.

However, the situation is less clear-cut when it comes to developments in the AI algorithm resulting from its self-learning capacity, where these lead to decisions triggered by the algorithm resulting in a malfunction of the IoT system. One might be tempted to treat this in a comparable manner to updates made to software/digital content after its initial supply, as discussed earlier. However, the machine learning process of the AI algorithm is based on both its operation within the IoT system and the various data inputs feeding into the mechanism alongside any user feedback. There is therefore a difference to software/digital content updates in that changes to the AI algorithm will often be the result of factors beyond the control of the supplier of that algorithm. However, this should not lead to the conclusion that the

---


82 The European Parliament expressly rejected the idea of legal personality for AI in its resolution on a civil liability regime for artificial intelligence (2020/2014(INL), 20 October 2020), at paragraph 7.
producer or supplier of the AI algorithm should escape liability for problems which arise during the operation of the AI algorithm in an IoT system. This is because the way in which the AI algorithm develops will in some part be due to how it has been structured and therefore how its self-learning capacity has been designed. It is possible that a decision by an AI algorithm causing a system malfunction could have its roots in the design of the AI algorithm. Moreover, it will be almost impossible to determine whether a decision taken by an AI algorithm was shaped by its initial design or as a consequence of its self-learning, or, indeed, because of its pre-deployment training. 

Furthermore, it may be that there is an interoperability issue between the AI algorithm and the various data inputs and the way in which the algorithm understands the data it receives (see below). In short, working out why a rogue decision was taken by an AI algorithm may be an impossible task, especially for the end-user.

Perhaps the simplest solution might be to impose strict liability on either the producer or the operator of an AI-algorithm integrated into an IoT system. The High Level Expert Group and the European Parliament both favour imposing strict liability on an operator (alongside a producer), distinguishing between a front-end operator and a back-end operator. The High Level Expert Group suggests that liability should be on the operator who has the greater control over the

---

88 Defined by the High-Level Expert Group as “the person primarily deciding on and benefitting from the use of the relevant technology “, and the European Parliament as the “person who exercises a degree of control over a risk connected with the operation and functioning of the AI-system and benefits from its operation”.
89 Defined by the High Level Expert Group as “the person continuously defining the features of the relevant technology and providing essential and ongoing backend support”, and the European Parliament as the “person who, on a continuous basis, defines the features of the technology, provides data and essential backend support service and therefore also exercises a degree of control over the risk connected with the operation and functioning of the AI-system”
risk flowing from the operation of the AI-algorithm, whereas the European Parliament prefers joint and several liability of all operators, with a right of recourse between them. The introduction of operator liability would be a novel step. In the context of an IoT-system controlled by an AI-algorithm, this might lead to instances where the end-user (as front-end operator) could be liable for damage suffered by another. This might be appropriate for a commercial setting, but perhaps less so in a consumer context. In respect of an IoT-system, it might be that the back-end operator is the better candidate for the imposition of liability rather than the front-end operator/end-user. Similarly, the European Parliament’s proposal for a Regulation on liability for the operation of Artificial Intelligence-systems had proposed introducing a strict liability regime for high-risk autonomous AI products backed up by mandatory insurance. Both front-end and back-end operators would be subject to this regime. Liability of front-end operators would assist third parties injured, but not where the product harms the operator themselves. However, under the proposal, liability would also extend to back-end operators. In contrast, the European Commission’s proposal for the Artificial Intelligence Act AI does not include provisions on civil liability. It seems clear that liability should take account of the structure of markets for AI products and services and the IoT. Connected issue also arise about whether redress can be facilitated by providing victims with access to data, or reversal of burden of proof and how to ensure equity between parties by ensuring effective recourse liability.

Strict liability is the solution supported by both the High Level Expert Group and the European Parliament. Such an approach would be akin to liability for software/digital content. There will be some elements

93 European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL))
94 Art.4.
95 Art.4 (4).
where the failure of the AI algorithm is akin to non-conformity of digital content, and as we seek to preserve established values and principles, this would mean that strict contractual liability should also apply here. With the impossibility of determining exactly what causes an AI algorithm to take a rogue decision (whether due to “AI developers; algorithm trainers; data collectors, controllers and processors; ...and the final user...”97), we argue that strict liability should extend to all instances when an AI algorithm takes a rogue decision. In our view, this would provide the degree of predictability and legal certainty needed by putting the onus on the parties better placed to manage the risks associated with the development and deployment of AI algorithms. However, where there is evidence that user behaviour was a key cause for the decisions taken by the AI algorithm, or where this was the result of external data influencing the AI algorithm’s decision-making processes, a defence could be available. Of course, in the context of the Product Liability Directive, where the question of defect requires inter alia consideration of “the use to which [a product] could reasonably be put”,98 reasonable misuses might be covered99 unless clearly warned against. We are conscious that strict liability for AI algorithms might have a detrimental effect on innovation,100 but as strict liability is well-established in other areas of the law, we do not regard this as a sufficiently strong objection.

### 4.5 Data transfers

We have explained the importance of data101 for the operation of an AI algorithm within an IoT system. The data which determines the decisions by the AI algorithm can come from a number of sources. Many of the devices comprising the IoT system will have sensors which record and transmit data to the AI algorithm, as well as other devices in the system. Data may also be fed into the AI algorithm from external sources, whether from third-parties (such as a weather report, traffic information or similar) or directly from the user of the IoT system. We are not distinguishing between personal data and non-personal data in this section. The relevance of data protection legislation in respect of personal data is crucial, of course, but for our purposes, we do not need to consider this particular dimension.

98 Art.6(1)(b) PLD.
99 Cf. Recital 6, excluding only misuses “not reasonable under the circumstances”.
101 We are not distinguishing between personal data and non-personal data in this section. The relevance of data protection legislation in respect of personal data is crucial, of course, but for our purposes, we do not need to consider this particular dimension.
system. We have already highlighted the difficulty posed by the interaction of data and the AI algorithm for establishing liability for rogue decisions taken by the algorithm. Insofar as data is supplied by one of the devices which are part of the IoT system, a problem with the data provided by that device, particularly when caused by a malfunctioning sensor, can be an aspect of the device itself and therefore would be governed by liability rules applicable to goods (see above). This is because the sensor is a physical component of the device and the provision of incorrect data due to a physical problem relates to the device itself.

Here, we focus on the possible liability of a third-party supplier. There are several aspects to this. First, the legal basis for such liability would have to be established. If there is a contract between the third-party and the user of the IoT system, then it may be possible to base liability on that contract. In the absence of a contract, liability might arise in tort/negligence provided that the conditions for such liability are made out. In the case of contractual, there would have to be a clear legal requirement to be met, whether that be expressed in terms of “conformity with the contract” or reasonable expectations of the recipient of the data. Such a legal requirement would also have to provide for the limits to the liability of the supplier of such data: for instance, the data itself might be perfectly accurate and flawless, but be provided in a format or using units of measurements different from those used by an AI-algorithm. Data portability and interoperability are crucial for the ability to use data. Where data is not portable nor interoperable, the data would not be suitable for use by the AI-algorithm. If the accompanying meta-data contains relevant details regarding the format or unit of measurement in which the data is supplied, but the AI-algorithm does not recognise this, then it would not be appropriate to impose liability on the supplier of the data. However, if such meta-data were absent, then liability for incompatible data could fall on the supplier of data.

Secondly, there will be questions regarding the extent of such liability. If the data is not of the quality expected, then there might be liability for the difference in value, but this might not suffice to

---

103 Were such liability based on negligence, the limitations regarding recovery for pure economic loss might be a problem where no personal injury or damage to property is caused.
compensate the end-user of the IoT system for the losses which have actually been suffered. The key issue therefore will be whether there could be liability for consequential losses, including losses resulting from the malfunction of the IoT system, or for the possible corruption of the AI algorithm if the rogue data supplied by the third-party affects the self-learning process of the AI algorithm.

In the consumer context, strict contractual liability already exists in some jurisdictions. Both the UK’s Consumer Rights Act 2015 and the EU’s DCDSD/SGD define “digital content” as “data which are produced and supplied in digital form”. If the supply of raw data would fall within this broad definition, and consequently, the provisions on conformity of digital content and remedies for non-conformity would, in principle, apply to a contract between a consumer and a trader for the supply of data. However, there are no corresponding rules for non-consumer transactions.

With the current legal situation regarding the supply of data outside the consumer context at best uncertain, the publication of the ALI-ELI Principles on the Data Economy in late 2021 is an important step forward. Offering default rules to guide the development of the law relevant to the data economy, one important aspect is the idea of default quality standard regarding data supplied. In summary, data supplied commercially should be of a level of quality that would reasonably be expected, particularly with regard to matters such as accuracy, currentness, integrity, formats, and the inclusion of metadata and other specifications which will be needed to make use of that data. This would be subject to agreement to the contrary through the terms of the contract between supplier and recipient. This approach offers one way of providing greater legal certainty regarding the obligations of a data supplier. However, the Principles do not make specific provision for remedies where data is not of the quality reasonably to be expected, referring only to the relevant (contract law) rules of the law applicable to the contract under which data is supplied. Insofar as data falling short of the reasonably expected quality results in consequential losses, such as the malfunction of an IoT system, general rules of contract law on causation and remoteness would therefore apply.

104 S.2(9) CRA; Art.2(1) DCDSD; Art.2(6) SGD.
105 See discussion above.
106 See Principle 7(2)(b), in particular.
107 Principle 4(1).
5 TOWARDS AN ALTERNATIVE LIABILITY SYSTEM

In the previous section, we discussed many of the liability issues arising in respect of five specific features of an IoT system controlled by an AI algorithm. For some aspects, we can identify existing legal provisions; for others, the law is at best uncertain or at worst, as yet silent. Further legislative steps will therefore be needed to tackle the liability issues of both IoT systems and AI algorithms, and the combination of both.

A general difficulty is that liability has traditionally been imposed on the basis of recognised legal relationships, either through contract or on the basis of a duty of care in negligence. Inroads into bifurcation were made by specific products liability systems dealing with injury or damage caused by faulty goods, where liability is imposed on the producer of the product even where there would be no liability in contract or negligence.

Nevertheless, the complexity of an AI-controlled IoT system is such that an end-user faced with the consequences of a system malfunction will face the very challenging task of having to identify the appropriate party to be held responsible, and then the need to establish whether there is a legal basis for imposing liability on that party. The least-difficult situation would be one where the entire IoT system, including the AI algorithm, are supplied under one contract and no data supplied by a third-party is involved. Here, the contract between end-user and system supplier would probably be a sufficient vehicle to provide redress in respect of a system malfunction. However, one might expect that many IoT systems will not be supplied under a single contract, and that there will be multiple contractual relationships as well as contributions by third parties not covered by any contract relating to an AI-operated IoT system.

Whilst clarifying liability issues for AI and IoT systems would be a crucial and important step forward, we suggest that there is a need to be bolder in that a different liability system for AI-operated IoT systems should be considered. A departure from traditional systems of allocating liability would neither be radical or altogether new. Extended liability allocations are already found in a number of areas of law. Indeed, the Product Liability Directive, which places liability for personal injury and damage to property on the “producer” of the defective item, the notion of “producer” has been given a meaning reaching beyond the manufacturer (although not as extensively as
under U.S. product liability rules, where liability can even be imposed on online platforms in some instances. “Producer” is defined as covering not only the manufacturer of the final product, but also (i) the producer of raw materials; (ii) the manufacturer of components; (iii) so-called “own branders”, i.e., business putting their name or trademark on products manufactured by someone else; and (iv) an importer of the product into the EU (or since Brexit an importer into the UK). In addition, for circumstances where none of these parties can be identified, any other supplier of the product, including the retailer who sold the product to the consumer, is treated as producer. However, such a supplier can evade liability if it is able to identify one of the parties within the definition of “producer”. This broad approach to the notion of “producer” could be viewed as reflecting an underlying principle that a consumer who has suffered harm should have an easy route to redress by being able to claim against anyone who is treated as a “producer”. A key consequence is that the final producer is liable for the errors of others in the production chain, such as component makers and designers.

A different type of liability extension can be found in the EU’s Package Travel Directive (2015/2302/EU). Here, the “organiser” of a package travel contract (defined as “a trader who combines and sells or offers for sale packages”, or, put in more general terms, a person who assembles various elements to sell a package) is legally responsible for the performance of all the travel services contracted for, irrespective of who the ultimate provider of those services is. There is a legislative option for Member States to extend this also to the retailer (“a trader other than the organiser who sells or offers for sale packages combined by an organiser”). The organiser is obliged to provide a remedy where the contract is not, or cannot, be performed as agreed. Once the organiser has provided a remedy to a traveller, the organiser has right to seek redress from the party “which contributed to the event triggering” the obligation to provide a remedy.

---

108 See Oberdorf v. Amazon.Com Inc., 2020 WL 3023064 (3rd Cir. 2 June 2020) and Bolger v. Amazon.Com, LLC, 2020 WL 4692387 (Cal. Court of Appeal, 13 August 2020). An appeal in Oberdorf to the Pennsylvania Supreme Court was ultimately abandoned; an appeal in Bolger is pending in California at the time of writing.
109 Art.3 PLD.
110 Art.3(2) PLD.
111 Art.3(3) PLD.
112 Art.3(8) PTD.
113 Art.13(1) PTD.
114 Ibid.
115 Art.3(9) PTD.
116 Art.13(3) PTD.
117 Art.22 PTD.
remedy. Both the Product Liability Directive and the Package Travel Directive reflect an approach to liability which involves placing liability towards the final user on an easily identifiable person, and, in the case of the Package Travel Directive, a right for this person to seek redress from the person who contributed to whatever resulted in the problem.

There are further instances where liability is imposed on non-contracting parties (albeit not channelled towards one counterparty). Both UK and EU consumer credit rules permit a consumer to claim against a credit provider in respect of non-supply or lack of conformity. 118 And with regard to autonomous vehicles, UK law provides that liability for injuries suffered in an accident caused by an automated vehicle falls on the vehicle’s insurer. 119 The insurer can, in turn, bring a claim against the person who would otherwise be liable to the injured person. 120

There are therefore a number of precedents which justify developing extended liability approaches for AI-operated IoT systems, based on the twin features of offering the end-user an easy access to a counterparty and the behind-the-scenes channelling towards the parties responsible for the problem. We propose that a solution would be to push the boundaries of current liability approaches even further. Our starting point is to treat all of the various legal relationships connected to an AI-operated IoT system as part of a single network. 121 Proceeding from the recognition of such a network, an end-user faced with an IoT-system malfunction should not be required to identify the party responsible for the malfunction. Instead, it would suffice for the end-user to pursue either the network as a whole, comprising all of the contracting parties, or to pursue one of the parties comprising the particular network. The end-user would be granted an appropriate remedy (compensation, other remedial action, etc). Within the network, there would then either be a system for allocating a share of the costs to meet the end-user’s claim to each member, or the liability would be channelled towards the person or person(s) to whom

119 Automated and Electric Vehicles Act 2018, s.2(1).
120 Section 5.
responsibility can be attributed. In circumstances where it is impossible to pinpoint the exact cause of the IoT-system malfunction, spreading the costs among all network members might be the only solution. The basis for this would need to be determined and a formula for determining an appropriate proportion would have to be determined.

Where it is possible to identify a single cause, such as a failure of a physical device, or a software flaw, then ultimate liability would be imposed on that person, and other network members would be compensated accordingly. In short, our proposed liability system would allow the end-user to seek redress without having to face the severe difficulties associated with identifying the correct defendant(s) whilst providing for a recourse system between the network members to ensure that the loss is ultimately channelled towards the party/parties responsible. At least in the context of EU consumer law, this approach would be in accordance with values and principles already established in other contexts.

A further benefit of a network liability approach would be to obviate the need to consider difficult questions of proof. Instead of having to prove the precise nature of the defect and identify the party responsible for this, it would suffice for the end-user to establish that the IoT system malfunctioned and caused injury or damage, or economic loss. There would be no need to identify the particular element of IoT system that caused the damage.

We derive some support for our idea from a proposal by the High-Level Expert Group on Liability and New Technologies. It has proposed to impose a form of joint and several liability where several persons have cooperated in the “provision of different elements of a technological unit” where it is not possible for the injured person to identify which element of that unit has caused the damage in issue. The illustration given in the Expert Group’s report is that of an alarm system manufactured by one person installed as an add-on to a smart home system created by another person and running on an ecosystem produced by third person, and the alarm system


123 See point [29], p.55. According to point [30], determining whether an arrangement constitutes a technological unit involves consideration of “(a) any joint or coordinated marketing of the different elements; (b) the degree of their technical interdependency and interoperation; and (c) the degree of specificity or exclusivity of their combination.”
subsequently fails. Unless the cause of the failure can clearly be identified, all three persons would be jointly and severally liable to the home-owner. However, this would only apply where there has been co-operation between the parties – it would not work where the user of an IoT system has put this together on a self-build basis. Here, the various liability issues would continue to be relevant.

6 CONCLUSIONS

In this chapter, we have identified many of the liability issues which arise in an IoT system, particularly where this involves an AI algorithm. The IoT itself presents complex liability questions, and the addition of AI complicates matters further. It is very likely that any IoT system will involve multiple contracts dealing with different aspects, each of which could be a separate basis for allocating liability for a particular malfunction. However, as we have explained, the evidentiary burden on the end-user of an IoT system of precisely identifying the cause(s) of an IoT system malfunction is almost unsurmountable. Whilst one might tolerate this in the context of systems used commercially, it would certainly not be acceptable for consumer systems. We have therefore argued in favour of a liability approach which makes it easier for a (consumer) user to obtain redress whilst ensuring a “behind-the-scenes” right of recourse so that responsibility is ultimately placed on the party responsible for a malfunction.

A key requirement such a system is that liability questions regarding the various elements of an IoT system involving the use of AI are clarified, not least to ensure that there will be a legal basis for seeking recourse. We have made a number of suggestions in that respect. With both the European Commission and the English Law Commission considering reforms to accommodate liability issues in the digital age, we hope that these will be considered seriously.