DOI: 10.18254/S278229070019585-9 Book review

Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies

© 2022 Natalia V. Kozlova[a], Daria A. Motovilova[b]

[a, b] Lomonosov Moscow State University, Russia

Abstract. The present work is a review of the book "Internet of Things and the Law" by Dr. Guido Noto La Diega. Unlike other analyses that tend to focus on individual issues and are US-centric, this study is an updated comprehensive reflection on the problem from a European socio-legal perspective. Having identified IoT-generated risks, the author critically assesses how these risks can be tackled by EU contract law, consumer protection law, data protection law and intellectual property law.

Keywords: Internet of things, EU law, consumer protection, data protection, intellectual property rights

For citation: Natalia V. Kozlova and Daria A. Motovilova. 2022. Internet of Things and the Law. *Law & Digital Technologies* 2(1): 43–48.

"Internet of Things and the Law" summarizes the many years research of Dr. Guido Noto La Diega, who is professor of Intellectual Property Law and Privacy Law at the University of Stirling, member of the European Commission's Expert Group on AI and Data in Education and Training, director of 'Ital-IoT' Centre of Multidisciplinary Research on the Internet of Things, research associate at UCL Centre for Blockchain Technologies and fellow of the Nexa Center for Internet and Society. This research started as a PhD thesis (Noto La Diega 2014), further developed in a series of articles (Noto La Diega 2016; 2017a; 2017b; 2018; Noto La Diega and Walden 2016; Noto La Diega and Sappa 2020) and finally condensed in the above-mentioned book.

Unlike other analyses that tend to focus on individual issues like privacy, cybersecurity or competition law and are US-centric, this study is an updated comprehensive reflection on the Internet of Things (IoT) from a European socio-legal perspective. The author defines his methodology as Marxist and aims to raise awareness, or in Marxist terms, "to heighten class consciousness" about the risks of technologically-driven capitalism.

The three pillars on which the analysis is build upon are the following. *Surveillance Capitalism* by Shoshana Zuboff draws a parallel between the industrial capitalism studied by Marx and the modern IoT-powered capitalism where every IoT user becomes a data producer exploited by capitalists (Zuboff 2019). *Re-engineering Humanity* by Brett Frischmann and Evan Selinger highlights the IoT risks of erasing the "freedom to be off, to be free from systemic, environmentally architected human engineering." (Frischmann and Selinger 2018, 124). *Between Truth and Power* by Julie E. Cohen demonstrates that both networked media infrastructures (code) and legal institutions mediate between truth and power and therefore "law is not – and never could be – simply an instrumentality for the promotion of just outcomes." (Cohen 2019, 5).

Along with its significant socio-economic impact, the IoT, according to Noto La Diega, "*disrupts many of the dichotomies upon which the law has been built, most notably good-service, hardware-software, tangible-intangible, consumer-trader, consumer-worker, human-machine, security-cybersecurity, online-offline*." This urges a cautious analysis of the phenomenon and a critical assessment of the existing regulation.

In Chapter 1 the author studies the obstacles to regulation of IoT and possible solutions proposed by the EU authorities. The first and foremost problem researchers face is the lack of a generally accepted definition of the Io T. Noto La Diega proposes to define a 'Thing' as *"[a]n inextricable mixture of hardware, software, service, and data that has (inter)connectivity, sensing, and actuating capabilities and interfaces the physical world*". As such, features as physicality, (inter)connectivity, equipment with sensors and actuators are more or less obvious for many scholars. This fact that IoT devices ('Things') are 'an inextricable mixture of hardware, software, service, and data' deserves special attention from legal researchers and regulators since it blurs the conventional software-hardware, goods-services, and online-offline dichotomies.

Along with the difficulty in understanding the concept, the author reveals other reasons why IoT becomes too complex to regulate. They are:

1) *The lack of single IoT taxonomy* resulting from sectoral fragmentation and partially standardised enabling technologies. For example, self-driving cars and drones both fall under the scope of 'Things' but are regulated by different authorities.

2) *The intrinsically transnational character of Things*, which are concurrently located in many jurisdictions and are highly mobile. The EU attempted to solve this problem through various legal instruments, three of which drew the author's attention[1].

3) *The 'relational black box'*, i.e., the IoT's complex supply chain and sophisticated ecosystem that led Thing users to enter into several relationships with different actors without necessarily being aware of it (further developed in Chapter 2).

Having identified these problems, Dr. Noto La Diega further describes the EU approach to IoT regulation. The researcher expounds that the European Union has a long history of IoT regulation via soft laws. The first non-binding way to indirectly regulate the IoT was through funding of research and innovation. These initiatives included the European Research Cluster on the Internet of Things (IERC, launched in 2010) and the IoT European Platform Initiative (IoT-EPI, launched in 2016). The second step was the launch of the Alliance for Internet of Things Innovation (AIOTI) to support the creation of 'an innovative and industry driven European Internet of Things ecosystem' in 2015. The third initiative was the attempt to implement European values in the IoT via European Commission Staff Working Document entitled *Advancing the Internet of Things in Europe*. The fourth recent trend is the ethical approach which is manifested in the proposed Artificial Intelligence Act. The fifth and the most recent way to regulate IoT via soft laws is the regulation by design. First articulated by Lawrence Lessig (1999) this idea has found its followers among both researchers and lawmakers. By way of illustration the author refers to the UK Government's *Code of Practice for Consumer IoT Security.* Accepting that soft law might be more efficient in burgeoning industries, Dr. Noto La Diega, however, presents several arguments against a soft approach to IoT regulation, the strongest of which is that self-regulation is not actual regulation since regulation aims "to *alter the behaviour of others*. . . with the intention of producing a broadly identified outcome or outcomes", while self-regulation is self-directed. As for EU hard law relevant for IoT, it includes Sale of Goods Directive, Digital Content Directive (both discussed in Chapter 3) and European Electronic Communications Code. The author argues that IoT regulation should comprise both hard and soft laws and "*the crucial point will be to find the right mix of the two*". This can be achieved via "coregulation", where public and private actors develop the rules together. At the EU level the successful example of coregulation was the industry-led framework approved by a public law body in relation to privacy impact assessments of RFID applications. However, it is an open question which institution should supervise IoT regulation at the international level. Dr. Noto La Diega concludes that IoT regulation should be viewed as a complex strategy with a focus on hard law.

Chapter 2 reveals the main consumer threats in the Io T. Recognizing that IoT has the potential to greatly benefit consumers and society at large, the author warns about the risks it creates. These risks include:

(i) Surveillance capitalism and its challenges to privacy and data protection.

(ii) The 'death of ownership' that transforms consumers into digital tenants because either IoT traders retain ownership of the Thing or retain control over it via IP rights, contracts, and technological measures.

(iii) Private ordering 'by bricking', that is the IoT traders' ability to remotely monitor consumers and automatically downgrade the Thing, discontinue the service, remove functionalities, determine the lifespan of the Thing and even deactivate or 'brick' it.

(iv) Defective and vulnerable Things. Current legal regimes struggle to cope with new defects (e.g., software updates, inaccurate sensors, etc.) and vulnerabilities (e.g., the limitations stemming from software instructions and training datasets that affect the capacity to predict human behaviour in real-world scenarios).

(v) IoT-commerce and the limited opportunities to inform consumers who make transactions while immersed in hyper-connected interface-free environments.

(vi) The Internet of Personalised Things. Things allow traders to personalise products, services, prices, and 'legals.' Situational data and granular knowledge of biases and human vulnerabilities allow these traders to manipulate consumers and even discriminate against them, thus hindering their trust.

(vii) The contractual quagmire, namely the plethora of agreements (terms and conditions, privacy policies, end-user licence agreements, etc., collectively 'legals') that IoT consumers are forced to accept when using their Things.

To illustrate how an IoT user sticks in the contractual quagmire, the author endeavors the case study of Amazon Echo (smart speaker) 'legals'. As the study shows, to understand his or her rights and obligations an Echo owner should get acquainted with 246 legals that include 24 core legals, 55 Thing-as-a-Service-related legals, 12 developers' legals, 56 legals for the prosumer, 97 cloud-related, and 2 sustainability legals. Moreover, consumers should

[1] Cross-Border Service Portability Regulation, Geoblocking Regulation, Free Flow of Non-Personal Data Regulation.

also consider the legals of 7,400 third parties providing 60,000 Things that interact with Echo. This extremely complex set of rules leaves no chances to IoT consumers to challenge this private ordering and even to understand it.

Chapter 3 focuses on consumer issues in the Io T. The author critically assesses whether EU consumer contract laws can be used to overcome the power imbalance in IoT business-to-consumer transactions. In the EU, the current rules on consumer contracts resulted from the 'New Deal for Consumers' package that includes Directive 2019/2161 (Omnibus Directive) and Directive 2020/1828 (Representative Action Directive). Among other measures, the former gives the national authorities the power to impose fines of up to 4% of the trader's turnover, or up to €2 million when information on turnover is not available. The latter obliges Member States to put in place effective procedural mechanisms to allow qualified entities (for example, consumer organisations or public bodies) to bring class actions, including the right to obtain injunctions and compensation.

Under Unfair Terms Directive (as amended by Omnibus Directive), unfairness in consumer contracts can be of two types: 'of substance' and 'of form'. Unfairness of substance takes place when terms, contrary to the requirement of good faith, cause a significant imbalance in the parties' rights and obligations. As the author demonstrated in the previous chapter, IoT traders' data power put them in a strong bargaining position allowing them to exploit consumers' vulnerabilities and biases. This leads to conflict between IoT's contractual quagmire and good faith, and is potentially unfair of substance. However, it is for the national authorities to assess the unfairness of specific contract terms considering the specific circumstances of each case. To illustrate how national regulators assess unfairness, the author refers to 'Cloud Storage: Consumer Compliance Review' prepared by the UK Competition and Market Authority. As a result of this review, new (and more fair) provisions were introduced in Amazon Drive Terms of Use. Endorsing this positive development, Dr. Noto La Diega notes that considering (and amending) "*only one element of an intricate web of legals constitutes an inadequate solution to the problem*". Unfairness of form means that contracts lack transparency and are not drafted 'in plain intelligible language'. The author concludes that IoT contracts lack both of these features, and an average IoT user has neither time nor literacy and cognitive resources to read and understand all contracts they enter. Noto La Diega suggests imposing IoT traders to draft legals, taking into account some readability tests like a Flesch-Kincaid readability, to reduce information imbalances between IoT traders and consumers. Overall, more public scrutiny is needed to make IoT contracts fair and consumer-friendly.

IoT traders use the contractual quagmire to retain the control over Things: they can downgrade them and even 'brick' them, i.e., deactivate them so that consumers can no longer use Things. The researcher asks whether depriving consumers of their Things' 'smartness' can constitute an unlawful lack of conformity under EU law. Under the First Consumer Sales Directive, traders of consumer goods must guarantee that the goods are in conformity with the contract for at least two years after their delivery. However, IoT products are very specific and may fall outside the scope of the Directive which define 'good' as 'any tangible movable item'. In fact, the key component of Things is not the hardware but the software which is subjected to other set of rules. The author further asks whether the non-hardware components' lack of conformity can trigger the consumers' rights under the First Consumer Sales Directive, namely the right to have the goods repaired, replaced, reduced in price or have the contract terminated if the goods fail to be in conformity with the contract: (i) 'as described,' (ii) fit for a particular purpose, (iii) fit for the usual purpose, or (iv) 'as reasonably expected'. He then concludes that all four conformity presumptions apply to the IoT, therefore, consumers can effectively counter 'bricking' and related practices by exercising their rights to have the Thing's smartness restored. Moreover, it will not be burdensome for IoT traders to repair or replace intangible components of Things remotely thus keeping the contracts alive.

From January 1, 2022, a new set of consumer protection rules came into force in the EU as a result of the adoption of Directive 2019/771 ('Second Consumer Sales Directive') and Directive 2019/770 ('Digital Content Directive'). For the first time the conformity requirements will expressly apply to digital content and digital services. Other important developments comprise the express inclusion of 'goods with digital elements', definition of sale and inclusion of non-monetary exchanges, specifically, personal data as consideration. Even though goods are still defined as 'any tangible movable items', the Second Consumer Sales Directive explicitly includes 'goods with digital elements'. The latter incorporate (or are inter-connected with) a digital content or a digital service in a way that the absence of that digital content or digital service would lead to misfunctioning of goods. The author endorses the new wording because a Thing *"is rarely just a medium; it is integrated with intangible components that are often vital to its functioning"*. However, he notes that "*there is a vast grey area between a good whose digital components are vital to its functioning – falling within the scope of the Second Consumer Sales Directive – and goods that are exclusively a carrier of the digital content, to which the Digital Content Directive will apply*". Another amendment to the EU consumer protection law is the new definition of 'sales contract' that means 'any contract under which the seller transfers or undertakes to transfer ownership of goods to a consumer, and the consumer pays or undertakes to pay the price thereof.' However, as the author notes "*if the consumer does not acquire the ownership of the Thing, the contract will not qualify as sale and the relevant remedies will not apply*." Unlike the Second Consumer

Sales Directive, the Digital Content Directive unequivocally covers the scenarios where 'the consumer provides or undertakes to provide personal data to the trader.' The author supports this pragmatic approach declaring that it "*has broadened the scope of EU consumer law to strengthen the protection of consumers*". The final innovation, brought about by EU consumer law reform, relates to conformity of goods. The most important additions relevant for IoT industry are the new interoperability requirement and the duty to update goods with digital elements. The author concludes that the EU reform is likely to benefit the IoT and the digital economy. Hence, the existing tangible-intangible divide leaves grey areas that should be covered by national lawmakers.

One of the important sets of EU consumer protection rules are pre-contractual information duties, which impose traders to communicate with consumers and inform them about rights, risks, and obligations resulting from a business-to-consumer transaction. These duties are implied by Consumer Rights Directive. However, as Noto La Diega notes after a move from brick-and-mortar shops to e-commerce "*there is a further shift because computers decrease in size and increase in numbers, to the point that consumers transact while immersed in a hyperconnected always-on interface-free environment. In this immersive IoT-saturated environment, everything is connected and can potentially be used to conclude transactions, with little if any consumer awareness of whether a transaction is initiated, let alone the awareness of the associated rights, risks, and obligations*". Thus, IoT commerce challenges pre-contractual duties of information. The author underscores that overall EU consumer law is fit for a world of IoT-commerce. He suggests that the general rule to inform consumers in a clear and intelligible manner should be interpreted in creative ways that go beyond the traditional terms of service available on the trader's website. The consumers should be given information in the same format as they get used to interacting with Thing, i.e., via audio or video interface.

Chapter 4 is devoted to the vulnerability of both Things as they are defective and IoT users prone to be manipulated via the so-called Internet of Personalised Things. According to Dr. Noto La Diega, *"the production of vulnerable Things – programmed to be consumed as quickly as possible – and of vulnerable humans – prone to all sorts of manipulations – is one of the ways that the IoT realises the capitalistic enterprise*." To answer the question whether EU law can fix the problem of vulnerability, the author critically assesses non-contractual consumer protection laws, particularly the Product Liability Directive and the Unfair Commercial Practices Directive.

Drafted in the mid-Eighties the Product Liability Directive applies to 'products,' which are defined as all movables even when incorporated into another movable or immovable including electricity. Things categorized as a mixture of hardware, software, service, and data fall outside the scope of the Directive if the vulnerability of a Thing is caused by software errors or service disruption. To tackle this problem, the European Commission recommended a clarification on the definition of the product to 'ensure that compensation is always available for damage caused by products that are defective because of software or other digital features.' The author supports this development and suggests re-defining the concept of product to expressly include software, service, and data. He also backs the European Consumer Organisation's recommendation that the Directive should be revised to precisely include non-material damages. This would raise the chances for consumers to receive compensation for the harm caused by IoT devices even if there is no actual harm (e.g., lack of cybersecurity or data breach). Noto La Diega concludes that the reform of the Product Liability Directive would overcome the binaries that the IoT is challenging, such as product-service, hardware-software, and cybersecurity-security.

Huge amounts of data generated by Things gave rise to the Internet of Personalised Things where traders can customize the way products are built, priced, negotiated, sold, and interacted with by consumers. Noto La Diega argues that the Unfair Commercial Practices Directive (as amended by Omnibus Directive) is now more IoT-ready thanks to a broader definition of product – 'any good or service including immovable property, digital service and digital content, as well as rights and obligations' and a new 'black list' of certain unfair practices. However, he warns about its limitations. First, the Directive mainly focuses on the consumers' economic interests. Second, the Directive views societal interests exclusively through the lens of a consumer willing to take a transaction, and therefore the Directive disregards the forms of consumer manipulation not directly linked to a transaction. The author suggests introducing the amendments "*shifting the focus from the consumer's economic interests to the broader societal impact of unfairness in the Internet of Personalised Things.*"

Chapter 5 studies the regulation of IoT from the viewpoint of data protection laws. The author critically assesses the fitness of the General Data Protection Regulation (GDPR) to tackle IoT risks. As reported by author, the main data protection issues in the IoT are the following:

(i) *Lack of control and information asymmetry*. IoT users neither control how Things interact nor know which data the Thing sends back to the manufacturer.

(ii) *Quality of consent*. The GDPR sets a high standard of consent which can be hardly achieved by IoT producers for a number of reasons. Another problem is repurposing of IoT systems, i.e., their use for purposes other than those originally foreseen.

(iii) *The contested status of inferential data*. Big data generated by IoT, combined with advanced data mining techniques, and data gathered from other sources result in highly valuable inferences about the user's behaviour and vulnerabilities.

(iv) *The chimera of anonymization*. Using Things leaves almost no chances for users to remain anonymous.

(v) *The shift of the compliance burden from the IoT company to the end-user*. The more Things are used at home and in public spaces (e.g., wearables and mobile), the more data are collected with the aid of users that give rise to IoT manufacturers' and users' joint controllership.

(vi) *Digital dispossession*. IoT manufacturers tend to control both the algorithms that underpin the IoT system and the data that this system produces. This is made via both 'technical' secrecy due to the opacity of the algorithms, and 'legal' secrecy established through a combination of trade secrets, proprietary software, and contracts. Being subjected to constant surveillance and manipulation, IoT users are deprived of their privacy, autonomy and dignity.

Trade secrets play a key role in digital dispossession. The author argues that the GDPR provides necessary tools to overcome the conflict between trade secrets and data protection and thus enables users to regain some control over personal data. However, one should not overestimate the role of the GDPR in the struggle against surveillance capitalism. According to Noto La Diega, data subjects are merely "unwitting workers of the data economy" and the GDPR just "*allows us data subjects-unwitting workers to maintain ourselves thus being available for future exploitations*."

In Chapter 6, the author provides insight into the role of IP rights (IPRs) in Io T. Based on *Owned,* the seminal work by Joshua Fairfield, and his statement about 'death of ownership', Noto La Diega further develops this idea by demonstrating how IP abuses in the IoT turn IoT users into digital tenants. He writes: "*IoT companies factually, technologically, and legally control the Thing – and ultimately its users – by controlling virtually each of its components and layers*." The author reinforces his statement by referring to Amazon Echo which is protected by 84 patents and 427 trademarks combined with dozens of legals. The combination of factual, technological, and legal controls over the Thing results in decreased user power over the Thing, and increased corporate power over the Thing and over user-generated content. Noto La Diega draws a parallel between IoT economy and feudalism and states that in the same manner as medieval villein was obliged to perform unpaid labour-service, IoT users are "becoming unwitting workers". To illustrate, the author considers an example where Facebook leveraged user-generated hashtags as a proxy to human annotations for training purposes and managed to achieve an all-time record-high score of 85.4 percent on image recognition accuracy.

Noto La Diega finds that existing IP limitations do not suffice to restore the balance between the IoT company-rightsholder and the end-user as well as between public interest and private interest generally. Due to overlapping IPRs, an act allowed under one regime (e.g., reverse engineering under copyright law) can be qualified as infringement under another (e.g., patent law or trade secret law). The author "*to leverage European fundamental rights – mainly freedom of expression and prohibition of abuse of rights – to (i) interpret existing exceptions as user rights that are of equal standing as the IP holder's rights; (ii) recognise an autonomous open-ended defence along the lines of fair use in the US.*"

We are aware that this review has highlighted only some of the problems raised by the author. We assume that in *Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies*, an inquisitive reader will find issues of their particular interest. We are of the opinion that the book under review contributes greatly to the studying of Internet of Things. The book combines rigorous analysis with brave thought-provoking ideas. Unlike other monographs, it tackles the IoT from different angles, thus allowing the reader to build a complete view of the problem. Its focus on EU law reveals both advantages and limitations existing in one of the leading world economies, and therefore might be beneficial for lawmakers from developing countries. Young scholars with academic potential may draw from this seminal work in their research on the risks created by techno-regulation. We wholeheartedly recommend *Internet of Things and the Law* by Guido Noto La Diega to our readers, and believe that the monograph will be greatly appreciated in Academia.

REFERENCES

1. Cohen, Julie E. 2019. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford Scholarship Online.
2. Fairfield, Joshua A.T. 2017. *Owned: Property, Privacy, and the New Digital Serfdom*. Cambridge University Press.
3. Frischmann, Brett M., and Evan Selinger. 2018. *Re-Engineering Humanity.* Cambridge University Press.
4. Noto La Diega, Guido. "Il paradigma proprietario e l'appropriazione dell'immateriale." PhD thesis. Università degli Studi di Palermo, 2014.

5. Noto La Diega, Guido. 2016. Clouds of Things: Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom. *Journal of Law & Economic Regulation* 9(1): 69–93.
6. Noto La Diega, Guido, and Ian Walden. 2016. Contracting for the "Internet of Things": Looking into the Nest. *European Journal of Law and Technology* 219.
7. Noto La Diega, Guido. 2017a. Machine Rules. Of Drones, Robots and the Info-Capitalist Society. *Italian Law Journal* 2: 367–404.
8. Noto La Diega, Guido. 2017b. Software Patents and the Internet of Things in Europe, the United States and India. *EIPR*39 (3): 173–184.
9. Noto La Diega, Guido. 2018. Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information. *JIPITEC*9(1).
10. Noto La Diega, Guido, and Cristiana Sappa. 2020. The Internet of Things at the Intersection of Data Protection and Trade Secrets. Non-Conventional Paths to Counter Data Appropriation and Empower Consumers. *Revue européenne de droit de la consommation / European Journal of Consumer Law* 3: 419–458.
11. Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.