Contracting for the 'Internet of Things': looking into the Nest

Guido Noto La Diega and Ian Walden *

Cite as Noto La Diega G. & Walden I., "Contracting for the 'Internet of Things': looking into the Nest", in European Journal of Law and Technology, Vol 7, No 2, 2016.

ABSTRACT

The world of the 'Internet of Things' ('IoT') is just one manifestation of recent developments in information and communication technologies ('ICTs'), closely tied to others, including 'cloud computing' and 'big data'. For our purposes, the 'Thing' in the IoT is any physical entity capable of connectivity that directly interfaces the physical world, such as embedded devices, sensors and actuators. In considering IoT contracts, this paper adopts a case study approach, examining the complexity of IoT through the lens of a specific product: the Nest connected thermostat, part of the Nest Labs business and owned by Google. We focus on the 'legals' of Nest (contractual documents, licences, etc.) to provide a case study of IoT complexity. After touching on some general contract law issues in relation to the IoT supply chain, we examine the rights and obligations represented in these legals and discuss the extent to which, collectively, they present a coherent and comprehensible private law framework. We then consider the extent to which certain statutory regimes may treat IoT contracts in terms of addressing two characteristic contractual concerns: liability attribution and unfair terms. Our main conclusion is that the world of IoT demonstrates a need to consider recasting the concept of product to reflect the frequent inextricable mixture of hardware, software, data and service.

Keywords: Internet of Things; IoT; Google; Nest; contracts; contract law; product liability; unfair terms; security; privacy; data protection; Terms of Service; privacy policies

1. INTRODUCTION

The world of the 'Internet of Things' ('IoT') is just one manifestation of recent developments in information and communication technologies ('ICTs'), closely tied to others, including 'cloud computing' and 'big data'. For our purposes, the 'Thing' in the IoT is "any physical entity capable of connectivity that directly interfaces the physical world, such as embedded devices, sensors and actuators". [1] This contrasts with other definitions that extend to virtual things, as well as physical, and can encompass the user. [2]

To examine IoT contracts different research perspectives could be adopted. We could engage on an empirical survey of the contracts used in the emerging IoT market; [3] embark on a theoretical study on contract law issues in an IoT context, or focus on a case study, examining the complexity of IoT through the lens of a specific product. It is the latter approach that this paper adopts. The case study is the Nest connected thermostat, part of the Nest Labs business, which was purchased by Google in February 2014 for $3.2bn. [4] Nest's main IoT products are a thermostat and smoke detector, although it has since launched a camera. [5] Nest was chosen simply on the basis that it appeared to the authors to be emblematic of the IoT revolution. Given the nature of the IoT environment, these products are inevitably designed to interconnect with an emerging array of other IoT products, known as the Nest ecosystem (or 'Works with Nest'), which includes cars, washing machines, lights, locks and communication devices. [6]

In this paper, we focus on the 'legals' of Nest Labs [7] to provide a case study of IoT complexity. [8] By 'legals' we mean the entire set of legal documents relevant for those who purchase the IoT device. The legal nature of each document varies and the set includes contractual documents, licences, notices, declarations, and reports. While acknowledging such variety, for the purposes of this paper we refer to them collectively as the 'legals' and focus primarily on the contractual aspects. [9] After touching on some general contract law issues in relation to the IoT supply chain, we examine the rights and obligations represented in these legals and discuss the extent to which, collectively, they present a coherent and comprehensible framework of private ordering. By private ordering, we do not mean simple compliance with agreements or their use to elude the law, [10] rather we consider contracts as one form of response to a legislative framework that always (and inevitably) lags behind technological developments, often resulting in regulatory lacunae. [11] As a consequence, looking at contracts is a legitimate and necessary field of enquiry for those who want to give an account of how law is operating in the IoT world.

In the second part of this article, we then consider the extent to which certain statutory regimes may treat IoT contracts in terms of addressing two characteristic contractual concerns: liability attribution and unfair terms. With regard to the former, the inevitable complexity of IoT products and their ecosystems may result in calls for the adoption of clearer liability rules for consumers; as represented by product liability regimes. For the latter, considerations of fairness may arise not simply from the unilateral imposition of inappropriate obligations (issues of substance), but also the unworkable multiplicity and layering of so many legals (issues of form). Both product liability and unfair terms are regulated at the EU level, which will be the jurisdictional perspective considered.

2. IOT AND CONTRACT LAW

Not surprisingly, many of the considerations that are valid for IoT contracts are equally applicable to the majority of ICT contracts. Such contracts can be notoriously difficult to understand for at least four reasons. First, they are often characterised by opaque wording incorporating a plethora of technological terms. Second, they have often been written with previous states of technological development in mind and thus are not wholly suitable for the new technology. Third, it is not unusual that the European version of a contract reproduces verbatim the contractual wording of the original US source. Finally, the multi-layered structure of the market can make it challenging to identify all the applicable contracts and to interpret them. [12]

On the two final points, we will say something more when analysing the Nest use case; it is sufficient to note that IoT contracts seem rarely to be drafted with EU law in mind. Moreover, the multi-layered structure of the market, which we have seen also in cloud computing contracts, can make contracts difficult to understand not only for consumers, but also for enterprise customers, due to a lack of awareness of all the actors involved.

In this web of legals, it is difficult to have a clear picture of the relevant documents, not only because it can be hard to find them, let alone read them, but also because they often claim to apply to just part of the IoT device, while they actually impact on its operation as a whole, or they purport to apply to a single IoT device, when they affect the whole cloud of things. [13]

IoT contracts also generate dependencies in two senses. On the one hand, in the constellation of IoT actors, where market power resides within the supply chain will vary considerably; from the retailer, to a software developer, a component manufacturer, or the cloud provider. On the other hand, the end-users are dependent in the sense of being locked-into a contract where there is no room for customisation (either at the moment of contractual acceptance or subsequently when you 'accept' every modification just by continuing to use the product or an associated service) and where interoperability and portability are very limited.

In 1990, Ray Kurzweil asserted that machine intelligence would become the same as that of a human brain, [14] while a year later Mark Weiser commented that computing was becoming ubiquitous and that "the most profound technologies are those that disappear". [15] These ideas provide a backdrop to the reality of the IoT. [16] In our modern commercial environment, lawyers have observed (and sometimes caused) a dehumanisation of the contract, with scant opportunities for authentic negotiation or customisation and everything shaped by the philosophy of adhesion: take it or leave it. [17] If the imposition of obligations for 'data protection by design and by default' [18] tells us anything, it is that a new frontier of law enforcement is technology. One could also envisage 'consent by design' [19] or 'awareness by design', where, for example, it would be feasible to disable the feature enabling the user to confirm that "I have read" the applicable terms when he could not have read them, e.g. an algorithm could measure the time spent on the page and scrolling through the text. Regarding awareness, we are seeing the emergence of applications that compare standard terms and alert users to any peculiarities in the documentation for due diligence purposes. [20]

Another contractual issue arises from the phenomenon of "things that sell things". [21] Although not that different from a vending machine that distributes drinks and snacks, [22] in an IoT environment the autonomy and decision-making ability of Things may develop to be of a qualitatively different nature. Brad, for example, is a toaster and a design

experiment named "Best in Show" at the 2014 Interaction Awards. Brad communicates with a social network of other toasters and wants to be used like the others: if one uses it less or does not even use it, Brad will try and draw the host's attention, until it eventually looks for a more suitable host. [23] In a time of consumerism and emancipation of the transaction from actual human needs, so-called 'smart' [24] things selling themselves may not seem such a dangerous idea. Our traditional understanding of property is a static one, whilst the IoT device can constantly evolve over time (whether automatically upgraded or downgraded) and as it develops an increasingly autonomous life it may, eventually, decide not to be our property anymore!

Lastly, it is worth noting the phenomenon of legal paternalism. It is widely recognised that European legislators have shaped consumer law on an assumption that the consumer is structurally the weaker party, incapable of fully understanding the contract and with no realistic prospect of being able to negotiate its terms and conditions. [25] This presumed asymmetry of bargaining power has resulted in laws and regulations that undermine the freedom of contract and has led to contractual remedies favourable to the consumer, to a point where it is possible to label the relevant political choice as paternalistic. [26] One of the few scholars who has dealt with IoT contracts has focused on this aspect, stating that "augmented reality calls into question leading justifications for distrusting consumer contracts - and thereby strengthens traditional understandings of freedom of contract as enforcing contracts as written". [27] The argument being made is that thanks to the IoT, consumers have ubiquitous real-time access to information about the places, goods, people, firms and contracts around them; therefore they can make more informed and conscious choices on a peer-to-peer level. The authors of this paper do not subscribe to such a view and do not consider the time has come to overturn the paternalistic approach to consumer contracts. Even with the tools available to consumers enabling them better to understand the reality; that reality has grown so much more complex with the IoT.

3. THE IOT SUPPLY CHAIN

We have already cast light on the multi-layered structure of the IoT ecosystem and some of its consequences. Providing a full account of all the actors in the IoT supply chain is beyond the scope of this research. One reason for the difficulties in achieving a shared definition of the IoT is that it encompasses a plurality of heterogeneous domains whose greatest common factor has not been found. One may talk about the actors in the healthcare sector, or in the transportation sector, energy or manufacturing, etc. Here, we examine the Nest product ecosystem as a use case, which helps narrow down the relevant supply chain to the smart homes environment (also known as 'domotics'). To simplify our analysis, we shall distinguish between the hardware, software and service components of the device; although, as we shall see, these distinctions are not necessarily sustainable or desirable from the perspective of the customer.

In its Terms of Service ('ToS'), Nest informs us that it "uses third party service providers to enable some aspects of the Services", but only provides an indicative list that includes Amazon Web Services ('AWS') for data storage, synchronization, and communication, and mobile device notifications through mobile operating system vendors and mobile carriers." [28] Mention of the use of other service providers, such as Rackspace for redundancy, [29] is scattered among the other legals, although it is not possible to assess whether all such subcontractors are listed. These 'third party service providers' also add to the legals that would require review were a comprehensive review to be carried

out. [30] The need to have transparency about subcontractors raises issues from both a legal and security perspective. From a contractual perspective, the customer is unable to identify the parties upon whom the service is dependent and therefore who may potentially be liable in the event of loss; while from a data protection perspective, knowledge of processors and sub-processors is seen as a pre-requisite for a data controller to ensure compliance with its obligations. [31] In terms of security, an absence of transparency would seem to substitute confidence with reliance on good faith and ignorance.[32]

To understand the complexity of the supply chain, it is useful to read the Nest Developer ToS, [33] which alert the developer that the "Nest API and other Nest Developer Materials may allow you [the Developer] to control Nest devices and software or gain access to certain information, which *may impact the safety of Nest customers and end users* of Nest's products and services" (emphasis added). [34] Customers may not expect that connecting their Nest products to third-party apps and devices can let third parties control their own product and affect their safety, therefore it is critical that this information is also stated clearly in the third party's ToS and privacy policy.

As people are at the centre of every IoT model, unlike the traditional machine-to-machine ('M2M') realm, it makes sense to start with them when describing the IoT supply chain, even though the end-user does not generally have significant power in the value chain, [35] above all because they usually have reduced control over the data flows. [36] Clearly the central person when it comes to a smart thermostat is the end-user, who is the main data subject (and sometimes data controller as well). However, two further distinctions of legal consequence need to be made. First, the end-user may be the contracting customer or a third party, such as a family member. Second, the device itself may be owned by the customer or may be leased to the customer by the supplier (or provided as part of rented or leased premises). In the case of ownership, the distinction between the device and the associated services becomes critical, because the Nest ToS states that if the device owner does not agree with the terms "you should disconnect your products from your account […] and cease accessing or using the services". [37] This raises an issue concerning the status of a 'disconnected IoT device'. Where the customer does not own the device but is simply leasing it, then the issue is relatively straightforward, since the contract can simply require the customer to return the device to the supplier. However, where title in the device is transferred to the purchaser, as in the case of Nest, [38] then the issues can be more complex. In terms of UK contract law, statute implies a term into the contract that the purchasers of goods will "enjoy quiet possession", [39] which term would be potentially breached if when the Nest device were disconnected it loses most of its functionality. [40] Indeed, in May 2016, when Nest announced it was to cease offering and supporting the Revolv app and hub device, which enabled users to control their IoT home devices, it offered a refund. [41] From a regulatory perspective, a contractual rule that restricts or prohibits use or reconnection of an IoT device could fall foul of competition rules. In the broadcasting sector, for example, *ex ante* intervention exists in respect of access control systems in television set-top boxes to ensure certain public interest objectives are met, specifically access by competitors and user access to certain content services. [42] One could envisage for certain IoT products considered integral to our daily lives that regulatory intervention may be deemed necessary, in the form of a 'must provide' obligation, to safeguard certain public interests in the event of IoT disconnection.

Any IoT supply chain will have a range of actors who are dependent on the smart hardware device. In terms of the manufacturer of the 'thing', most IoT products will be compound, with different manufacturers responsible for different aspects of any "thing of things", such

as a smartphone. Even when there is simply one thing, during the process of manufacturing a lot of different people will be involved, contributing components and facilitating the production process.

As with many large companies, Nest also has established a network of resellers, [43] retailers, wholesale distributors, [44] and installers. Resellers have to enter into the "Nest Pro" agreement, the terms of which are not publicly available. As regards installers, even though Nest "maintains a list of recommended installers of the Products on its website", [45] it declares that it is not "responsible for any conduct of or liability associated with these installers".

Unsurprisingly, Nest as the central actor responsible for the device as well as the services and software, is in reality a shorthand for Nest Labs Inc. and its various affiliates and subsidiaries, such as Nest Labs (Europe) Ltd. When it comes to services, the supply chain becomes even more complex. We have already referred to the cloud providers (AWS and Rackspace), but there are also the analytics tools provided by Google Analytics (a 'third-party' despite being part of the same group of companies), the credit card processing service provider CyberSource, [46] and advertising services provided 'by third-party ad partners, such as Google Display Network and AdRoll' (WPP). [47] Another service is 'Safety Rewards', [48] even though it is not mentioned in any of the legals, in which Nest is partnered with leading insurance companies. [49] Similarly, Nest partners with 'energy partners', npower for the UK, whose services are based on machine learning technologies (so-called 'Auto-Tune'), from which peculiar liability issues may arise. [50] Even though the US legals mention them and the UK ones do not, there are 'Customer Agreements for Rush Hour'[51] and 'Customer Agreements for Rebates' [52] with Nest energy partners that will share data with Nest, which in return, "may also collect your energy usage and pricing data from your energy provider." [53] These energy partners are apparently "helping to subsidize all the processing power required to implement Auto-Tune, which needs a huge amount of memory, storage and processing power, all maintained in the cloud." [54]

To complete the supply chain picture, one should also mention the website developer and webmaster, the 'app' store, [55] the embedded software developer(s), other software providers, the facilitators of communication between things, the rights-holders, the eCommerce platforms, [56] and the network operators.

4. THE NEST USE CASE

A consumer [57] interested in a thermostat does not expect to face a legal mountain. However, if a UK-based customer wants to have a comprehensive picture of the rights, obligations and responsibilities of the various parties in the supply chain, he has to read at least 13 legal items.[58] The main documents are:

- The Terms of Service ('ToS'), with 'Nest Labs, Inc. and its subsidiaries and affiliates (collectively, "Nest")', covering sites, web apps, mobile apps, and 'subscription services'; [59]
- The End-User Licence Agreement ('EULA'), with 'Nest Labs, Inc', including embedded software; [60]
- The Terms & Conditions of Sale ('T&Cs'), with 'Nest Labs (Europe) Ltd', covering hardware and certain aspects of the services;
- The Limited warranty ('Warranty'), with 'Nest Labs (Europe) Ltd';

- The Privacy Statement, regarding information relating to the operation of Nest products and services ('Privacy Statement'); [61]
- The Website Privacy Policy ('WPP') for information collected through the websites, including the online store; [62] and
- The Security policy. [63]

It may also be important to read also the Open-source Compliance notice, [64] the "Intellectual Property and other notices", [65] the Community Forum Agreement, [66] the Transparency Report, [67] the EU Declarations, [68] the Installation ToS [69] and the Developer ToS.

To these documents one can add the legals of the partners, affiliates, etc., plus those of the actors of interoperable products (both the "Works with Nest" realm, as well as interoperable apps), [70] and some Nest documents that are not published, such as the Nest Pro agreement and the terms of the free trials of subscription services. [71]

Unsurprisingly, the list goes on. In fact, the essence of the grand vision of the IoT is the idea of a network of things (and people). In the Nest use case, this is epitomised by the section "Works with Nest", [72] which is - in the ambitious words of the company - "about making your house a more thoughtful and conscious home." Nest suggests a number of devices and apps that interact with the thermostat, the smoke alarm and the camera, thus ensuring "personalized comfort, safety and energy savings." So, for example, one can simply speak the command: "OK Google. Set the temperature to 75 degrees" and the thermostat will do as you say. In addition, with Google Now, you can be on your way home and your thermostat will start heating or cooling before you get there. Too lazy to speak? No problem, your Mercedes-Benz automatic car adapter will tell your thermostat to start getting your home comfortable before you arrive. The new version of the thermostat can even control your boiler. [73] The list of useful connections is continually growing, encompassing smart sprinklers, webcams, locks, sleep systems and lights. All these apps, devices and appliances send data to Nest, as well as receiving data from Nest on terms that are not easy to understand, as one has to cross-refer to the Nest Privacy Statement, the Nest WPP and third-party privacy policies. [74] If you add to Nest legals those of the connected devices, apps and appliances, the result is that for what appears to be a single product, a thousand contracts may apply!

The following subsections examine some of the key themes that operate across the legals, in terms of understanding what comprises the Nest, how it handles and secures your data, which laws apply and where and how a dispute would be handled.

4.1. THE CONCEPT OF PRODUCT

One of the main conclusions of this research is that a new legal conception of a 'product' may be required in the context of the IoT. Even though the ToS professedly apply only to the Nest-related services [75] and not to the Nest hardware, what is left when one is obliged to disconnect the product from the account and to cease accessing and using the service, because one disagrees with or cannot accept the provisions of the ToS? [76] The end customer's ability to use the hardware's functions would be profoundly affected.

The same thing happens to the concept of product under the T&Cs. Originally, they referred only to the Nest product as hardware, but now they openly cover both the product and any subscription services, [77] notwithstanding the fact that the ToS "constitute the entire

agreement between you and Nest regarding the use of the Services", which include also the subscription services. [78] This is confirmed in the "Privacy Statement", where it says: "Nest Products also include our Web Apps, Mobile Apps, and Subscription Services" (were the websites not covered by the WPP?). [79]

It is then useful to look at the EULA. If the customer does not agree with its provisions, they simply "should cease accessing or using the product software" (the same happens if you do not consent to software updates). Not only can the customer not modify the agreement, but the company has the right to modify it "without providing any additional notice or receiving any additional consent." [80] If you do not want such updates, "your remedy is to stop using the Product." [81] The situation is slightly better for the T&Cs, since amendments should not affect the customer's position, given that "Every time you order Products from Nest, the Terms & Conditions in force at that time will apply between you and Nest." This rule, however, does not apply to the subscription services, in which case Nest will notify changes affecting the subscription. [82]

From the above, it would seem that this IoT product has become an inseparable mixture of hardware, software and service. Despite attempts through the legals to distinguish the different elements, this has become untenable. This convergence has, we would argue, implications for the applicability of consumer protection laws, discussed further below.

4.2. SECURITY, PRIVACY AND DATA PROTECTION

Data security is already an increasingly 'hot' topic for the Internet, but it becomes utterly critical in an IoT context for at least two reasons. [83] First, IoT is not only about sensing, but also about actuating; this impact on the physical world may result in greater risks for personal safety (e.g. hacking a smart vehicle can cause a car accident). [84] Second, with the IoT the Internet is everywhere (or 'everyware'), [85] in every nook and cranny of private spaces (home, office) and also constantly with you (wearables, ingestibles, etc.). Potentially (but not necessarily), this means the generation of much more data (big data) and more intimate data. Thanks to the dynamic flow of information within the IoT system and potentially between systems, [86] it is also easier to infer personal data even from raw data, while benign streams of personal data can become sensitive once combined.[87] Let alone the latest developments in cross-device tracking. [88] It is therefore not comforting to read the EULA and discover that the company "makes no warranty that the product software will be uninterrupted, free of viruses or other harmful code, timely, secure, or error-free"; particularly if that fault leaves you in the cold! [89] Once again, the distinction between hardware and software in an IoT context dissolves; software insecurity may mean physical insecurity.

Further security issues may arise from two other characteristics of the IoT. First, the Thing may be capable of being controlled in a number of ways that could conflict with each other, leading to unexpected actions and potential harm. This issue will be exacerbated where there is a multitude of users (e.g. family members) who have different preferences. For instance, while Apple's Siri cannot control the Nest thermostat, it can control the Philips Hue lights that in turn can control the Nest thermostat, which can be controlled manually, as well as via the Nest app, the website or third party-apps and devices, such as 'Kontrol' an app designed for communication between the Apple Watch and Nest products. Second, IoT products are being equipped with a greater range of sensors, although the information they gather may not be consistent which can have consequences for actuation. For instance, the Nest smoke alarms feature 'Wave', whereby one could switch the alarm off by waving the

hands. As of 3 April 2014, the feature has been disabled, because "movements near Nest Protect that are not intended as a wave can be misinterpreted by the Nest Wave algorithm. If this occurs during a fire, this could delay the alarm going off". [90]

One of the main problems stemming from the labyrinth of IoT contracts is that it is difficult to understand the protection actually granted to a user's personal data. It is not always possible to read and interpret the scattered provisions; while, when gathered together, they do not provide a uniform level of protection. Moreover, there are some differences between what Nest declares publicly (thus creating an expectation in the minds of customers) and what the legals state. For example, with respect to the microphone on 2nd generation Nest Protect devices, while the website reassures visitors that the microphone is used exclusively for the sound check and that no data are sent to Nest servers, the Privacy Statement only states that "Nest Protect emits sound samples during Safety Checkup or Sound Check that the microphone will capture to verify that the speaker and horn are functioning." [91]

The Nest Privacy Statement notes that "once this information is shared with the particular Third-Party Product and Service, its use will be governed by the *third party's privacy policy and not by Nest's privacy documentation*." [92] (ToS). Even though one would naturally be led to think that 'third party' refers to the realm of 'Works with Nest', there is a broader and indistinct universe that needs to be taken into consideration. In fact, one feature of the last update to the Nest legals is a provision whereby the company states that it will share information with and receive information from unspecified "third parties outside of the Works with Nest program" [93], and that some of this information may be associated or stored with the user's Nest account. Information will be pulled without the customer's awareness, whereas "Nest may *also* share information with your permission" (emphasis added).

Furthermore, in the IoT it is difficult to identify who the controller is and who the processor is for data protection purposes. [94] The Nest ToS state that "You agree that you (and not Nest) are responsible for ensuring that you comply with any applicable laws when you use the Products and Services, including, but not limited to, (i) any laws relating to the recording or sharing of video or audio content that includes third parties, or (ii) any laws requiring notice to or consent of third parties with respect to your use of Dropcam/Nest Cam." [95] (ToS) Such a provision implies that the customer is considered by default as the controller, which contrasts with the reality of much of the data processing occurring in the IoT.

Data security can be hindered by the peculiar nature of the product in an IoT environment. If the thermostat was merely a simple piece of hardware, it could be defective at the moment of the purchase or stop working at some point, but there would be no security problem. The fact that IoT products are a mixture of hardware, software and services means that weak or reduced security of any one of these elements will probably impact on the others. So, for example, Nest declares not to have any "responsibility to provide maintenance or support services with respect to the Product Software." (EULA). From this it follows, that if there is no more maintenance or support, the thing as a whole can become open to external integrity attacks.

The Privacy Statement does not say much about security. It states that some information is processed and stored directly on the Nest device (and other information on cloud servers, e.g. using AWS's S3 cloud service) and that "All personal information is *encrypted as it is transmitted* to Nest and cannot easily be accessed" (emphasis added). [96] This begs the

question of how data 'at rest' are protected. Moreover, Nest says it complies with the US-EU Safe Harbor Framework and the US-Swiss Safe Harbor Framework, as set forth by the US Department of Commerce. [97]

The WPP is more detailed and strikes a balance between security and Nest's commercial interests, with the balance appearing to incline in favour of the latter. In fact, the physical, administrative, and technological methods to transmit the data are those considered "commercially reasonable." [98]However, again as stated in the ToS, Nest admits that it "cannot guarantee that unauthorized third parties will never be able to defeat our security measures or use your personal information for improper purposes." [99]

Another point that is often stressed relates to the physical location of data. [100] It is useful to underline that by signing the Nest contract, the customer acknowledges that his personal data will be transferred to the United States and the fact itself of providing the data is considered equivalent to the expression of an informed consent. Here we can see another example of the complexities of interpreting all the legals. Why does the WPP inform us about the transfer and obtain our consent, exempting Nest from its obligation not to transfer data to a country without an 'adequate level of protection'; while the Privacy Statement stresses adherence to the relevant Safe Harbor Privacy Principles, which is intended to establish 'adequacy'? [101] To a certain extent, this represents a common legal response to a regulatory environment, providing a range of possible justifications or defences to reduce the risk of non-compliance. However, the compound nature of IoT legals is likely to exacerbate this issue and, from a data subject's perspective, a multiplicity of conflicting messages would seem to undermine and confound any expectation they may have about the basis for the processing and the protections offered.

It has recently been forecast that "every IoT-enabled device, whether an iron, vacuum, refrigerator, thermostat or light bulb, will come with terms of service that grant manufacturers access to all your data." [102] This may sound like mere conjecture, but it is not pure science fiction. Nest informs us that the product "regularly sends the data (…) to Nest" (Privacy Statement). However, which data are stored 'on-board' the device and which on Amazon's S3 cloud platform? The legals inform us of the storage itself (WPP) but not the location, although we are told in the security policy what data is held on the device itself. [103] The granularity, quality and quantity of personal data stored will depend on the type of product; for instance, the Nest Cam, especially if one subscribes to Aware, enables the company to "capture, process and retain video and audio data recordings from your device for the duration of your recording subscription period." [104]

On the basis that everything can be sent to Nest (and thereby to AWS), it is important to know that not only Nest vendors, service providers, and technicians who help with some of the processing and storage can "access certain information about you or your account" [105] , but so can "Nest employees". Moreover, it is not even clear if this can happen exclusively for external processing purposes: the access is envisaged not simply *for* that purpose, but *in line with* it (with the blurred boundary phrase of "non-Nest purposes"). In addition, while listing the situations where the company states that it shares personal information, this issue is kept separate by the reference to 'external processing'. Besides, Nest declares that is has strict policies and technical barriers in place to prevent unauthorized employee access to video data. One may question why these measures are confined to video data and to employees and why Nest does not conform to Google's policy of strict contractual confidentiality obligations. [106]

Regarding data sharing, which may occur locally among devices, between Nest Products and the customer's mobile device or application, or on Nest's servers, three more justifications are given. First, explicit consent, where Nest makes sure that "you can change your mind at any time" (WPP). However, if one does not give consent to the exchange of data with third parties providing products and services, use of those products and services will be impossible. [107] The same applies to sharing with partners (e.g. energy and insurance companies). This seems to ignore that processing 'necessary for the performance of a contract' is an equally valid justification under data protection law. [108]

Even before that, there is a technical reason why consent and awareness are threatened in the IoT. As stated also by the UK Information Commissioner's Office (ICO), [109] IoT devices often have no physical interface through which an individual can set, interact and control information flows, consequently one might question if the consent qualifies as valid and informed. On this point, it is important to stress that the Developer ToS bind the developer to "provide and adhere to a privacy policy for your Client that (…) is conspicuously displayed to all end users of your Client." [110]

Another justification is labelled "Business Transitions". It refers to the possibility of the sale or transfer of the Nest company or of all or part of its assets: in this case, the purchaser will be requested to treat the data in a manner consistent with the Privacy Statement in place at the time of its collection (even though it is unlikely that this point would be a deal-breaking clause).

Lastly, Nest reserves the right to share information in the case where it "believe[s] in good faith" that there are "legal reasons" to do so. This appears to us as one of the most risky clauses of the legals relating to personal data. Its wording is significantly different from the average contract, where one usually finds expressions such as "legal requirement" [111] or "legal process", [112] let alone the cases when the company guarantees not to hand over user data to authorities unless a warrant issued by local court is presented." [113]

While it is true that the Nest WPP specifies the legal process and commits to comply with state and federal laws, this is only provided as an example. Moreover, the fact that the example offered is from a US perspective ("with state and federal laws or the applicable laws of foreign countries other than the United States"), notwithstanding that the document is for the UK market, is evidence that the Nest legals are US-originating contracts that have been simply (and softly) adapted to a European context. [114]

It is well known why strict wording is important when it comes to disclosure of personal data. Law enforcement agencies (LEAs) can use laws with extraterritorial effect to force not only companies based in the US into handing over user data (including preventing notification to customers about whom Nest has been asked to disclose data). An order can be addressed also to European subsidiaries having parents in the US, or to EU companies using the services of a US subsidiary for data processing, or, again, using any third-party to store or process data in the US. [115] The last case occurs in the Nest scenario and the conflict with EU law does not necessarily guarantee non-disclosure. [116]

As we have already underlined, part of the essence of the IoT is networking between things, often mediated through cloud services. [117] This means that things talk to each other. One should not be surprised then, when it is discovered that the thermostat "pulls information directly from your heating and cooling (HVAC) system" (Privacy Statement). And this is not the end, because obviously Nest products talk to other Nest products (and to the immense

realm of "Works with Nest). Consequently, "the products will share certain information with each other" (Privacy Statement). It is also noteworthy that the communication in the smart home does not entirely rely on one's house connection to the Internet. In fact, Nest Protects operates on Nest Weave that uses 802.15.4 and Wi-Fi 802.11 b/g/n; therefore, multiple products can remain connected to one another even if the household's connection to the Internet stops working. [118]

Now, one might imagine reacting to the massive collection of data with a sort of private enforcement of privacy by design. [119] There are many tools that aim at shielding the customer from being tracked. An example is the "Do Not Track" option provided by a browser. [120] It is important not to rely on such methods. Nest informs its users that the selection of the mentioned option "*may not have any effect on our collection of cookie information* for analytic and internal purposes" (WPP) (emphasis added).

This warning leads us also to the purpose of data collection via IoT products. Google has warned that "A few years from now, we and other companies could be serving ads and other content on refrigerators, car dashboards, thermostats, glasses and watches, to name just a few possibilities." [121] As far as we are aware, advertisements are not currently displayed on Nest products, but the data from these products are nonetheless used to advertise. Even though Nest repeats several times that the information is used to provide users with Nest products and services, under this *leitmotiv* is buried what is really important: the commodification and the commercial use of the users' personal data. In fact, what is collected is used "to provide advertising that is relevant to your interests" (WPP).

This can deeply affect the customer's privacy, given that once again the multi-layered structure can act as a disclaimer of responsibility. As unsurprising as it may be, Nest warns that it permits third-party advertising partners to use cookies and other technology to collect information and that "we have *no control over and cannot confirm whether these third party ad parties honor the Do Not Track* browser signal" (WPP)(emphasis added) [122]. Furthermore, the fact that advertising is part of the contract can additionally threaten the customer's privacy. Let us not forget, indeed, that the processing of personal data is lawful even without consent if necessary "for the performance of a contract to which the data subject is a party". [123]Consequently, with all the activities of processing, tracking and profiling forming part of the contract, the company could easily claim that the customer has no right to prevent such processing of their data.

Finally, it should be recalled that the IoT is not only about sensing and sending/receiving data, it is also about actuating. Actuation can affect both the physical environment and the processing of data. A good example is provided by a change in the most recent update to the ToS, whereby "you acknowledge that *Nest may activate Bluetooth on your smartphone or tablet*, with or *without prior notification*, in order to facilitate proper operation of the Services; enable communication with Nest Products connected to the same Nest account and enable certain features (such as remote silencing of a smoke or CO alarm on Nest Protect)" (emphasis added). [124] It is arguable that customers need to be aware that the IoT is not only a matter of people controlling things, but also things controlling people.

4.3. APPLICABLE LAW AND JURISDICTION

When it comes to any contract, an important issue is the applicable law and jurisdiction. This has some unusual aspects in an IoT context. A customer who looks at a thing is likely to believe that the thing is located geographically in the place where the customer is. But what if I have a US device sold in Venezuela, whose embedded software runs, say, in Ireland, whose smartphone app is provided by a Chinese company, whilst the customer accesses the relevant account in Tunisia: Where is the thing?

The contract might provide some assistance. However, this is not the case in the Nest scenario. Under the EULA and the ToS, California Law applies, even though the "courts in some countries will not apply California law to some types of disputes", presumably due to overriding mandatory rules of the state where the user is located, [125] whilst under the T&Cs Irish Law applies.

Once again, one notices a fabricated separation, this time between embedded software and apps and services. In a case regarding a single IoT product, a judge may be required to create a novel expression of existing laws by applying fragments of Californian law and fragments of Irish law.

On top of everything, the Limited Warranty, which professedly concerns the product only as hardware, [126] states that "For a full description of your legal rights you should refer to the laws applicable in your jurisdiction". This clause can reasonably be interpreted as referring to the law of the customer's jurisdiction, whether under consumer protection law, private international law or otherwise. Therefore, even for issues related to the same part of the product (the hardware), the judge should apply different pieces of legislation. The importance of ascertaining the applicable law is well illustrated by the Limited Warranty. As a matter of fact, the disclaimers, exclusions, and limitations of liability under the Limited Warranty will not apply "to the extent prohibited by applicable law", not to mention that "to the maximum extent permitted by applicable law, Nest Labs disclaims all express, implied, and statutory warranties" and that "to the maximum extent permitted by applicable law, Nest Labs also limits the duration of any implied warranties or conditions to the duration of this limited warranty."

The judge therefore needs not only to determine which is the applicable law, he also has to create it by the combination of different pieces of legislation and clarify what is "the extent prohibited by applicable law", a clause so unclear it can be hardly be considered reasonable and fair. While such phrases may not be novel in commercial agreements, and are indeed widely present in the ICT sector, the compound nature of the IoT lends such phrases an enhanced opaque quality.

The collection, processing, and storage in non-EEA countries (namely in the US and in unspecified "other countries where our servers reside") [127]give rise to considerable problems. In fact, as a result "your personal information may be subject to legal requirements, including lawful requirements to disclose personal information to government authorities, in those jurisdictions" (WPP). [128]

Applicable law and jurisdiction are connected issues. IoT contracts often include arbitration clauses in which both the applicable law and appropriate forum are designated, while also indicating that certain matters may be litigated rather than arbitrated. Both under the ToS and the T&C, for example, Nest customers submit themselves to binding arbitration and

further agree "arbitration is final and binding and subject to only very limited review by a court" and accept to waive the right to any form of appeal, review or recourse to any court or other judicial authority, insofar as such waiver may be validly made.

At the same time, a trial could be initiated before at least three different courts. As a matter of fact, any action or proceeding relating to the ToS and the EULA must be brought "in a federal or state court located in Santa Clara County, California", but only the latter provides that Nest may seek injunctive relief "in any court having jurisdiction to protect its intellectual property or Confidential Information." As regards the disputes under the T&Cs, then, "The courts of Ireland will have non-exclusive jurisdiction" and customers may have the right under relevant consumer protection laws to bring proceedings in their country of residence (the reference is clearly addressed to a consumer). For the EULA, whereas the Court of Santa Clara County will (theoretically) judge on cases regarding apps and services, the Court of San Francisco will judge if one sends a counter-notice under the Digital Millennium Copyright Act (DMCA), claiming that the "user submissions" (mainly user-generated content) that was removed (or to which access was disabled), does not infringe the DMCA. [129]

So there would appear to be as many applicable jurisdictions as the number of legals. Therefore, in respect of the Nest product, it seems that one should initiate a dispute before different courts and it may also happen that even though the same right is at stake (e.g. copyright) different courts may claim the jurisdiction. There is a real quagmire here.

5. PRODUCT LIABILITY

Product liability regimes address the attribution of liability between the producer of a product and the person using that product. They represent a departure from traditional contractual and tortious rules under which an injured party in litigation has to prove that the defendant is either in breach of contract or at fault and in breach of a duty of care towards the claimant. By contrast, under product liability law, the injured person is not required to adduce evidence of either a contract or any fault, and will usually be able to bring a claim against a broader category of persons. By imposing strict liability, the law increases the risk of liability for the producer; enhances protection and the possibility of redress for the consumer and, as a by-product, should ensure the safety and quality of products sold on the market. [130]

In Europe, the product liability regime dates back to a 1985 Directive, [131] which was seen from the outset as a response to "solving the problem, peculiar to our age of increasing technicality, of a fair apportionment of the risks inherent in modern technological production". [132] The regime cannot, therefore, be dismissed as not being intended to cover recent developments such as the IoT. However, the rules regarding liability for defective products seem to have been somewhat neglected over recent years, [133] due in part to the growth of our service-based economy, which includes the Internet and more generally intangible digital products and services. [134] Indeed, it has been noted that while the liability model established under the Product Liability Directive has been hugely influential internationally, to date "the practical impact of its ideas has been close to negligible." [135]

Although the Product Liability Directive has been relatively dormant, the Court of Justice has recently been asked to consider its application in a case involving health-related IoT devices, in the form of 'pacemakers and implantable cardioverter defibrillators'. [136] While it is too early to predict with any certainty, the implications of this decision for product

liability regimes may be very significant. [137] With the explosive growth of the IoT market, and an expansive concept of 'product', we consider the possibility of a revival of product liability. On this basis, it is worth examining the EU regime and considering its applicability to our case study, Nest.

In *Boston Scientific* products contained a defect that could result in premature battery depletion and subsequent loss of certain functionality, including telemetry, i.e. transmitting recorded data to an external device. Following identification of the defect, the supplier offered their replacement free of charge. However, claims were made for compensation in respect of the costs of the implantation of the original faulty products. The first issue for consideration by the court was whether a "product belonging to the same group or forming part of the same production series"[138] could be said to be defective under Article 6(1) without the need to evidence that the specific product was defective. The court held that it could, especially given the nature of the product and the high expectations of users of that product. Second, the court was asked to determine whether damage under the first limb of its definition, relating to death and personal injury, [139] extended to the surgical procedure required to replace the defective device. The court held that it did, but only if the operation was necessary to overcome the defect. [140]

The Product Liability Directive is applicable to 'products', which is defined as all 'movables', even when incorporated into another movable or immovable, and including electricity. [141] Further clarity around this definition may be found in the instruments transposing the measure into national law. In the UK, for example, a product includes "a product which is comprised in another product, whether by virtue of being a component part or raw material or otherwise". [142] In a Nest and IoT context, therefore, a key issue is to what extent the 'product' can be said to include its intangible component parts, specifically the software and data. The Commission saw the Directive's definition as extending to software, but not services, with Lord Cockfield noting that the Directive "applies to software in the same way….that it applies to handicraft and artistic products".[143] Notwithstanding the Commission's statement, uncertainty about the application of the Directive to software has persisted over the years, partly from the fact that software may be considered a service in certain circumstances. [144] While UK law is also unclear, the concept of a 'product' includes that whose "essential characteristics of which are attributable to an industrial or other process having been carried out." [145] This would certainly seem applicable to a product's integrated software. However, to date, there has not been any European case applying the Product Liability Directive directly to software, which has exacerbated the uncertainty.

The Nest legals have chosen to expressly distinguish the software from the 'Product', with the 'Limited Warranty' stating that it "does not cover consumable parts, including batteries, unless damage is due to defects in materials or workmanship of the Product, *or software (even if packaged or sold with the product)*"(emphasis added). [146] The validity of this exclusion would seem to depend not on Nest's ability to distinguish between hardware and software within the product, but rather on the basis that while Nest Labs (Europe) Ltd is acknowledging that it is the producer of the hardware, and hence liable for any 'defect', it is not accepting this role in respect of the software, which, by virtue of the EULA, it would argue was produced by Nest Inc. Whether such a position would be vulnerable to challenge is debatable, as it is certainly a lacuna in the protective regime; but, if accepted, the treatment of the software itself as a component part of a product would continue to be an arguable point.

One of the main concerns for customers of IoT products is that the multi-layered structure of the supply chain could effectively act as a disclaimer of responsibility. Put simply, there is a risk that the manufacturer of the hardware claims that the software developer is the real party responsible for any defect, or tries to shift responsibility to the service provider. Under a strict liability regime, this should not be allowed. Under Article 3 of the Product Liability Directive, the concept of the 'producer' is multi-layered, to prevent any shifting of responsibility. In the first instance, it means the manufacturer of the finished product, or the manufacturer of a component part, or any person who presents himself as its producer, by putting his name, trade mark or other distinguishing feature on the product. [147] Next, where the product is imported and distributed in the territory, that person is deemed responsible as producer, which extends the territorial application of the Directive to foreign products. [148] Finally, where neither the producer nor the importer can be identified, then the supplier is considered the responsible producer, unless he can identify the producer, the importer or the person that supplied him within a reasonable time. [149] Such an inclusive and broad concept would seem perfectly applicable to the characteristic of IoT markets, where nearly all things are composite things. However, in relation to certain technological developments, such as 3D printing, the emergence of 'prosumers' may challenge existing regulatory concepts. [150]

Under the Product Liability Directive, the injured person has to prove three things: the defect, the damage and the causal relationship between the two. [151] Of these, the first and last can be significant hurdles to overcome. With regard to defects, the threshold is that the product does "not provide the safety which a person is entitled to expect, taking all circumstances into account". [152] What constitutes a reasonable expectation may obviously vary considerably depending on the market segment in which the IoT device is deployed. In *Boston Scientific*, the Court held that such expectation must be assessed on the basis of "the intended purpose, the objective characteristics and properties of the product in question and the specific requirements of the group of users for whom the product is intended." [153] With regard to the specific devices under consideration, the Court felt that an expectation of a near zero failure rate in an implantable device would be reasonable for patients, even though medical experts are aware that such devices are not free of the risk of failure. [154] To date, who bears the burden of evidencing that a defect exists has varied considerably across the Member States. [155] However, following *Boston Scientific*, it now appears sufficient for the claimant to demonstrate the risk of a defect or the 'potential for failure', rather than that a specific device has a defect, which significantly lowers the threshold. [156]

A producer can also raise various defences, the most relevant of which in the context of IoT devices is:

> "that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered". [157]

This provision, commonly known as the 'development risk' or 'state-of-the-art' defence, was seen as a compromise between the interests of consumers and facilitating innovation. [158] Since 1985, debate has continued over the relative costs and benefits of this provision for both consumers and producers. It has been held that this provision does not require consideration of the "practices and safety standards in use in the industrial sector in which the producer is operating", which would be a consideration under a traditional negligence analysis, [159] but instead requires a more holistic perspective involving

considerations of accessibility. [160] Legislators were evidently aware that this defence could provide producers with too much wiggle room, especially in rapidly evolving sectors such as ICTs, where states of industry knowledge can be very difficult to determine with certainty. They therefore provided Member States with an option to exclude this defence, such that a producer would be liable "even if he proves that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of a defect to be discovered". [161]

Evidencing the causal relationship between the defect and damage can also be a challenge, particularly when complex technologies are involved. In *Hufford v Samsung Electronics (UK) Ltd.*, [162] for example, the claimant was unable to discharge the burden of proof that a fridge-freezer caused a fire in his home. Such difficulties have led some Member States and consumer groups to call for the Product Liability Directive to be amended either to reverse the burden of proof or to adopt a presumption of producer liability. [163] However, producers and insurers inevitably contest such proposals.

The concept of damage under the Product Liability Directive is limited to death, personal injury and damage to any other item of property. [164] In *Boston Scientific*, however, the Court took an expansive view of what damage should be compensated, including "all that is necessary to eliminate harmful consequences and to restore the level of safety which a person is entitled to expect". [165] Where the damaged property is for private use or consumption, a maximum recoverable threshold of €500 is imposed, which would apply to the Nest products. [166] For recovery of non-material damages, such as distress, this is left for the Member State's law to determine. Finally, it is not permissible for a producer to limit or exclude his liability under the Directive. [167]

It must also be noted that product liability regimes are closely linked with the related field of product safety law. While the former addresses liability for defects in a product that is already on the market, the latter imposes controls on the quality of products that can be "placed on the market". [168] With respect to IoT devices, there is a range of potentially applicable product safety laws at an EU level, both general and sectoral, such as the type approval regime applicable to all 'radio equipment' [169] and 'medical devices'. [170] These provide for *ex ante* compliance procedures coupled with an *ex post* oversight mechanism. The *ex ante* compliance procedures may be carried out by external 'notified bodies' or through self-certification mechanism. [171] Once a product completes the 'conformity assessment procedure' (also known as 'type approval'), it can be placed on the European market. Once on the market, if a defect is subsequently identified, the associated exposure under the Product Liability Directive (especially given the broadening of liability risk to potential defects under *Boston Scientific*) should create a positive feedback loop into the producer's product safety management systems. [172] In the context of IoT, for example, one could imagine the need to have software update procedures in place, to enable 'defects' to be addressed rapidly and en masse. [173]

It is easy to infer the potential unenforceability of some of the Nest clauses outlined above under product liability rules. For example, in the Limited Warranty, Nest states that products supplied 'AS IS' are 'ineligible products', without any further elaboration as to why they should fall outside the warranty. The phrase 'AS IS' is another example of US wording being transplanted into a European marketplace; despite it being known that such phrases would be unenforceable in many European states. However, Nest also acknowledges that its provisions may not apply "to the extent prohibited by applicable law", [174] which would obviously include product liability rules.

6. UNFAIR TERMS

Controlling the imposition of unfair contractual obligations by a producer or supplier upon a customer is a central strand of all mature consumer protection regimes. While product liability laws focus on defective products already on the market and the 'producer' who made them, unfair contract terms laws focus on the balance of rights and obligations established between the seller or supplier of the product and the consumer. The rules proceed on the presumption that the consumer is in a weak position "both in his bargaining power and his level of knowledge", [175] and provide a public law framework to remedy private law failings. Unfair contract terms laws must also be distinguished from rules protecting consumers at other points in the transaction process, such as marketing practices. [176]

Within Europe, such matters are primarily governed by national laws implementing Directive 93/13/EEC 'on unfair terms in consumer contracts'.[177] The Directive is only applicable where the term has not been individually negotiated, while a term is considered 'unfair' if:

> "contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer" [178]

The Directive elaborates two different types of unfairness. First, it provides an 'indicative and non-exhaustive' list of terms that may be regarded as unfair. [179] These can be referred to as 'issues of substance', since the focus is on the rights and obligations detailed in the agreement itself. Second, the Directive provides that 'unfairness' can also be assessed on the basis of "all the circumstances attending the conclusion of the contract", which includes any other contract on which the main contract is dependent, as well as the language in which the terms are drafted, which should be "in plain intelligible language". [180] These can be referred to as 'issues of form', as it is the manner in which the contract is presented to the customer that is being considered. Our assessment of the Nest terms must therefore consider both issues of substance and form.

To date, European case law under the Unfair Terms Directive has generally focused on issues of substance rather than form. However, in *Kásler* ,[181] the Court held that the requirement of transparency, in terms of 'plain, intelligible language', "cannot...be reduced merely to their being formally and grammatically intelligible", [182] but rather must be understood in 'a broad sense', on the basis of an "average consumer, who is reasonably well informed and reasonably observant and circumspect" [183] and who should be able to "assess the potentially significant economic consequences for him". [184]

In *RWE Vertrieb*, [185] the Court noted that it was not sufficient to include a "mere reference, in the general terms and conditions, to a legislative or regulatory act determining the rights and obligations of the parties. It is essential that that the consumer is informed…of the content of the provisions concerned." [186] The Court went on to note that the level of information required will vary depending on the circumstances, with both*RWE Vertrieb* and *Invitel* being concerned with the levying of charges. However, on the face of it, such an obligation could have very significant implications for contractual drafting in Europe. [187]

In the Nest T&Cs, for example, it is noted that the consumer has 'certain legal rights' and that any exclusions, disclaimers or limitation of liability provisions will apply to the extent permitted by law. However, as regards what such rights may be, the terms simply suggest "you should refer to the laws applicable in your country or jurisdiction". [188] In the UK, the Competition and Markets Authority ('CMA'), the relevant enforcement authority, has stated that wide exclusion clauses "qualified merely by a statement that the trader's liability is excluded only to the extent permitted by statute" are manifestly both unfair and lacking transparency. [189] While Nest's phrasing would appear to be common industry practice, [190]one could imagine that for certain IoT applications, especially the more intimate they are to the user's well-being, a higher standard of transparency could be imposed on providers under unfair contract terms rules.

In the UK, the applicable legislation extends to non-contractual 'notices' as well as contracts, [191] which would include the use of disclaimers stuck on, or packaged with, IoT products, attempting to add another layer of protection for the producer or supplier. With regard to the Nest legals, two key examples are the EULA for the product software and the 'Open-source Compliance' notice. In both cases, although Nest attempts to make them contractual in nature, [192] such characterisation is debateable and could be subsequently rejected by a court, giving rise to legal uncertainty. Both also attempt to limit liability. In the latter case, as well as listing all the open source modules contained in the Learning Thermostat, providing access to the related source code and indicating the applicability of GPLv3; it also disclaims all warranties and shifts the 'entire risk and the entire liability' to any consumer who uses those software modules to modify the device. The rules on unfairness do not apply, however, where the notice is mandatory, which would be applicable to the EU Declarations of Conformity supplied by Nest and associated CE marking. [193]

The CMA has emphasised that although unfair contract terms rules have a distinct requirement of transparency, [194] which it terms a 'transparency test', this in fact is simply an integral component of any assessment of fairness. [195] The UK requirement adds 'legibility' to the need for plain and intelligible language provided for in the Directive. However, while a finding that a term, an agreement or a set of agreements lack transparency may not in itself be sufficient to render a contract 'unfair', any uncertainty about meaning arising from the lack should be interpreted in a manner most favourable to the consumer. [196] The need for transparency within a contract varies according to the nature of the provision. As noted above, the Nest legals make extensive use of text in capitals in order to give 'appropriate prominence' [197] to terms that may be considered disadvantageous to the consumer.

From our earlier analysis, the Nest legals do not obviously contain any provisions that expressly fall foul of the 'blacklist' or 'greylist' of terms detailed in the Directive's Annex. However, with respect to issues of form, it would seem at least arguable that, taken as a whole, the Nest legals could be seen as lacking sufficient transparency, by not enabling an 'average consumer' to understand the complex dependencies and interaction between the product, service and software agreements that, as a minimum, underpin the Nest products. While each agreement in itself might be considered as clearly drafted, European law expressly recognises the critical impact that "another contract on which it is dependent" may have and the need for the relationship between terms among these dependent contracts, as much as within the individual agreements themselves, to be clearly set out.

7. CONCLUSIONS

This paper has focused on the Nest legals as a case study; a qualitative rather than quantitative approach, designed to identify issues of concern that may, or may not, [198] be rife within the emerging IoT marketplace. After giving an account of some general contract law issues relevant to IoT, we have illustrated the complexity of our chosen IoT supply chain and its associated legals. Many issues we discuss are not specific to the IoT context, especially the lack of bargaining power for consumers and issues of applicable law and jurisdiction. Other issues may be more important in other IT contracts, such as cloud computing, but do not have particular resonance in the provision of the IoT.

Our main conclusion is that the emerging world of IoT already demonstrates a need to consider recasting the concept of product to reflect the increasingly inextricable mixture of hardware, software, data and services. The Nest legals attempt to treat each element separately in a manner that seems either, at best, unworkable or, at worse, nonsensical. In particular, the treatment of 'disconnected' IoT devices may require public law intervention, especially where it is considered to provide 'essential' functionality. [199] When you add the web of third parties into IoT mix, the contractual complexity inevitably multiplies. While third parties that comprise part of the supply chain for an IoT device should not present unique challenges, the web of IoT devices that 'work with' (*read* interoperate with) the purchased device does generate concerns, particularly with respect to the handling of personal data and information security in general.

Product liability and unfair contract term regimes are just two strands of a broader set of consumer protection rules designed to address the asymmetry of bargaining power in modern commerce. [200] Whether the integration of IoT devices into our lives will lead to a significant rise in claims being made under such laws, either for 'harmful consequences' or for being unfair, will obviously depend on a range of factors, including national conditions in relation to access to justice, such as the availability of class actions. However, uncertainties in the applicability of current rules lend support to the idea of a consumer protection regime designed, or redesigned, to address the realities of the IoT.

---

* The authors are grateful to the members of the Microsoft Cloud Computing Research Centre (MCCRC) and others for their valuable comments and to Microsoft for generous financial support. The views, however, are solely the authors'.

[1] MCCRC definition. See also Singh, J. et al., "Twenty Security Considerations for Cloud-Supported Internet of Things." *IEEE Internet of Things Journal*", PP(99), pp.1-15, 2015.

[2] See respectively, ITU-T Recommendation Y.2060, *Overview of the Internet of Things* (06/2012), at 3.2.3, which includes virtual things, and ISO/IEC JTC 1, *Internet of*

Things (IoT). Preliminary Report 2014, 2015, at 4.1, which infers that persons are included within the definition.

[3] See Bradshaw, Millard and Walden "Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services"*International Journal of Law and Information Technology* (2011) 19 (3).

[4] https://investor.google.com/releases/2014/0113.html (All URLs cited in this paper were accessed on 8.12.2015). Google has since become a subsidiary of Alphabet Inc.

[5] See https://nest.com/uk/camera/meet-nest-cam/

[6] E.g. Mercedes, Kevo, hue, ooma and Whirlpool. See https://nest.com/uk/works-with-nest/.

[7] Also referred to as 'Nest' or 'the company'.

[8] As regards the main clauses analysed, we have found many analogies with IoT contracts of businesses different from Nest, which could confirm the validity of the chosen use case.

[9] Some of the non-contractual documentation, e.g. the IP licences and the privacy policy, is incorporated into the contract.

[10] For a range of possible meanings of 'private ordering' see Castle, D., (ed.), *The Role of Intellectual Property Rights in Biotechnology Innovation*, Edward Elgar, Cheltenham, 2009, 312, especially notes 42-44.

[11] This phenomenon is described as 'legal hysteresis' by Noto La Diega, G., *In light of the ends. Copyright hysteresis and private copy exception*, in Quaderni di Diritto Mercato Tecnologia, 2015(II).

[12] See Bradshaw, n. 3.

[13] Hon, Millard and Singh, "Twenty legal considerations for the Clouds of Things", MCCRC discussion document (available athttp://ssrn.com/abstract=2716966), defines 'Clouds of Things' as the "ecosystems in which there are communications between things and clouds, including M2M communications mediated by cloud."

[14] Kurzweil, R., *The Age of Intelligent Machines*, MIT Press, Cambridge, 1990.

[15] Weiser, M., *The Computer for the 21st Century*, American Ubicomp Paper after Sci Am Editing, 1991,https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf

[16] An example of a nearly autonomous thing that bought things is Random Darknet Shopper, a bot that, for art's sake, purchased randomly counterfeit clothing (namely a pair of "Diesel" jeans and a "Louis Vuitton" handbag), a baseball cap with a hidden camera, a stash can, a pair of Nike trainers, a decoy letter, two hundred Chesterfield cigarettes, a set of fire-

brigade issued master keys, and ten ecstasy tablets (http://www.theguardian.com/technology/2014/dec/05/software-bot-darknet-shopping-spree-random-shopper).

[17] See Mik, E., "The unimportance of being 'electronic' or popular misconceptions about 'internet contracting'", 19 *Int'l J.L. & Info. Tech.* 324

[18] See the General Data Protection Regulation (2016/679; OJ L 119/1, 4.5. 2016), at Art. 25.

[19] See Clarck, D.D., et al., *Tussle in Cyberspace: Defining Tomorrow's Internet*, IEEE/ACM Transactions on Networking, June 2005, 13, III, 473, where they observe that "the laws of men and the so-called whims of bureaucrats are part of the fabric of society, like it or not. They are some of the building blocks of tussle, and must be accepted as such. We, as technical designers, should not try to deny the reality of the tussle, but instead recognize our power to shape it".

[20] See Mills, M., "Artificial intelligence in law - the state of play in 2015?", Legal IT Insider, 3 November 2015, available athttp://www.legaltechnology.com/latest-news/artificial-intelligence-in-law-the-state-of-play-in-2015/ .

[21] Hon-Millard-Singh, n. 10, at p. 13.

[22] We do not only have in mind the Coke machine at Carnegie Mellon that reportedly was the first IoT device. See M.U. Farooq et al., *A Review on Internet of Things (IoT)*, in *International Journal of Computer Applications*, 2015, I, 113, 1.

[23] For more information see the video https://vimeo.com/41363473 or visit the website of Brad's designer Simone Rebaudengohttp://www.simonerebaudengo.com/#/addictedproducts/.

[24] Although we use the adjectives 'smart' and 'intelligent' in respect of IoT applications, reflecting common usage, we consider it confers undesirable anthropomorphic connotations; while in the not too distant future, if everything is smart, then nothing will be.

[25] See Benöhr, I., *EU Consumer Law and Human* Rights, OUP, 2014, and Reich, Micklitz, Rott and Tonner, *European Consumer Law*, 2 nd ed., Intersentia, 2014.

[26] A similar effect can also be seen in the US, e.g., the doctrine of unconscionability. See Murray, J.E., *Unconscionability*, 31 U. Pitt. L. Rev. 1 (1969-1970) and Stedronsky, H.J., *Unconscionability and Standardized Contracts*, N.Y.U. Rev. L. & Soc. Change 65 (1975).

[27] Peppet, S.R., *Freedom of Contract in an Augmented Reality: The Case of Consumer Contracts*, U of Colorado Law Legal Studies Research Paper No. 11-14. Available at SSRN: http://ssrn.com/abstract=1919013.

[28] ToS (17.6.2015 version), at 5(b).

[29] See https://nest.com/uk/security/

While the Nest security policy references the Nest privacy statement, the latter simply pledges to use 'best-in-class security tools', without further elaboration.

[30] E.g. http://www.rackspace.co.uk/legal.

[31] See Article 29 Working Party Opinion 1/2010 'on the concepts of controller and processor' (WP 169), at III.2, regarding the 'plurality of processors' (see also Opinion 5/2012 'on cloud computing', WP196). The draft 'Data Protection Code of Conduct for Cloud Service Providers', prepared by the Cloud Industry Select Group established by the European Commission (see further https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-code-conduct), requires service providers to "maintain an up-to-date list of any subcontractors engaged in the processing personal data under the Services agreement." (at 5.4). However, note Article 29 Working Party Opinion 2/2015 'on C-SIG Code of Conduct on Cloud Computing' (WP232), adopted on 22 September 2015.

[32] It is perhaps noteworthy that following the latest update to the Nest legals, most references to 'cloud' have been deleted. The security policy and website privacy policy still mention cloud, but the Privacy Statement, the ToS, the T&C, and the EULA are silent on the matter. The role of third party cloud providers is confirmed in information about Nest Aware, only available in the Nest blog (https://nest.com/support/article/WhatdoIgetwithNestAwareforNestCam), which notes that advanced algorithms aimed at sending more accurate motion and audio alerts and motion sensing features (i.e. face detection and depth sensing) require a lot of computing power, "much more than Nest Cam can deliver by itself. So we have to use powerful cloud servers to deliver this state of the art detection."

[33] The Developers Terms of Service are available at https://developer.nest.com/documentation/cloud/tos (last update 14.1. 2015).

[34] Ibid., at IX Liability.

[35] Carré and Strauss, *Roadmap for the Emerging "Internet of Things"*, edited by Fell, M. 2014 (available athttp://sweden.nlembassy.org/binaries/content/assets/postenweb/z/zweden/netherlands-embassy-in-stockholm/iot_roadmap_final_draft_0309145.pdf).

[36] The situation might change in a personal cloud context, where people can have more control over their data.

[37] ToS Preamble.

[38] I.e. T&Cs, at 5: "...Title for Products purchased from the Store passes to the purchaser at the time of delivery by Nest to the freight carrier…"

[39] E.g. UK, Sale of Goods Act 1979, s. 12(2)(b).

[40] See *Rubicon Computer Systems Ltd. v United Paints Ltd* (2000) 2 T.C.L.R. 453.

[41] http://revolv.com/ . See also BBC Technology, 'The problem with forced tech obsolescence', 7 April 2016.

[42] Ofcom statement, *Review of Sky's Access Control Services Regulation*, 17.3.2015.

[43] For instance, in the HVAC or Electricity sector.

[44] As far as we know, the only Nest UK Wholesale Distribution Partner is WF Senate, following an agreement between the latter's parent company Rexel and Nest Labs (http://www.voltimum.co.uk/articles/wf-senate-distribute-google-owned-nest-self-learning-domestic-energy-saving-and-safety ; for the WF Senate contractual quagmire seehttp://www.wfsenate.co.uk/d/22/Terms_%26_Conditions%2C_Privacy_Policy_%26_Legal.html). In the US there is for instance eDist, a New Jersey company (see http://security.edist.com/index.jsp?path=nest-distributor).

[45] The Terms & Conditions of Sale ('T&Cs') are available at https://nest.com/uk/legal/sales-terms/. See also the Installation Terms of Service available at https://nest.com/uk/legal/installation/.

[46] Cybersource, a California e-commerce credit card payment system management subsidiary of Visa, "will collect and store full payment card information from you, even as a guest user, when an order is placed until when it ships. If you create a Nest account and elect to have payment card information saved, CyberSource will store your payment information." (Privacy Policy for Nest Web Sites). There is always the possibility to use e-commerce platforms, for instance one may buy the product via eBay and therefore it may be necessary to take into account also PayPal's privacy policy and other relevant legals.

[47] The qualifier "such as" suggests other unnamed partners and third parties offering advertising services.

[48] Nest will let the insurer know that Nest Protect is installed and working. In exchange, the insurer will take up to 5% off the insurance premiums. Nest promises that "Your insurer will never know if the alarm went off because you burned the popcorn." the insurer should know if the batteries are charged, the sensors are working and the Wi-Fi connection is good. Elsewhere (https://nest.com/support/article/When-I-enroll-in-Safety-Rewards-what-kind-of-data-is-shared-with-my-insurance-company), one discovers that Nest will provide monthly basic summarized information about your Nest Protect to your insurance company and that the summary 'includes' the three pieces of information (battery, sensor and connection), which does not mean that other information is excluded, such as your postal code and the names of the rooms where you have your Nest Protects installed. While Nest promises not to share "any smoke or carbon monoxide alarms that may have occurred in your home", if the batteries rapidly run low, it is not hard to infer that an alarm occurred. One can decide not to grant permission to share the data requested in connection with the Safety Rewards service, but, again, "you won't be able to participate in Safety Rewards." The service appears in the US website, but the UK version of the Website Privacy Policy mentions insurance companies among the partners.

[49] The information is available at https://nest.com/insurance-partners/. Along with what has been stated in the note above, it is not clear, for instance, what would happen if my house catches fire and Nest sends the insurance company information that I had been alerted when it had not alerted me (Nest does not guarantee the accuracy of the shared information).

[50] See https://nest.com/energy-partners/. The services offered are Rush Hour Rewards and Seasonal Savings; the technology involved is Auto-Tune. Among the main legal issues relevant to machine learning and artificial intelligence are liability (e.g. is the owner of a Thing liable for its autonomous actions?) and contracts (can a contract be concluded autonomously by a Thing?).

[51] The "Customer Agreements for Rush Hour" is available at https://nest.com/legal/customer-agreements-for-rush-hour-rewards/.

[52] See https://nest.com/legal/customer-agreements-for-rebates/. Currently this service is provided only by Xcel Energy. 'Rebates' is not regulated by Nest legals, but by "Xcel Energy's Rebate Terms & Conditions", even though "Nest is providing this Rebate Redemption Tool in accordance with, and your use of the Rebate Redemption Tool is subject to, the Nest Terms of Service, privacy policies and other policies on Nest's website." In any event, unlike the insurance case, here Nest states that it will 'share the information provided by you in your application (including, but not limited to, your name, email address, service address, Xcel Energy account number, Nest Learning Thermostat serial number, date application completed.' Furthermore, on Xcel Energy's website, the general ToS are readily available. (http://www.xcelenergy.com/staticfiles/xe/Admin/CLI_1793261_10_FINAL_CLEAN_Xcel%20Energy_OAM_My%20Account_Terms%20and%20Conditions.pdf), but not the "Xcel Energy's Rebate Terms & Conditions".

[53] Privacy Statement: "With your consent, MyEnergy may access different types of information from your utility. For example, MyEnergy may download, analyze, and store your utility bill statements."

[54] https://nest.com/support/article/What-is-Auto-Tune .

[55] The Nest app is available on the Apple's iTunes and Google Play, as well as the web. See https://nest.com/blog/2015/06/17/one-home-one-app/

[56] Nest products can be bought from e-commerce platforms, such as eBay, Amazon and Alibaba. Under the T&Cs, it notes that that the 'Store' is accessible worldwide, but states that if you use Nest products and services "outside the United Kingdom, Ireland, France, Belgium or the Netherlands (each, a "Target Country"), you do so on your own initiative and you are solely responsible for complying with the applicable local laws in your country. You understand and accept that the Store and our Products and Subscription Services are not designed for use in a non-Target Country and some or all of the features of the Store, Products and Subscription Services may not work or be appropriate for use in such a country. To the extent permissible by law, Nest accepts no responsibility or liability for any

damage or loss caused by your access or use of the Store, Products and Subscription Services in a non-Target Country." One can question if Nest can limit its liability to products sold in 'Target' countries when they acknowledge that their products are purchased worldwide: See https://nest.com/blog/2014/09/06/nest-is-coming-to-the-EU/, where the company admits that their products are installed in over 120 countries.

[57] There is apparently no separate contract for businesses, but the T&Cs state that "The Store is for retail sales to private consumers only. Please contact euorders@nestlabs.com if you wish to purchase wholesale supplies". Presumably separate terms are used for such purchases, but they are not publicly available.

[58] Since Google acquired Nest, it seems likely that Google's legals will eventually come to influence the Nest legals.

[59] It is not entirely clear what these subscription services are, which is surprising given that their inclusion is one of the stated reasons for the last update of Nest legals. The ToS say nothing more than that the subscription services include "services that can be accessed using the Web Apps and Mobile Apps." In addition, the Privacy Statement refers to the ToS for the definition (which is not provided), while the ToS refers to the Terms of Sale (either the Nest's T&Cs or the service provider's terms) for the regulation of the fees ("Certain Services may be provided for a fee. You shall pay all applicable fees in connection with the Services selected by you in accordance with the Terms of Sale.").

[60] The EULA is available at https://nest.com/uk/legal/eula/.

[61] One can find the Privacy Statement for Nest Products and Services at https://nest.com/uk/legal/privacy-statement-for-nest-products-and-services/ . Previous policies are available at https://nest.com/uk/legal/privacy-statement/archive / whilst the old Dropcam Privacy Policy is athttps://www.dropcam.com/privacy/dropcam. If the Privacy Statement is accessed from the Nest app, the US version appears.

[62] The scope of these privacy policies is unclear. While the Privacy Statement covers information collected through Nest products, which include web apps, mobile apps, and subscription services; the WPP provides that Nest uses permanent cookies in order to understand "how you use our website *and products and services*, to diagnose and fix technology problems, and otherwise enhance our Site, products, and services."

[63] Vulnerabilities that users discover should be reported to 'Google's Vulnerability Reward Program or security@nest.com'.

[64] Some 30 open source code modules for the thermostat are listed with associated compliance notices; available athttps://nest.com/uk/legal/compliance/. These notices are generally required of those that wish to use open source modules, under the module licences.

[65] At https://nest.com/uk/legal/ip-and-other-notices/, with regard to patents, trademarks, the Trademark Usage Policy and the Policy Regarding Unsolicited Idea Submissions.

[66] The Community Forum Agreement is available at https://nest.com/uk/legal/community-forum-agreement/.

[67] The Transparency Report was introduced with the update of 17.6.2015 and deals with requests received for law enforcement purposes (https://nest.com/uk/legal/transparency-report/. It states that if a US government agency presents Nest with a warrant to investigate a crime they think was captured by Nest products, the company would not just hand over user data. Nest would analyse the request to be sure that the warrant was not overly broad and then they would make sure the information the agency requested was within the scope of the warrant.

[68] At https://nest.com/uk/legal/eu-declarations/ there are various declarations of conformity for the Nest Thermostat. This means that the product is stated to be in conformity with the Low Voltage Directive (2006/95/EC), Electromagnetic Compatibility Directive (2004/108/EC), Telecommunications Terminal Equipment Directive (1999/5/EC), the Ecodesign Requirements for Energy Related Products Directive (2009/125/EC) and the Hazardous Substances in Electrical and Electronic Equipment Directive (2011/65/EU). As a consequence the product carries the CE mark.

[69] E.g. the Installation ToS states: "These terms and conditions are in addition to any terms and conditions of the Installer."

[70] Interoperability is a major issue in the IoT. Reportedly, Nest products are not compatible with Apple HomeKit and cannot be controlled via Apple's voice controller Siri, although a Nest application is available for the Apple Watch.

[71] An end user may not expect that they have to take into consideration not only Nest's third parties, but also the third parties' third parties. See the Developer ToS: "You [the developer] will not permit use of any Customer Data or disclose any Customer Data to any third party except to those third parties who provide services on your behalf in connection with your Client and who are obligated to maintain Customer Data only for your own benefit and under reasonable confidentiality terms". One may question why this provision is limited to the developer, whereas Nest's parent provides that "We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are subject to *strict contractual confidentiality obligations* and may be disciplined or terminated if they fail to meet these obligations." (Italics added).

[72] At https://nest.com/works-with-nest/ one can find more information on "Works with Nest".

[73] On 17.11.2015, Nest has announced its third generation thermostat (see more at http://www.wired.co.uk/news/archive/2015-11/17/nest-third-generation-boiler).

[74] To find out more about the data shared within the context of "Works with Nest" see https://nest.com/support/article/What-kinds-of-data-is-shared-with-Works-with-Nest-developers . Please note that even though you set "United Kingdom" as the relevant country, the website redirects you to the United States version. Along with the Works with Nest legals, the customer has to double-check also those of the connected devices, apps and appliances (see, for example, Daimler privacy policy at http://drive-kit-plus.com/en/privacy/).

[75] Under these ToS, Nest provides (1) a Nest user account website that may be accessed at home.nest.com or www.dropcam.com (each a "Site"), (2) services accessible through the Sites ("Web Apps"), (3) software that may be downloaded to your smartphone or tablet to access services ("Mobile Apps"), and (4) a MyEnergy user account website that may be accessed at www.myenergy.com ("MyEnergy Service"), all for use in conjunction with Nest hardware products ("Products") and in other ways that Nest provides.

[76] The same clause can be found verbatim in the Legal Terms of Azert LLC Smart(er) Socket http://www.smartersocket.com/legal-terms/. This US smart socket supports in-door navigation, proximity based messaging, power consumption monitors and presence sensors.

[77] The previous wording was "These Terms constitute the entire agreement between you and Nest regarding the use of the Services" (and the same section can still be found, for instance, in the Wellntel Terms of Service Agreement). After the last update, the situation got even more complex, given that hardware products and subscription services are regulated "by these Terms & Conditions of Sale ("Terms & Conditions") and any additional terms we provide, including but not limited to our Terms of Service and the terms of the Limited Warranty included in-box with a Product." Hence, a single aspect of a product is covered by an unpredictable number of legals (see the subscription services, regulated at least by the Privacy Statement, the ToS and the T&C).

[78] The services covered by the ToS are the websites, web apps, mobile apps, subscription services and MyEnergy Service, whereas the services under the T&C seem to refer to the subscription service only, thus creating a partial, albeit confusing, overlap. MyEnergy is the only service enjoying a separate section of the Privacy Statement.

[79] The most recent update to Nest legals has gone in the direction of a further blurring of the lines between hardware, software and services. We should mention the substitution of the term 'service' with the term 'product' in the Privacy Statement.

[80] This clause is quite common in IoT and cloud contracts; e.g. the Leeo, Inc. Smart Alert™ Nightlight ToS (https://www.leeo.com/legal/terms-service/) and Snupi Technologies, Inc. WallyHome ToS (http://www.wallyhome.com/legal/).

[81] See also the EULA of Orion (http://www.orionlabs.co/eula-android/).

[82] This is an improvement of the last update to the T&C and leaves out the changes of prices, for which Nest will provide notification "via (at its option) email to the primary email

associated with your Nest account, hard copy, or posting of such notice on the Nest website." Under the previous regime, continued use of the services indicated acknowledgement of the changes and the burden of checking the site to see if any modification was posted was on the customer. In the unlikely event that a user checked the legals over time, if the changes were not highlighted and previous versions were not stored and made easily accessible, it would be very difficult to understand what had changed.

[83] Singh et al., n. 1, where it is explained that "Work in IoT tends towards the subsystem, often focusing on particular technical concerns or application domains, before offloading data to the cloud. As such, there has been little regard given to the security, privacy and personal safety risks that arise beyond these subsystems; that is, from the wide-scale, cross-platform openness that cloud services bring to IoT."

[84] These scenarios are not entirely new, see for example, Zammit and Savio, *Tort Liability For High Risk Computer Software*, 23 PLI/PAT 373, 375 (1987), for a case in which a bug in a computerized therapeutic radiation machine caused it to administer incorrect dosages and, as a consequence, two people were killed and several others were seriously injured. Let us imagine, however, what can happen if entire hospitals are affected. See also Massingale and Borthick, *Risk Allocation For Injury Due to Defective Medical Software*, 2 J. Prod. Liab. 181 (1988).

[85] This is one of the many names given to the IoT. See Greenfield, A., *Everyware: The Dawning Age of Ubiquitous Computing*, New Riders, Berkeley, 2006.

[86] The current lack of interoperability, the heterogeneity of standards and protocols and the prevalence of proprietary models render communications between the 'silos' difficult. See Desai, Sheth and Anantharam, *Semantic Gateway as a Service Architecture for IoT Interoperability*, 2015 IEEE International Conference on Mobile Services (MS), 27.6-2.7.2015, 313.

[87] This leads to the issues of recombination, repurposing and reconfiguration, which merit further research. As to Nest legals, see for instance the section of the Privacy Statement whereby "MyEnergy data can be combined with other information in your Nest account and can help us to better understand things like your energy usage." or, as regards the exchanges of data and requests for control by third parties, "Nest requires your explicit consent before sharing information in these circumstances. We may also obtain information from other sources and combine that with the information in your Nest account."

[88] On the use of high-frequency sounds to covertly track across a range of devices see Calabrese et al., *Comments for November 2015 Workshop on Cross-Device Tracking*, Letter of the Center for Democracy & Technology to the Federal Trade Commission, 16.10.2015, available athttps://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf .

[89] BBC, 'Nest thermostat bug leaves users cold', 14 January 2016, available at http://www.bbc.co.uk/news/technology-35311447

[90] https://nest.com/support/article/Nest-Protect-Safety .

[91] https://nest.com/uk/support/article/Learn-more-about-Sound-Check and https://nest.com/uk/support/article/Learn-more-about-Nest-Protect-s-microphone . The former statement may be designed to address public concern over the Samsung Smart TV 'listening in' on family conversations:
see http://www.bbc.co.uk/news/technology-31296188

[92] The Privacy Statement specifies that the moment which determines the application either of Nest policy or of the third party's one is the time when the data are in the third party's "possession". Possession of data is not always easy to assess, especially in the IoT. Furthermore, data could be replicated, and be in the possession of both the third party and Nest at the same time. If there is a problem with Nest's service affecting data stored with it, can Nest escape all liability just because the same data has previously been sent to a third party?

[93] Nest provides the example of rewards programmes provided by its partners, but if one reads carefully, they discover that "We may also obtain information from *other sources* and combine that with the information in your Nest account."

[94] Hon, Millard and Singh, n. 10.

[95] This provision has to be read jointly with the section of the Privacy Statement whereby "Data protection and privacy laws in your country may impose certain responsibilities on you and your use of Nest Cam. You (not Nest) are responsible for ensuring that you comply with any applicable laws when you use Nest Cam. For example, you may need to display a notice that alerts visitors to your home that you are using Nest Cam. Note in particular that recording and sharing clips that involve other people may affect their privacy and data protection rights." See Case C-212/13,*František Ryneš v Úrad pro ochranu osobních údaju,* [2015] 1 W.L.R. 2607.

[96] Under the previous version of the Privacy Statement, all information was professedly encrypted.

[97] The relevant documents are available at http://www.export.gov/safeharbor/. However, see also C-362/14 *Maximillian Schrems v Data Protection Commissioner*, [2016] 2 C.M.L.R. 2, which declared the Commission decision on Safe Harbor (Decision 2000/520) invalid.

[98] These measures include HTTPS, TLS/SSL protocol, AES and RSA data encryption.

[99] The exact wording of this clause can be found in a vast variety of contracts (Googling the cited passage, generates 140,000 results).

[100] See Millard, C., *Forced Localization of Cloud Services: Is Privacy the Real Driver?,* IEEE Cloud Computing, vol.2, no. 2, pp. 10-14, Mar.-Apr. 2015, doi:10.1109/MCC.2015.37 and Hon, Millard, Reed, Singh, Walden and Crowcroft,*Policy, Legal and Regulatory Implications of an Europe-Only Cloud*, Queen Mary School of Law Legal Research Paper 191/2015, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2527951. For the technical

considerations underpinning regional clouds see Singh, Bacon and Crowcroft, Madhavapeddy, Pasquier, Hon and Millard,*Regional clouds: technical considerations*, November 2014, also available at http://www.mccrc.eu/Pages/Events.aspx.

[101] The former reflects Article 26(1)(a) of Directive 95/46/EC, while the latter falls under article 25(6).

[102] Goodman, M., *Hacked dog, a car that snoops on you and a fridge full of adverts: the perils of the internet of things*, 11.3.2015,http://www.theguardian.com/technology/2015/mar/11/internet-of-things-hacked-online-perils-future .

[103] https://nest.com/uk/security/ , see: "What information is stored on Nest devices? Your Nest devices collect setup information like your ZIP or postal code, your Wi-Fi network information, environmental data from sensors like temperature and humidity, temperature adjustments, usage and occupancy information, and more". For a "full list" it refers to https://nest.com/uk/legal/privacy-statement-for-nest-products-and-services/#what-does-nest-collect

[104] See further n. 27. It has recently been reported that the Nest Cam remains 'always on', even when the user has turned it off. See ABI Research,Teardown Phone/Device: Nest Cam Works Around the Clock, 16.11.2015, at https://www.abiresearch.com/press/nest-cam-works-around-clock/. Nest says there is no truth in these allegations. "When Nest Cam is turned off from the user interface, it does not fully power down, as we expect the camera to be turned on again at any point in time," a Nest spokesperson told *El Reg*. "With that said, when Nest Cam is turned off, it completely stops transmitting video to the cloud, meaning it no longer observes its surroundings." (http://www.theregister.co.uk/2015/11/25/nest_cam_doesnt_spy/) .

[105] The same provision of Privacy Policy for Nest Web Sites (including the reference to the employees) can be found in the Sugr Privacy Statement (http://www.sugrsugr.com/index.php/privacy-statement/).

[106] "We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations." (Google Privacy Policy, as amended on 19.8.2015, http://www.google.com/policies/privacy/). It should be noted that Alphabet's privacy policy (and overall legals) are not available yet.

[107] The Nest legals provide plenty of examples of such 'fictitious' consent. We have already seen and will see further cases where the only alternative to consent is not to enjoy the product.

[108] Directive 95/46/EC, at art. 7(b).

[109] ICO, *Response to Ofcom's consultation 'Promoting investment and innovation in the Internet of Things'*, October 2014,https://ico.org.uk/media/about-the-ico/consultation-responses/2014/2512/ico-response-to-ofcom-consultation-on-internet-of-things-20141001.pdf .

[110] The same provision can be found in the Bluvision Developer ToS. Fibar group is a Polish manufacturer of wireless home automation systems; its "Climate" plug-ins work with Nest.

[111] See, for example, LinkedIn Privacy Policy at https://www.linkedin.com/legal/privacy-policy (last revised on 23.10.2014).

[112] An example is provided by Google Privacy Policy. Google explains that it "regularly receives requests from governments and courts around the world to hand over user data", but it ensures that "frequently push back when the requests appear to be overly broad or don't follow the correct process" (http://www.google.com/policies/privacy/example/legal-process.html).

[113] See JottaCloud Privacy Guarantee (https://www.jottacloud.com/its-your-stuff-guaranteed/, last updated on 16.6.2013).

[114] The US 'feel' of the Nest legals has become stronger since the last update of the legals. For instance, the UK version of the Privacy Statement has been changed to substitute 'unauthorised', 'programme', 'postcode', 'neighbourhood', 'personalise' with 'unauthorized', 'program', 'postal or ZIP code', 'neighborhood', 'personalize'.

[115] Such orders may also come from European LEAs and be imposed on US companies.

[116] Bodle, I., *EU Data Protection Law and the Patriot Act in the Cloud*, 21.3.2012, http://www.webanalyticsworld.net/2012/03/eu-data-protection-law-and-the-patriot-act-in-the-cloud.html , especially when it is reported that "Well known global software and search engine companies have admitted that EU customer data has been disclosed by them as a consequence of requests under the Patriot Act".

[117] For the interesting concept of "Social Internet of Things" (SIoT) see Atzori, Iera and Morabito, *Making Things Socialize in the Internet - Does it Help Our Lives?* , Proceedings of ITU Kaleidoscope 2011: The Fully Networked Human? - Innovations for Future Networks and Services (K-2011), 12-14.12.2011, http://www.social-iot.org/d/kaleidoscope.pdf.

[118] The customer might be led to think that switching off their Wi-Fi router is sufficient to stop the communication between their devices. Therefore this information had better be provided in the legals, not in Nest blog (https://nest.com/uk/support/article/HowdoesNestProtectconnectwirelessly).

[119] It should be noted that policy routing, cryptographic techniques, information flow control (IFC) constitute a cost, hence policy makers (and contracts drafters) have to strike the balance between privacy (by design) and competition.

[120] E.g. https://www.mozilla.org/en-GB/firefox/dnt/.

[121] See Clifford, C., 'Google: In a few years, ads will show up on refrigerators, thermostats and glasses', 21 May 2014 (emphasis added),http://www.entrepreneur.com/article/234122.

[122] In the original wording, Nest suggests that the customer might avoid third-party tracking, but in the most recent update, it notes that one can only avoid use of this information for advertising "if these third party ad parties honor the Do Not Track browser signal".

[123] Directive 95/46/EC, art. 7(b).

[124] The customer who reads the Privacy Statement and not the ToS may be led not to understand this point. In fact, under the former "Bluetooth-enabled Nest Products (such as Nest Protect 2nd generation and Nest Cam) may broadcast an identifying signal wirelessly. This is used to connect with your Bluetooth-enabled devices."

[125] E.g. under intellectual property or consumer protection laws.

[126] "This warranty does not cover consumable parts, including batteries, unless damage is due to defects in materials or workmanship of the Product, or software" (sec. 4 of the Limited Warranty).

[127] We do not know, for instance, if the servers used by Rackspace for redundancy are those in London or the ones in Chicago, Dallas, Northern Virginia, Hong Kong, or Sidney. Likewise, it is not clear which data centre is used by AWS (AWS edge locations: Ashburn, VA (3), Atlanta, GA, Dallas/Fort Worth, TX (2), Hayward, CA, Jacksonville, FL, Los Angeles, CA (2), Miami, FL, New York, NY (3), Newark, NJ, Palo Alto, CA, San Jose, CA, Seattle, WA, South Bend, IN, St. Louis, MO).

[128] This is a significant development in the most recent update of the Nest legals. At the time of writing, we are still waiting for the appeal process to be completed in a case in which Microsoft has challenged a warrant issued by a New York magistrate requiring production of emails held on a server in Ireland.

[129] In particular, the user has to allege that the content is not infringing, or that they have the authorisation from the copyright owner, the copyright owner's agent or pursuant to the law.

[130] For a contrary view of product liability, see Mitchell Polinsky and Shavell, "The uneasy case for product liability", 123 *Harv.L.Rev*, 6, April 2010, 1437.

[131] 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' (OJ L 210/29, 7.8.85)('Product Liability Directive'). It was amended by Directive 1999/34/EC (OJ L 141/20, 4.6.199) to include agricultural and fishery products.

[132] Ibid., at recital 2.

[133] See Commission, Fourth Report on the application of Council Directive 85/374/EEC, COM(2011) 547 final, 8.9.2011 ('4th Report'), at 3, which notes that the number of cases rose in some countries such as Germany and France.

[134] The Commission has considered a similar initiative on 'safer services' ('Consumer Policy Action Plan', COM(1998) 696 final, 1.12.1998, at 4.3), but no such proposal has been published.

[135] Reimann, M., "Product Liability in a Global Context: The Hollow Victory of the European Model", *European Review of Private Law* 2-2003, at 129.

[136] Joined cases C-503/13 and 504/13, *Boston Scientific Medizintechnik GmbH v AOK Sachsen-Anhalt & ors,* [2015] 3 C.M.L.R. 6 ('Boston Scientific').

[137] Van Leeuwen and Verbruggen, "Resuscitating EU Product Liability Law? Contemplating the Effects of Boston Scientific Medizintechnik GmbH v. AOK Sachsen-Anhalt and Betriebskrankenkasse RWE (Joined Cases C-503/13 and C-504/13)" (4.8.2015), available at SSRN:http://ssrn.com/abstract=2639582

[138] Ibid, at para. 28.

[139] Product Liability Directive, at art. 9(a).

[140] With regard to the defibrillators, evidence suggested that the defect could be addressed by deactivating a magnetic switch on the device, rather than removal.

[141] Product Liability Directive, at art. 2.

[142] Consumer Protection Act 1987, s. 1(2).

[143] Answer given by Lord Cockfield on behalf of the Commission (15.11.1988) to the Written Question No 706/88 by Mr Gijs de Vries (LDR-NL) (5.7.1988) (89/C 114/76), available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOC_1989_114_R_0001_01&qid=1429892489522&from=EN .

[144] Reed and Angel, *Computer Law*, 6th ed., 2007, at 113, observed that "it seems likely…that the Act applies only to software which is marketed on some form of tangible medium (for example, a tape or disk) ownership of which is transferred to the purchaser". Others consider most consumer purchases of software as a sale of goods; eg. Adams, J., "Software and digital content", *Journal of Business Law*, 2009, 4, 396-402.

[145] Consumer Protection Act 1987, s. 1(2), the wording appear in relation to the definition of a 'producer'.

[146] Nest Labs (Europe) Ltd., Limited Warranty, at clause 4.

[147] Product Liability Directive, at art. 3(1).

[148] Ibid, at art. 3(2). As noted above, the majority of consumers are likely to buy direct from Nest's website or from an eCommerce platform.

[149] Ibid, at art. 3(3). See C-402/03 *Skov AEG v Bilka Lavprisvarehus A/S* [2006] 2 C.M.L.R. 16, where the Court of Justice confirmed that the Directive focuses liability on the producer, not any intermediary party in the supply chain (except where the producer is not identifiable), since "by obliging all suppliers to insure against such liability, it would result in products becoming significantly more expensive" (para. 28). See also C-358/08 *Aventis Pasteur SA v OB* [2010] 2 C.M.L.R. 16, which confirmed that where an injured person was not reasonably able to identify the producer, the supplier is obliged to act "on its own initiative and promptly" to identify the producer.

[150] See Berkowitz, N., "Strict liability for individuals? The impact of 3-D printing on products liability law", 92 Wash. U. L. Rev. 1019 (2015). Available at: http://openscholarship.wustl.edu/law_lawreview/vol92/iss4/8 .

[151] Product Liability Directive, at art. 4.

[152] Ibid, at art. 6(1) and recital 6.

[153] *Boston Scientific* , at para. 38.

[154] Ibid, at para. 26.

[155] 4th Report, n. 129, at p. 7. For the UK, see *Ide v ATB Sales Ltd.* [2008] EWCA Civ 424.

[156] Opinion of Advocate General Bot (21.10.2014), at para. 3.

[157] Product Liability Directive, at art. 7(e).

[158] Fondazione Rosselli, *Analysis of the economic Impact of the Development Risk Clause as provided by Directive 85/374/EEC on liability for defective products*, Contract No. ETD/2002/B5, available at http://www.palmigiano.it/wp-content/uploads/2013/12/dev-risk-clause-study_final-report.pdf

[159] See *Baker v Quantum Clothing Group* [2011] UKSC 17.

[160] *Commission v United Kingdom (Re the Product Liability Directive)(C-300/95)* , [1997] 3 C.M.L.R. 923, at 26-28.

[161] Product Liability Directive, at art. 15.1(b). Only Luxembourg and Finland have adopted this position. Reed and Angel, n. 141, at p. 113, note that given the practice of releasing software that is not entirely 'bug-free', it would be arguable that a software producer who failed to discover even a serious defect would be able to take advantage of the defence, so long as the defect is not in an area of the program that would be tested as a matter of course by others in the industry.

[162] [2014] EWHC 2956.

[163] 4th Report, n. 128, at p. 7.

[164] Product Liability Directive, at art. 9. So damage to the device itself, so-called 'transaction damage' is not covered. See C-285/08, *Société Moteurs Leroy Somer v Société Dalkia France* [2009] E.C.R. I-4733.

[165] *Boston Scientific* , at para. 49.

[166] Product Liability Directive, at art. 9(b).

[167] Ibid, at art. 12.

[168] Directive 2001/95/EC 'on general product safety' (OJ L 11/4, 15.1.2002), at Art. 1(1). As pointed out by Pisciotta, G.,*La responsabilità per danno da prodotto e la produzione Agricola con metodo* biologico, in *Diritti fondamentali. Qualità dei prodotti agricoli e tutela del consumatore*, edited by Capizzano, Camerino (1993), a product can be 'secure' under the product safety regime and 'unsecure' under the product liability regime.

[169] Directive 2014/53/EU 'on the harmonization of the laws of the Member States relating to the making available on the market of radio equipment' (OJ L 153/62, 22.5.2014). Radio equipment "means an electrical or electronic product which intentionally emits and or receives radio waves for the purpose of radio communication and or radiodetermination or an electrical or electronic product which must be completed with an accessory such as antenna so as to intentionally emit and or receive radio waves for the purpose of radio communication and or radiodetermination" (Art. 1(1)).

[170] Council Directive 93/42/EEC 'concerning medical devices' (OJ L 169/1, 12.7.93), as amended. The Directive defines such 'devices' as including "the software necessary for its proper application" (art. 1(2)(a)).

[171] Nest Protect has been tested to comply with safety standards in the United States and Canada set out by: Underwriters Laboratories Inc., California State Fire Marshal, Canadian Standards Association, and the British Standards Institution.

[172] See Van Leeuwen, n. 133, at p. 14.

[173] Although updates may obviously also be the cause of a defect. See 'Nest thermostat bug', at n. 84.

[174] Limited Warranty.

[175] C-484/08 *Caja de Ahorros y Monte de Piedad de Madrid v Asociacion de Usuarios de Servicios Bancarios (Ausbanc)* [2010] 3 C.M.L.R. 43, at para. 27.

[176] See Directive 2005/29/EC 'on unfair commercial practices', OJ L 149, 11.6.2005.

[177] OJ L 95/29, 21.4.1993, as amended ('Unfair Terms Directive'). The provisions were transposed into UK law by the Unfair Terms in Consumer Contracts Regulation 1999 (SI No

2083), but these were replaced by the Consumer Rights Act 2015, Part 2 ('CRA') as from 1.10. 2015.

[178] Ibid, at art. 3(1).

[179] Ibid, at art. 3(3), referring to the Annex.

[180] Ibid, at arts. 4(1) and 5 respectively. Art. 4(2) is a limitation to the scope of assessment, excluding 'the definition of the main subject matter' and 'the adequacy of the price and remuneration', if they are drafted in plain and intelligible language; although Member States may ignore this limitation when transposing the Directive, in favour of a higher level of protection (see *Caja de Ahorros*, n.171).

[181] C-26/13 *Árpád Kásler v OTP Jelzálogbank Zrt* [2014] Bus.L.R. 664.

[182] Ibid, at para. 71.

[183] This wording has been inserted into the CRA at s. 64(5).

[184] *Kásler* , at para. 74. See also C-96/14 *Van Hove v CNP Assurances SA* [2015] 3 C.M.L.R. 31.

[185] C-92/11 *RWE Vertrieb AG v Verbraucherzentrale Nordrhein-Westfalen eV* [2013] 3 C.M.L.R. 10.

[186] Ibid, at para. 50. See also C-472/10 *Nemzeti Fogyasztovedelmi Hatosag v Invitel Tavkozlesi Zrt* [2012] 3 C.M.L.R. 1, at 29.

[187] See Leone, C., "Transparency revisited - on the role of information in the recent case-law of the CJEU", *European Review of Contract Law* Vol. 10, Issue 2, 312-325.

[188] T&Cs, preamble.

[189] CMA, *Unfair contract terms guidance*, CMA37, 31.7.2015 ('CMA Guidance'), at para. 2.54. Available on www.gov.uk.

[190] See for instance Meshare Terms and Conditions of Sale at https://www.meshare.com/sales-terms/; Losono General Terms and Conditions athttps://lono.io/general-terms-and-conditions-of-sale; Neposmart Sale Terms and Conditions at https://neposmart.com/sales-terms-and-conditions.

[191] CRA, s. 61.

[192] The EULA states that 'THIS IS A LEGAL AGREEMENT', while the OS Compliance Notice states that by clicking 'Accept' you have read and accepted the Download Agreement. The uncertain status of OS notices is well recognized, see McDonagh, L., 'Copyright, Contract and FOSS' in Shemtov and Walden, *Free and Open Source Software: Policy Law and Practice*, OUP, 2013.

[193] CRA, s. 73.

[194] Ibid, s. 68.

[195] CMA Guidance, at para. 2.5.

[196] Unfair Terms Directive, at art. 7.

[197] Phrase used by Lord Bingham in *The Director General of Fair Trading v First National Bank plc* [2001] UKHL 52.

[198] E.g. the Ecobee 3 smart thermostat comes with only three documents: Privacy Policy & Terms of Use, Terms of Sale, Reseller Terms (https://www.ecobee.com/legal/).

[199] E.g. the Insolvency Act 1986 has recently been amended (by SI 2015/989) to prevent supply contracts for certain IT goods and services from terminating on an insolvency event where they are considered 'essential' to a business.

[200] See also, for example, the treatment of 'digital content' contracts under the Consumer Rights Directive 2011/83/EU (OJ L 304/64, 22.11.2011) and the Commission's proposal 'concerning contracts for the supply of digital content' COM(2015) 634 final, 9.12.2015.