Scattarreggia, Emanuele

Conference Paper

Protecting Consumers & the Market in the Cyborg Era

ITS 33rd European Conference 2025: "Digital innovation and transformation in uncertain times", Edinburgh, UK, 29th June – 1st July 2025

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Scattarreggia, Emanuele (2025) : Protecting Consumers & the Market in the Cyborg Era, ITS 33rd European Conference 2025: "Digital innovation and transformation in uncertain times", Edinburgh, UK, 29th June – 1st July 2025, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/331306

Emanuele Scattarreggia *

PROTECTING CONSUMERS & THE MARKET IN THE CYBORG ERA

Abstract

The digital economy is currently experiencing an unprecedented phase of transformation, driven by the relentless evolution of artificial intelligence (AI) and the Internet of Things (IoT). These technologies have transcended from being mere tools of convenience to becoming integral components of daily life, ushering in what can be described as the era of consumer cyborgification. This term captures the essence of how humans are increasingly merging with technology, not just physically through wearable devices but also in decision-making processes through AI-driven insights and nudges. As these technologies grow more sophisticated, they collect, analyse, and act upon enormous volumes of personal data. This capability, while beneficial in tailoring services and enhancing user experiences, simultaneously raises profound questions about privacy, autonomy, and consumer rights. The potential for misuse or overreach in data handling poses threats to individual privacy, while the autonomous decision-making aspects of AI challenge traditional notions of consumer autonomy. Yet, there is a silver lining. AI presents significant opportunities to guide consumers towards more informed, healthier, or economically beneficial choices. Through strategic nudging, AI can enhance consumer well-being, leading to a more efficient market where consumers are not only protected but empowered. However, the integration of such technologies calls for a re-evaluation of existing regulatory frameworks to ensure that they are fit for purpose in this new digital landscape. This paper delves into how current AI and consumer protection regulations can be adapted to meet these emerging challenges. The objective is to propose a framework where technological advancement and consumer protection can coexist synergistically. We aim to explore how laws can be refined to safeguard privacy and autonomy without stifling the innovation that drives economic and social benefits.

SUMMARY

* PhD student in Law at the University of Sydney. E-mail: esca0791@uni.sydney.edu.au.

1 INTRODUCTION

The digital economy is undergoing a profound transformation, driven by the rapid integration of artificial intelligence (AI) and the Internet of Things (IoT) into everyday life[1]. These technologies are reshaping the architecture of consumer choice not only through physical integration – via wearable and smart devices – but also through cognitive convergence, where AI systems directly guide consumer decisions via data-driven insights and behavioural nudges[2].

This paper employs the concept of *consumer cyborgification* to capture this dual transformation: the fusion of human and machine, both physically and cognitively[3]. While such innovations promise enhanced personalisation, efficiency, and decision-making[4], they also raise profound legal challenges[5]. The automated processing of vast amounts of personal data and the increasing use of AI-powered "hyper-nudges" may threaten individual privacy[6] and autonomy[7], calling into question traditional notions of informed and voluntary consumer choice.

Against this backdrop, this paper examines whether existing legal frameworks in the UK and EU can effectively address both the opportunities and the risks of consumer cyborgification. In particular, the research investigates whether these frameworks can promote innovation while safeguarding autonomy, privacy, and human dignity. Drawing on behavioural law and economics, this interdisciplinary study explores how the law can encourage beneficial nudging while mitigating the risks of manipulation.

The overarching research question is:

- How can current AI and consumer protection laws in the EU and UK be adapted to safeguard individual privacy, autonomy, and human dignity in an era where technology increasingly blends with everyday life, while simultaneously ensuring that such regulations do not stifle innovation?

2 AI, IOT, AND CYBORGS

Our contemporary world is undergoing an unprecedented technological transformation. On one hand, AI is reshaping not only how we live and work, but also how we conceive of

[1] Norhilmi Muhammad *et al.*, 'The Impact of Industry 4.0 on Digital Marketing: Leveraging Emerging Technologies for Business Growth' (2023) 13 International Journal of Academic Research in Business & Social Sciences 12, 66-67.
[2] Karen Yeung, ''Hypernudge': Big Data as a mode of regulation by design' (2017) 20 Information, Communication & Society 1, 122.
[3] Nicole J. Jess *et al.*, 'Served by a Cyborg: Understanding Consumer Responses to Human Enhancement Technologies' (2024) 24 Marketing Science Institute Working Paper Series 149 <https://thearf-org-unified-admin.s3.amazonaws.com/MSI_Report_24-149.pdf> accessed 12 June 2025.
[4] Albérico Travassos Rosário and Ricardo Jorge Raimundo, 'The Integration of AI and IoT in Marketing: A Systematic Literature Review' (2025) 14 Electronics 1854, 21.
[5] Ibid. 18.
[6] *See* (n 2) 124-126.
[7] Ibid. 123-124.

ourselves as human beings[8]. Questions once confined to science fiction and philosophy – *Are we the sole intelligent species? Can human intelligence be replicated or even surpassed[9]?* – are now the subject of serious academic and policy discussions[10]. The very notion of intelligence, long defined and measured by tools such as IQ, is increasingly strained in a world where machines are surpassing humans in executing complex tasks[11]. This evolution challenges deeply held assumptions about human uniqueness and calls into question our role:

- Are we creators destined to coexist with our creations, or progenitors who must fade for the next generation of intelligence to thrive?

On the other hand, the IoT represents a technological framework capable of bridging the physical and digital worlds. Typically composed of a three-layer architecture – 1) the perception layer, which collects data via sensors and smart devices; 2) the network layer, which enables data transmission and device communication; and 3) the application layer, which processes data to generate personalised outputs and behavioural nudges[12] – IoT systems are going to be increasingly integrated with AI technologies. Deep neural networks can now enhance not only the sensory and processing capacities of these systems, but also their ability to tailor outputs in dynamic and environment-sensitive ways[13].

In this context, the trajectory of human-machine interaction appears to be less about replacement and more about integration. Rather than being eclipsed by our creations, we are entering a phase of convergence.

We are witnessing the emergence of a **cyborg era** – an era in which humans and intelligent systems are becoming cognitively and functionally intertwined[14].

2.1 WHO IS THE CYBORG, AND WHAT DOES THAT MEAN FOR CONSUMER LAW?

The proliferation of IoT technologies in consumer markets has led to the emergence of a new kind of consumer: the cyborg consumer. But who are they?

The concept of the "cyborg consumer" explores how technology – particularly the integration of human and machine – reshapes consumer behaviour, identity, and

[8] Murray Shanahan, 'The Technological Singularity' (The MIT Press 2015) xv.
[9] Ibid. xvi.
[10] Mindaugas Kiškis, 'Legal framework for the coexistence of humans and conscious AI' (2023) Front. Artif. Intell. 1-8.
[11] Cf. Shane Legg and Marcus Hutter, 'Universal Intelligence: A Definition of Machine Intelligence' (2007) 17 Minds & Machines 4, 391-444.
[12] Jing Zhang and Dacheng Tao, 'Empowering Things with Intelligence: A Survey of the Progress, Challenges, and Opportunities in Artificial Intelligence of Things' (2020) 20 IEEE Internet of Things Journal 10, 1.
[13] Cf. Agostino Marengo, 'The Future of AI in IoT: Emerging Trends in Intelligent Data Analysis and Privacy Protection' (2023) Preprints.org 7-8 <www.preprints.org/manuscript/202312.2184/v2> accessed 12 June 2025.
[14] Cf. Benjamin Clubbs Coldron *et al.*, 'When the Internet Gets Under Our Skin: Reassessing Consumer Law and Policy in a Society of Cyborgs' (2025) Journal of Consumer Policy 5.

vulnerabilities within both digital and physical marketplaces[15]. In essence, the cyborg is a hybrid resulting from the blending of the human and the machine[16]; and the cyborg consumer is that hybrid acting as a consumer[17] – namely, a natural person acting for purposes that are outside their "trade, business, craft or profession[18]". Human-machine hybridisation is embraced in exchange for the promise of an enhanced life experience and, in the realm of consumption, for tailored, interactive, and personalised outputs that aim to improve the efficiency of economic decision-making by enabling machines to infer and respond to our preferences and needs[19].

Notably, the merging of AI and IoT – commonly referred to as the Artificial Intelligence of Things (AIoT) – can leverage AI's capacity to process, analyse, and categorise immense volumes of data[20], while taking advantage of the IoT's unique characteristic of "following the person" across all domains of life, including the most intimate ones[21]. Through wearables or even implanted devices, AIoT technologies can develop a continuous and dynamic profile of the individual consumer, ultimately getting to know them better than they – and, perhaps, anyone else – know themselves[22].

This brings us to the second part of the question posed in the title of this paragraph: what does consumer cyborgification mean for consumer law?

To begin answering this, two foundational reflections are required. *First*, it is essential to recall the normative foundation of consumer law. This field emerged from the recognition of a structural imbalance in B2C transactions, which are physiologically characterised by the presence of a more vulnerable contractual party – the consumer, the weaker party – who requires protection, and a stronger party – the trader – who possesses superior bargaining power, information, and resources. To remedy this structural imbalance, consumer law has historically operated on the assumption that empowering consumers with adequate information would enable them to make rational and informed decisions[23]. Accordingly, legal frameworks have focused on imposing duties of transparency and disclosure upon traders. Indeed, the primary threat to consumer empowerment was considered to be information asymmetry. Therefore, imposing a duty

[15] Ibid. 4-7.
[16] Cf. Donna Haraway, *Simians, Cyborgs, and Women: The Reinvention of Nature* (Routledge 1991) 150.
[17] Cf. Markus Giesler and Alladi Venkatesh, 'Reframing the Embodied Consumer as Cyborg. A Posthumanist Epistemology of Consumption' (2005) Advances in Consumer Research 32, 664.
[18] *See* both Article 2(3) UK Consumer Rights Act 2015, and Article 2(a) EU Unfair Commercial Practices Directive.
[19] Cf. (n 14) 1.
[20] *See* Shakhrul Iman Siam *et al.*, 'Artificial Intelligence of Things: A Survey' (2024) ACM Trans. Sensor Netw. <https://arxiv.org/pdf/2410.19998> accessed 12 June 2025.
[21] *See* (n 14) 11.
[22] Cf. Shabahang Arian, 'Vulnerability in the Age of Metaverse and Protection of the Rights of Users Under EU Law' in Camilla Crea and Alberto De Franceschi (eds.), *The New Shapes of Digital Vulnerabilities in European Private Law* (Nomos 2024) 189-190.
[23] Bettina Heiderhoff, 'Information Obligations (Consumer Contracts)' (2009) Max-EuP 2012 <https://max-eup2012.mpipriv.de/index.php/Information_Obligations_(Consumer_Contracts)> accessed 12 June 2025.

on the trader to provide all the information to the consumer was regarded as an optimal strategy to place the latter in a position to make an informed and rational choice[24].

However, behavioural science has since revealed that this assumption is flawed[25]. Information asymmetry, while significant, is not the sole obstacle to optimal decision-making. Cognitive biases, heuristics[26], limited attention[27], and the influence of our emotions[28] all play substantial roles in our economic decisions[29] – factors that pure transparency cannot rectify[30].

In parallel, the digital environment has introduced new threats – such as dark patterns[31], addictive design[32], and manipulative personalisation[33] – collectively referred to as digital manipulation[34], further complicating the consumer landscape. Consequently, the concept of the "average consumer" as the rational standard – onto which consumer law has been built – appears increasingly outdated[35]. Likewise, many of the traditional consumer protection safeguards are being outpaced by the sophistication and inherent opacity of AI-driven systems.

This brings us to the *second* reflection. Consumers today are increasingly enmeshed in digital environments that continuously observe, learn from, and interact with them[36]. Wearable fitness trackers, smartwatches, AI-powered voice assistants, AI-driven cars, and algorithmic recommendation systems[37] are not merely passive tools; they actively shape the consumer's experience. These technologies collect personal data, anticipate preferences, adjust outputs in real time, and – importantly – nudge users towards certain

[24] Michael G. Faure and Hanneke A. Luth, 'Behavioural Economics in Unfair Contract Terms. Cautions and Considerations' (2011) J. Consum. Policy 34, 338.
[25] Cf. Daniel Kahneman, *Thinking Fast and Slow* (Farrar, Straus and Giroux 2013). Daniel Kahneman *et al.*, *Noise. A Flaw in Human Judgement* (William Collins 2022) 161-175.
[26] Steve Dale, 'Heuristics and biases: The science of decision-making' (2015) 32 Business Information Review 2, 93-98.
[27] Richard H. Thaler and Cass R. Sunstein, *Nudge. Improving Decisions About Health, Wealth, and Happiness* (Yale University Press 2008) 35.
[28] Scott Rick and George Loewenstein, 'The Role of Emotion in Economic Behavior' in Michael Lewis *et al.* (eds), *Handbook of Emotions* (The Guilford Press, 3rd edn, 2008) 138-150.
[29] M. Neile Browne *et al.*, 'Protecting Consumers from Themselves: Consumer Law and the Vulnerable Consumer' (2015) Drake Law Review 63, 182.
[30] *See* Cass R. Sunstein *et al.*, 'A Behavioral Approach to Law and Economics' (1998) 50 Stanford Law Review 1471, 1533-1534.
[31] Catalina Goanta *et al.*, 'Consumer Protection and Digital Vulnerability: Common and Diverging Paths' in Camilla Crea and Alberto De Franceschi (eds), *The New Shapes of Digital Vulnerability in European Private Law* (Nomos 2024) 32-34.
[32] Ibid. 76-77.
[33] Francisco Lupiáñez-Villanueva *et al.*, *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation* (European Commission, Final Report 2022).
[34] *See* Philipp Hacker, 'Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection and privacy law' (2023) Eur Law J. 29, 142-175.
[35] Cf. Anne-Lise Sibony, 'Can EU Consumer Law Benefit from Behavioural Insights? An Analysis of the Unfair Practices Directive' (2014) European Review of Private Law 6, 903.
[36] *See* (n 14) 5. Zanda Davida, 'Consumer Decision-Making Autonomy in the Digital Environment: Towards a New Understanding of National Courts' Obligation to Assess Ex Officio Violations of Fair Commercial Practices' (2024) European Journal of Risk Regulation 15, 1034.
[37] *See* Luigi Portinale and Alessandro Abluton, 'Artificial Intelligence for Consumers. Advances in Recommendation Systems' in Larry A. DiMatteo *et al.* (eds), *The Cambridge Handbook of AI and Consumer Law* (Cambridge University Press 2024) 9-18.

behaviour or choices. In so doing, they not only respond to but may also create new desires, expectations, and dependencies[38].

What we are witnessing, therefore, is a decisive shift into what may rightly be called the **cyborg era**, in which human decision-making is persistently influenced, complemented, and at times delegated to intelligent systems[39]. This integration is not solely physical – it is decisional. Consumers are not simply using AI-enhanced tools; they are also – whether consciously or unconsciously – relying on them to filter information, prioritise options, and navigate markets. Consumer cyborgification, in this sense, refers to the progressive outsourcing of cognitive processes to machines that function as invisible co-pilots in everyday life. As the boundaries between human and machine agency become increasingly blurred, core legal categories such as "choice", "intent", and "consent" demand critical re-examination[40].

In this evolving reality, it becomes evident that consumer law – designed for "just human" consumers – may no longer suffice. There is an urgent need not only to reinterpret existing norms through the lens of behavioural science and in light of technological advancements, but also to propose legal reforms that can both mitigate the risks and harness the opportunities of the cyborg era.

2.2 REAL-WORLD ENCOUNTERS: AIOT AND THE CYBORG CONSUMER IN PRACTICE

The theoretical construct of the cyborg consumer finds tangible expression in contemporary technologies that seamlessly integrate AI with IoT. AIoT technologies exemplify the convergence of human and machine, where these advanced devices not only augment human capabilities[41] but also influence decision-making processes in real time[42]. This paragraph aims to provide some real-world examples of AIoT and their interaction with consumers.

- **AI-Powered Smartwatches**

Among the most advanced and widespread manifestations of AIoT integration are AI-powered smartwatches, such as the Apple Watch. These devices employ AI algorithms to process data from onboard sensors (e.g., accelerometer, gyroscope, heart rate sensor, and ECG), offering consumers real-time feedback and predictive insights across health, fitness, and daily routines. For example, activity monitoring adapts to user behaviour to

[38] *See* (n 22) 190-191.
[39] Mark Fenwick and Paulius Jurcys, 'From Cyborgs to Quantified Selves. Augmenting Privacy Rights with User-Centric Technology and Design' (2022) 13 JIPITEC 1, 28. Lena Bjørlo *et al.*, The Role of Consumer Autonomy in Developing Sustainable AI: A Conceptual Framework (2021) 13 Sustainability 2332, 6-7.
[40] *See* (n 14) 10.
[41] Rustam Pirmagomedov and Yevgeni Koucheryavy, 'IoT technologies for Augmented Human: A survey' (2021) Internet of Things 14, 1-9. Jie Li *et al.*, 'Beyond Human: Cognitive and Physical Augmentation through AI, Robotics, and XR – Opportunities and Risks' (2025) Workshop at the Augmented Humans (AHs) International Conference 2025 <https://arxiv.org/pdf/2503.09987> accessed 12 June 2025.
[42] *See* (n 2) 122.

suggest optimal times for physical exercise. Heart rate analysis can detect anomalies such as atrial fibrillation with reportedly high accuracy[43]. Furthermore, AI can enable more complex functions: for instance, an app developed by the Mayo Clinic is designed to detect left-ventricular dysfunction through AI analysis of ECG data collected by the Apple Watch[44].

Through on-device machine learning, Apple's smartwatches also provide personalised sleep analysis[45], proactive health alerts, crash and fall detection[46], and gesture-based interactions (e.g., the "Double Tap" feature[47]). According to Bloomberg, Apple is also working on a project to use AI and the data collected through the Apple Watch to deliver tailored recommendations and coaching programs[48].

These developments illustrate how smartwatches extend beyond passive tools and how they are becoming increasingly integrated agents that track, predict, and interact with users in near-continuous feedback loops. In effect, the Apple Watch acts as an externalised, AI-enhanced nervous system, augmenting consumer awareness and decision-making, thereby functioning as an extension of the user's cognitive and physiological faculties. At the same time, the machine's analysis of consumer data translates into tailored outputs that aim to influence consumer behaviour. The Apple Watch learns to understand the individual consumer, detect behavioural patterns, and deliver personalised, data-driven micronudges that ultimately steer consumer choices[49].

Gamification elements, such as Apple's "Activity Rings[50]", further reinforce the wearable's ability to guide the decision-making process by appealing to users' psychological triggers[51] – encouraging behaviour through activity awards, streaks, and challenge badges[52]. These techniques may be beneficial for their capacity to steer

[43] Sufyan Shahid *et al.*, 'Diagnostic Accuracy of Apple Watch Electrocardiogram for Atrial Fibrillation. A Systematic Review and Meta-Analysis' (2025) 4 Jacc: Advances 2, 1-10.
[44] Diagnostic and Interventional Cardiology, 'New App for Apple Watch Uses Artificial Intelligence to Detect Left-ventricular Dysfunction' (DAIC, 18 May 2022) <https://www.dicardiology.com/content/new-app-apple-watch-uses-artificial-intelligence-detect-left-ventricular-dysfunction> accessed 12 June 2025.
[45] Press Release, 'Apple introduces groundbreaking health features to support conditions impacting billions of people' (Apple, 9 September 2024) <apple.com/newsroom/2024/09/apple-introduces-groundbreaking-health-features/> accessed 12 June 2025.
[46] Press Release, 'Introducing Apple Watch Series 10' (Apple, 9 September 2024) <https://www.apple.com/newsroom/2024/09/introducing-apple-watch-series-10/> accessed 12 June 2025.
[47] Press Release, 'Apple Watch double tap gesture now available with WatchOS 10.1' (Apple, 25 October 2023) <https://www.apple.com/newsroom/2023/10/apple-watch-double-tap-gesture-now-available-with-watchos-10-1/> accessed 12 June 2025.
[48] Mark Gurman, 'Apple Plans AI-Powered Health Coaching Service and Mood Tracker' (Bloomberg Law, 25 April 2023) <https://news.bloomberglaw.com/health-law-and-business/apple-plans-ai-powered-health-coaching-service-and-mood-tracker> accessed 12 June 2025.
[49] Natasha D. Schüll, 'Data for life: Wearable technology and the design of self-care' (2016) 11 BioSocieties 3, 327-329.
[50] Apple, 'Close Your Rings' <https://www.apple.com/watch/close-your-rings/#:~:text=Three%20rings%3A%20Move%2C%20Exercise%2C,Activity%20app%20on%20Apple%20Watch> accessed 12 June 2025.
[51] *See* Michael Sailer *et al.*, 'How gamification motivates: An experimental study of the effects of specific game design elements on psychological need satisfaction' (2017) Computers in Human Behavior 69, 374-375.
[52] Gamification refers to the incorporation of game-like elements into the design of systems whose primary purpose is not game-related, with the aim of enhancing user engagement, sustaining motivation, and improving consumer

consumers towards beneficial choices for their bodies' and minds' health, but at the same time raise critical concerns regarding subtle manipulation and the autonomy of the user in decision-making processes.

- **AI-Enhanced Smart Glasses**

Smart glasses, such as the Ray-Ban Meta[53] and Envision Glasses[54], represent a cutting-edge frontier in AIoT integration. These wearable technologies embed AI to offer real-time functionalities, including language translation, contextual information delivery, and environmental awareness. By overlaying digital information onto the user's field of vision, smart glasses hold the potential to augment perceptual capabilities, effectively blending human sensory experience with AI[55].

The integrated AI operates as an assistant that continuously analyses both environmental stimuli and user-specific data to generate personalised outputs. These interactions create a fluid, dynamic relationship between the human and the machine: users may ask the AI for a recipe suggestion based on the contents of their fridge, request currency conversions, or receive relevant information about the building they are viewing. Over time, the AI adapts to individual preferences – such as recognising the user's favourite flowers – evolving into a context-aware, attentive, and emotionally attuned companion[56].

While these smart devices can offer profound benefits – particularly for consumers who are blind or have low vision – they also embody the core of cyborg consumerhood[57]: a human-machine hybridisation that extends cognitive and sensory functions. However, this

retention. *See* Muhammad Z. Hydari, 'Health Wearables, Gamification, and Healthful Activity' (2023) 69 Management Science 7, 3921.

[53] To get a full look at the AI-powered Ray-Ban Meta glasses' sponsored capabilities, *see* Meta, 'AI Glasses' <https://www.meta.com/gb/ai-glasses/> accessed 12 June 2025.

[54] *See* Envision, 'meet ally – your everywhere AI assistant now on the Envision Glasses' on YouTube (25 November 2024) <https://youtu.be/GcwstAtgHOM?si=5RP4M3GMhtvvEkzi> accessed 12 June 2025.

[55] *See*, for instance, Orion – a Meta AI-powered smart glasses project: Meta, 'The future of wearables' <https://www.meta.com/en-gb/emerging-tech/orion/?srsltid=AfmBOooNppb_BHO-cJhvRWsghxVCCcytylSEZUXdbkjaznGSL-NMnYtd> accessed 12 June 2025.

[56] It is worth noting that one of the AI capabilities promoted by Meta is the system's ability to anticipate the user's needs and deliver recommendations even before the consumer formulates a request. *See* Meta, 'Ray-Ban Meta Glasses Add Live AI, Live Translation, & Shazam Support' (Blog, 16 December 2024) <https://www.meta.com/en-gb/blog/ray-ban-meta-v11-software-update-live-ai-translation-shazam/> accessed 12 June 2025. While this holds significant potential to enhance decision-making efficiency and save consumers considerable time, it also raises important concerns regarding consumer autonomy. If users come to rely on the AI's ability to know them better than they know themselves, and to provide solutions before questions even arise, it could ultimately weaken their autonomy and erode their capacity for independent thought. Thus, this development carries the dual potential to enhance human life while simultaneously risking the mortification of human cognition.

[57] The term "cyborg consumerhood" is used in this context to highlight how the very identity, role, and experience of being a consumer change when technology – such as AIoT – becomes deeply integrated into people's lives, shaping how they perceive themselves and their surrounding environment through a continuous loop of interactions. The consumer-AIoT experience often begins with an initial act of consumption – namely, the purchase of the product – but extends beyond it, persisting whenever the individual chooses to wear (or be integrated with) the device. Within this context, the boundaries between human and machine can become increasingly blurred, especially when assessing the impact of consumer cyborgification on human decision-making, preferences, and even awareness – all of which may be continuously shaped or co-created by the human-machine interaction.

integration also risks fostering psychological dependence. The AI's continuous presence, attentiveness, and responsiveness may lead to decisional overreliance[58] and psychological addiction[59], potentially shaping users' behaviour, consumption patterns, and even emotional expectations. The fact that these glasses are designed to process and respond to whatever the user sees – and fails to see – further underscores their deep cognitive embeddedness.

This development raises important implications for consumer law. The shifting locus of agency, where decisions and perceptions are co-produced by AI systems, challenges the foundational assumptions about informed choice and autonomous intent[60]. As these technologies become perceptual extensions of the individual, questions of manipulation, data governance, and behavioural nudging acquire a heightened urgency.

- **AI-Driven Vehicles**

In the realm of transportation, Tesla exemplifies the application of AIoT in vehicles[61]. Tesla cars – such as the S, 3, X, and Y models – are equipped with advanced AI and IoT technologies that create a networked, data-driven experience. These features position Teslas as AIoT vehicles, blending sensors, connectivity, and machine learning to interact with their drivers. Key AIoT elements include:

- **Autopilot and Full-Self Driving (FSD)**: Tesla's Autopilot and FSD (Supervised)[62] use AI to process data from cameras, radar, ultrasonic sensors, and GPS for semi-autonomous driving tasks, such as lane-keeping[63] and adaptive, traffic-aware cruise

[58] Cf. Ala Yankouskaya, 'Can ChatGPT Be Addictive? A Call to Examine the Shift from Support to Dependence in AI Conversational Large Language Models' (2025) Human-Centric Intelligent Systems 82-83.

[59] Human-AI interactions are characterised by a high level of personalisation: the AI analyses the user's unique cognitive and emotional patterns and delivers tailored emotional cues. The AI's ability to recognise individual preferences and satisfy psychological needs reinforces the development of a human-machine parasocial relationship, leading the human to experience a deep emotional bond towards a machine incapable of genuine reciprocity. Ibid. 78-79.

[60] In the context of cyborg consumerhood, AI-human interactions may evolve into what could be termed "co-intelligence". This notion refers to a shared decision-making process between the human and the AI system with which they interact. The AI continuously processes environmental and personal data inputs, and its outputs – which may take the form of suggestions and recommendations – along with the user's overreliance on AI's capacity to anticipate their needs and provide relevant, timely answers, may significantly influence the consumer's decision-making. This dynamic may transform the AI into a "cognitive partner", making it increasingly difficult, on a case-by-case basis, to determine who is more "accountable" for specific choices: the human or the AI. Cf. ibid. 83.

[61] Dashveenjit Kaur, 'When AI meets IoT – will the AIoT convergence reshape industries?' (TechWire Asia, 10 March 2021) <https://techwireasia.com/2021/03/when-ai-meets-iot-will-the-aiot-convergence-reshape-industries/> accessed 12 June 2025.

[62] To view the official Tesla descriptions, warnings, and note about FSD (Supervised), *see*, for example, Tesla, 'Model Y Owner's Manual', 'Full Self-Driving (Supervised)' section <www.tesla.com/ownersmanual/modely/en_us/> accessed 12 June 2025,.

[63] The Lane Assist system automatically steers the Tesla vehicle towards a position considered safer by the AI when it detects that the car is approaching an object. *See* ibid., 'Lane Assist' section <https://www.tesla.com/ownersmanual/modely/en_eu/GUID-ADA05DFF-963D-477D-9A51-FA8C8F6429F1.html> accessed 12 June 2025.

control[64]. FSD aims for advanced capabilities like traffic light and stop sign recognition[65]. Drivers engage with AI through the vehicle's touchscreen, voice commands[66], or steering yoke/wheel, receiving real-time feedback (e.g., lane change suggestions[67], obstacle warnings[68]). FSD (Supervised) requires active driver supervision, creating a collaborative human-AI dynamic[69].

- **Summon and Autopark**: Summon[70] enables drivers to remotely move and park their Tesla using the mobile app[71], while Autopark allows the vehicle to park itself in a selected spot with minimal driver input[72]. Tesla vehicles consequently combine AI and IoT to extend the driver's control, even beyond their physical presence, and to execute complex manoeuvres autonomously.

- **A Personalised Experience**: AI adjusts settings – such as seat position, climate, preferred media, audio levels, and steering sensitivity – learning and adapting on the driver's profile built over time thanks to behavioural algorithms, camera, and seat sensors[73]. IoT sensors feed data to AI, which personalises the experience[74],

[64] Traffic-Aware Cruise Control adjusts the Tesla's speed based on the presence of a vehicle in the same lane. If the road ahead is clear, it maintains the set speed. When a vehicle is detected, the system slows the car as necessary to maintain a safe distance from the vehicle in front. However, it does not replace the need for the driver to remain alert and manually apply the brakes when required. *See* Tesla, 'Model S Owner's Manual', 'Traffic-Aware Cruise Control' section <https://www.tesla.com/ownersmanual/2012_2020_models/en_us/GUID-50331432-B914-400D-B93D-556EAD66FD0B.html> accessed 12 June 2025.

[65] *See* Tesla, 'Model Y Owner's Manual', 'Traffic Light and Stop Sign Control' section <https://www.tesla.com/ownersmanual/modely/en_eu/GUID-A701F7DC-875C-4491-BC84-605A77EA152C.html> accessed 12 June 2025.

[66] Tesla, 'Voice Commands' (Tesla Support) <https://www.tesla.com/support/voice-commands> accessed 12 June 2025.

[67] *See* Tesla, 'Model S Owner's Manual', 'Autopilot Features' section: <https://www.tesla.com/ownersmanual/models/en_ie/GUID-20F2262F-CDF6-408E-A752-2AD9B0CC2FD6.html#:~:text=If%20you%20ignore%20a%20route,re%2Drouted%20to%20your%20destination> accessed 12 June 2025.

[68] *See* Tesla, 'Model X Owner's Manual', 'Doors' section: <https://www.tesla.com/ownersmanual/modelx/en_us/GUID-7A32EC01-A17E-42CC-A15B-2E0A39FD07AB.html> accessed 12 June 2025.

[69] For a visual representation of FSD capabilities, *see* the video 'Autopilot Full Self-Driving Hardware (Neighborhood Short)' on Vimeo (18 November 2016) <https://vimeo.com/192179726> accessed 12 June 2025.

[70] Strictly speaking, during Summon, the human is not physically inside the AIoT system (the Tesla vehicle) nor wearing an AIoT device that integrates their body with the machine – although an exception occurs when the consumer uses a smartwatch to initiate summoning. However, the driver's smartphone operates as an AIoT extension of the user's agency, functioning as a real-time remote-control interface connected to the vehicle's AI system.

[71] Tesla, 'Model 3 Owner's Manual', 'Summon' section <https://www.tesla.com/ownersmanual/model3/en_us/GUID-7D207174-88CD-4795-8265-9162A72AA578.html> accessed 12 June 2025.

[72] For a visual representation, *see* Tesla, 'Autopark | Model 3 and Model Y' (Tesla Support Videos) <https://www.tesla.com/support/videos/watch/autopark-model-3-and-model-y> accessed 12 June 2025.

[73] William Johnson, 'Tesla receives mind-blowing interior 'personalization system' patent' (Teslarati, 14 April 2023) <https://www.teslarati.com/tesla-interior-personalization-system-patent/> accessed 12 June 2025.

[74] Team DigitalDefynd, '10 Ways Tesla Is Using AI [Case Study]' (digitaldefynd, 2025) 6 <https://digitaldefynd.com/IQ/tesla-using-ai-case-study/> accessed 12 June 2025.

while cloud connectivity synchronises driver profiles across the different Tesla vehicles they may use[75].

- **Behavioural Nudges**: Tesla's AI delivers nudges to influence driver behaviour, such as visual alerts to keep hands on the wheel during Autopilot[76] or Sentry Mode warnings when a threat is detected[77]. These nudges guide safer driving and alert behaviour, subtly steering individual actions without restricting choice.

As a result, a consumer driving a Tesla can be considered a cyborg consumer due to the significant human-machine symbiosis enabled by AIoT features like Autopilot, Smart Summon, and personalised nudges, which augment driving capabilities and integrate drivers into a networked, data-driven ecosystem. The continuous feedback loop (driver data improving AI) and reliance on AI for critical tasks mirror the cyborg consumer characteristics of deep technological integration augmenting human capabilities.

It is worth noting that the examples of AIoT-human cyborg integration discussed here may represent only the *dawn* of the cyborg era. AIoT-enhanced wearables and vehicles can be seen as early steps towards a future where human and machine integration becomes increasingly seamless, including through the implantation of AIoT devices to compensate for impaired functions or augment existing capabilities. Emerging initiatives, such as Elon Musk's Neuralink project, aim to develop implantable brain-computer interfaces that could eventually merge human consciousness with AI[78]. While such advancements remain largely prospective, consumer law must already begin adapting to safeguard human dignity, autonomy, and privacy in the evolving age of cyborg consumerhood, regardless of the current state of technological development.

3 HYPER-NUDGING: AN ENHANCED HUMAN HELP OR AN AGGRESSIVE COMMERCIAL PRACTICE?

The new millennium is marked by the widespread adoption of surveillance technologies and the continuous generation of digital personal data, which individuals produce

[75] Blake Morgan, '3 Ways Tesla Creates A Personalized Customer Experience' (Forbes, 10 May 2021) <https://www.forbes.com/sites/blakemorgan/2021/05/10/3-ways-tesla-creates-a-personalized-customer-experience/> accessed 12 June 2025.

[76] To use the Autopilot feature, drivers must agree to keep their hands on the steering wheel throughout the journey. If the system detects that the driver has let go of the wheel, it issues a visual reminder designed to prompt compliance with the required conduct. Tesla, 'Autopilot and Full-Self Driving (Supervised)' (Tesla Support) <https://www.tesla.com/support/autopilot#:~:text=Before%20enabling%20Autopilot%2C%20the%20driver,your%20hands%20on%20the%20wheel.%22> accessed 12 June 2025.

[77] Tesla, 'Model 3 Owner's Manual', 'Sentry Mode' section <https://www.tesla.com/ownersmanual/model3/en_us/GUID-56703182-8191-4DAE-AF07-2FDC0EB64663.html> accessed 12 June 2025.

[78] *See* Andrea Lavazza *et al.*, 'Neuralink's brain-computer interfaces: medical innovations and ethical challenges' (2025) Front. Hum. Dyn. 1-7.

whenever they navigate online environments or interact with smart devices[79]. In this context, online navigators and (A)IoT users act simultaneously as data subjects and data producers[80], generating information that reflects nearly every aspect of their lived experience[81]. AI, increasingly embedded in both digital platforms and physical technologies such as wearables, increases their capacity to collect, process, and analyse data at scale. As a result, AI systems are able to detect behavioural patterns and construct detailed consumer profiles[82]. This enables the AI to function as a choice architect whenever its outputs exert a tangible influence on consumer decision-making.

This chapter examines the phenomenon of hyper-nudging – particularly, as it arises through the interplay of AI, IoT, and AIoT technologies. It explores how these technologies can shape consumer choices and assesses how consumer laws in the UK and EU can both harness their benefits and mitigate their potential risks.

First, it is necessary to introduce the concept of **hyper-nudging**. The term refers to a phenomenon at the intersection of computer and behavioural sciences, where traditional nudging is amplified by the real-time capacity of smart technologies to collect, process, and analyse data. This capability enables the dynamic personalisation of nudges tailored to the specific individual being targeted[83].

The **nudge** – as described by Thaler and Sunstein – is a form of choice architecture that seeks to steer individual choices towards particular outcomes, by incentivising, without mandating, options that the architect considers optimal for the individual[84]. Simply put, a nudge is a gentle environmental cue towards the path of efficiency that preserves the autonomy of the agent[85].

On the other hand, the hyper-nudge differs from the traditional nudge in its high degree of personalisation. Indeed, hyper-nudges combine behavioural science with the analytical power of Big Data, leveraging extensive personal data collection, behavioural profiling and user categorisation[86]. They are designed as an efficient response to the heterogeneity problem posed by conventional nudging strategies[87]. As Sunstein explains, when a targeted population is diverse and nudges are impersonal, active choices may be necessary for individuals to maximise their own self-interest. This is because a default option – serving

[79] A. Michael Froomkin, 'The Death of Privacy?' (2000) 52 Stanford Law Review 5, 1475-1476.
[80] Guido Noto La Diega, *Internet of Things and the Law. Legal Strategies for Consumer-Centric Smart Technologies* (Routledge 2023) 10.
[81] Shoshana Zuboff, *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019) 14-16.
[82] Stefano Faraoni, 'Persuasive Technology and computational manipulation: hypernudging out of mental self-determination' (2023) Frontiers in Artificial Intelligence 1.
[83] Stuart Mills, 'Finding the 'nudge' in hypernudge' (2022) Technology in Society 71, 1.
[84] Richard H. Thaler and Cass R. Sunstein, *Nudge. Improving Decision About Health, Wealth, and Happiness* (Penguin Books 2008) 6.
[85] By definition, a choice architecture tool can be deemed a nudge only if it preserves human agency. It must constitute a gentle push in a certain direction, without mandating choices or imposing heavy incentives or disincentives. Cass R. Sunstein, 'The Ethics of Nudging' (2015) Yale Journal on Regulation 32, 417.
[86] *See* (n 2).
[87] *See* (n 82) 2-3.

as a nudge – may be tailored for the average member of the addressed population and fail to suit the specific individual. As a result, active choosing, when contextualised in every aspect of human life, may be utopian and time-consuming[88].

By contrast, the personalisation of nudges has the potential to resolve this problem. In fact, hyper-nudges are nudges that succeed in encountering the individual person: the option selected by the choice architect is shaped by the peculiar cognitive and behavioural characteristics of the individual consumer. To achieve this, they involve *real-time*, *personalised*, and often *opaque* adjustments, which are algorithmic-driven and based on continuous data collection[89]. These systems can modify what information is presented, when, and how, tailoring the nudge to the individual consumer – who is often deeply known by the AI system. As a result, the consumer is guided towards certain choices, even if unaware.

Therefore, the choice architect holds great power – and with it, great responsibility – as the persuasive force of the nudge, enhanced by AI-driven personalisation, can be wielded to promote consumer well-being or to manipulate consumers for corporate profit[90]. In fact, hyper-nudges are dynamic and adaptive, generated through machine learning processes that respond to individual behavioural profiles. While these can serve valuable goals – such as promoting healthier lifestyles and financially sustainable consumption – they also present risks of manipulation[91], loss of autonomy[92], and exploitation of vulnerabilities[93]. Furthermore, the consumer's reduced ability to perceive or resist these influences complicates the legal concepts of meaningful consent and informed choice[94].

In this context, the role of the law must be to prevent consumer manipulation and impose a duty on traders to act fairly, in order to achieve the objectives of consumer protection and market efficiency, while fostering innovation in the delicate age where humans meet machines and become cyborgs.

3.1 IS HYPER-NUDGING AN AGGRESSIVE PRACTICE UNDER THE EU UCPD AND UK DMCCA?

As previously discussed, hyper-nudges have the capacity to significantly influence individual decision-making processes. Consequently, AIoT technologies may shape consumer economic behaviour by steering their actions towards particular consumption

[88] Cass R. Sunstein, 'Impersonal Default Rules vs. Active Choices vs. Personalized Default Rules: A Triptych' (2012) 3-4 unpublished manuscript <https://dash.harvard.edu/server/api/core/bitstreams/7312037c-b0e6-6bd4-e053-0100007fdf3b/content> accessed 12 June 2025.
[89] *See* (n 2).
[90] Ibid. 119.
[91] Ibid. 123-124.
[92] Ibid. 127.
[93] Isabel Richard, ''Hypernudging': a threat to moral autonomy' (2024) AI and Ethics 6.
[94] *See* (n 2) 131-132.

decisions. This sub-paragraph evaluates whether hyper-nudging strategies employed by traders can be deemed aggressive commercial practices under the EU Unfair Commercial Practices Directive (UCPD[95]) and the UK Digital Markets, Competition and Consumers Act 2024 (DMCCA).

In both the EU and UK legal frameworks, aggressive practices constitute one form of unfair commercial practice[96], alongside misleading actions[97], misleading omissions[98], and breaches of professional diligence[99]. All such practices share a common feature: they cause the average consumer to take an economic decision that – absent the practice – they would not have taken[100].

The definitions of aggressive commercial practices under the UCPD and DMCCA are closely aligned. Article 8 UCPD provides that commercial practices are considered aggressive if they (are likely to) significantly impair "the average consumer's freedom of choice or conduct" in relation to the product to which the practice refers, and thereby (are likely to) cause the consumer to take an economic decision they would not have otherwise taken. The provision identifies three forms of trader conduct that may constitute the "tools of the aggression": harassment, coercion – including physical force – and undue influence.

Similarly, Section 228(1) DMCCA refers to the same "aggressive tools" as criteria for determining whether a commercial practice is aggressive.

In the case of hyper-nudges, coercion – understood as "the use or threat of physical force[101]" – can certainly be excluded. The same applies to harassment. Indeed, if either of these were present, the persuasive strategy adopted by the trader could not be classified as a nudge, which, by definition, must – at least theoretically – respect human autonomy, reflecting the principles of libertarian paternalism[102].

This leaves *undue influence*. Under both legal frameworks, this concept involves the trader's exploitation of their position of power over the consumer, thereby pressuring them in a manner that "significantly limits the consumer's ability to make an informed decision[103]". The question, then, is the following:

- Are hyper-nudges aggressive commercial practices that employ undue influence?

To answer this question, further reflection is required. In the case of hyper-nudges, the traditional imbalance of power between traders and consumers is amplified by AI-

[95] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005.
[96] Articles 5(4)(b) and 8 UCPD; Sections 225(4)(a)(iii) and 228 DMCCA.
[97] Article 5(4)(a) and 6 UCPD; Sections 225(4)(a)(i) and 226 DMCCA.
[98] Article 5(4)(a) and 7 UCPD; Sections 225(4)(a)(ii) and 227 DMCCA.
[99] Article 5(2) UCPD; Sections 225(4)(a)(iv) and 229 DMCCA.
[100] Article 5(2)(b) UCPD; Section 225(4) DMCCA.
[101] Section 228(3)(b) DMCCA.
[102] *See* (n 84) 5.
[103] Article 2(j) UCPD; Section 228(3)(b) DMCCA.

enhanced data-analytical techniques, which can detect and exploit consumer vulnerabilities in ways that impair their ability to make informed and autonomous decisions[104].

Suppose an AIoT device can detect that a consumer is hungry[105] – through behavioural and biometric analysis – and subtly suggests, via vivid audiovisual images, that a discounted cheeseburger is available at a nearby fast-food outlet. These images might be projected through the consumer's AI-enhanced glasses or displayed on the screen of their AI-powered car or smartwatch. If the AIoT device also inferred – for instance, by analysing past food choices, purchase frequency, and the consumer's behavioural response to particular consumption patterns[106] – that cheeseburgers are among their favourite foods, and presents the offer at the precise moment of heightened vulnerability, capturing their attention and simplifying the path to purchase, can we still claim that the consumer retained meaningful autonomy or the capacity to make an informed choice in that moment[107]?

Article 9(a) UCPD and Section 228(2)(a)-(b) DMCCA provide that, in determining whether undue influence has been exercised by the trader, the *nature* and *timing* of the practice must be taken into account. In the example provided, the hyper-nudge – thanks to its high degree of personalisation – has been able to identify the precise temporal window (*timing*) in which the consumer's need arises and "gently" suggests a relevant product (the cheeseburger) at that moment. Critically, the *nature* of such a practice lies in its strategic exploitation of everything the AIoT system knows about the consumer: their temporary mental state (hunger), personal preferences (a strong liking for cheeseburgers), vulnerabilities (tendency to lose self-control when hungry), and behavioural patterns (impulsive decision-making)[108]. By drawing on this rich consumer profile, the AIoT device is able to orient the consumer's economic decision, ultimately nudging them towards a specific choice – purchasing the product – pre-planned by the choice architect (the trader).

If, in this example, the consumer ends up purchasing the cheeseburger as a direct result of being hyper-nudged – making a choice they would not otherwise have made – can we consider the hyper-nudge an aggressive practice employing undue influence? Suppose the consumer had been diligently following a diet that restricted cheese intake due to high cholesterol, as advised by their doctor, and had already consumed cheese at breakfast. In the absence of the hyper-nudge, the consumer might have stuck to their rational plan and opted for a healthier meal, such as baked fish with a fresh tomato salad. The question,

[104] *See* (n 14) 22-23.
[105] Cf. Muhammad Tausif Irshad *et al.*, 'SenseHunger: Machine Learning Approach to Hunger Detection Using Wearable Sensors' (2022) 22 Sensors 7711, 16.
[106] Jindi Song, 'The Threat of Consumer Autonomy under Personalised Recommendations' (2024) 1 Dean&Francis 5, 3 <https://www.deanfrancispress.com/index.php/hc/article/view/482> accessed 12 June 2025.
[107] Cf. (n 14) 2.
[108] Cf. Usep Suhud *et al.*, 'The drivers of addiction to online shopping, social media, and tourism: A study of cyborg consumers' (2024) International Journal of Data and Network Science 8, 1405.

then, is whether the hyper-nudge – by overriding the prior intention and exploiting a moment of vulnerability – crosses the line into undue influence under consumer protection law.

If we consider how human-decision making operates – particularly, the binary distinction proposed by Kahneman between System 1 and System 2[109] – it becomes clear that the hyper-nudge in this example targets System 1. This system governs our instinctual and unconscious decisions, relying on cognitive biases, heuristics, and emotional responses[110]. By exploiting it, the hyper-nudge bypasses the consumer's rational faculties, thereby impairing their ability to make an informed choice[111]. Such a decision, indeed, requires the engagement of the rational, deliberate, and conscious System 2, which is essential to preserving autonomy of will[112].

As a result, a behaviourally informed interpretation of the UCPD[113] and DMCCA should classify as aggressive those hyper-nudging practices that – through undue influence[114] arising from the manipulative use of AIoT-driven behavioural analysis – steer consumer economic choices in ways that:

a) Distort the decision-making process;

b) Impair rational deliberation (i.e., the functioning of System 2) and, consequently, the consumer's ability to make autonomous and informed decisions;

c) Lead consumers towards decisions that do not promote their long-term wellbeing, thereby harming them.

Indeed, if EU and UK consumer protection laws such as the UCPD and DMCCA are intended to serve as future-proof regulations, our interpretation of them must take into account both insights from behavioural science regarding human decision-making and the modern AI- and AIoT-driven commercial practices capable of profoundly shaping how we think, desire, and ultimately behave.

[109] Daniel Kahneman, Thinking Fast and Slow (Farrar, Straus and Giroux 2011).
[110] Steve Dale, 'Heuristics and biases: The science of decision-making' (2015) 32 Business Information Review 2, 94.
[111] Cf. (n 82) 3.
[112] Ibid. 9.
[113] Cf. (n 35) 908.
[114] Fabrizio Esposito and Thaís Maciel Cathoud Ferreira, 'Addictive Design as an Unfair Commercial Practice: The Case of Hyper-Engaging Dark Patterns' (2024) European Journal of Risk Regulation 15, 1011-1012.

3.2 HYPER-NUDGES AND THE VULNERABILITY OF CYBORGS: IS THE AVERAGE CONSUMER STANDARD STILL ADEQUATE?

The cyborg era – marked by the proliferation of AIoT technologies – provides fertile ground for a brand-new form of consumer vulnerability[115]. As humans continuously generate data that is collected, processed, and analysed to deliver personalised outputs, including hyper-nudges, a fundamental question arises:

- Is the consumer protection standard of the average consumer still fit for purpose?

This benchmark assumes rational choice as the norm, viewing consumers as wellbeing-maximising economic agents. Within this framework, the intrinsic imbalance of power between traders and consumers is primarily understood as informational and traditionally addressed through a duty of full disclosure on the trader's part, aimed at enabling consumers to make informed choices. However, behavioural insights have challenged the rational consumer paradigm, demonstrating that consumer decision-making is more often biased, heuristic-driven, and context-dependent – suggesting consumer rationality is the exception rather than the norm[116].

These concerns are further exacerbated by the new complexities of digital environments, which have deepened the asymmetries of power in B2C interactions[117]. When consumers engage online, they generate a continuous stream of data that exposes them to behavioural profiling[118] and hyper-personalised commercial practices. This condition has been termed *digital vulnerability*: a state of heightened exposure to data-driven digital commercial practices tailored and adapted to the personal characteristics of each targeted consumer, inferred from their online behaviour[119].

This situation becomes even more complex in the context of algorithmically-driven automated decision-making systems that personalise outputs such as recommendations, contractual terms and conditions, and nudges – a phenomenon that exacerbates the B2C relationship by placing consumers in a position of *algorithmic vulnerability*[120].

Cyborg consumers face an additional layer of vulnerability, further weakening their position and exacerbating the power imbalance between them and traders. Indeed,

[115] *See* (n 14) 7-11.
[116] Rossella Incardona and Cristina Poncibò, 'The average consumer, the unfair commercial practices directive, and the cognitive revolution' (2007) J Consum Policy 30, 29-33.
[117] Dominik Lubasz *et al.*, 'Protected by Design. The Case of Personalised Advertising' in Larry A. DiMatteo *et al.* (eds), *The Cambridge Handbook of AI and Consumer Law* (Cambridge University Press 2024) 148.
[118] Niklas Eder, 'Privacy, Non-Discrimination and Equal Treatment: Developing a Fundamental Rights Response to Behavioural Profiling' in Martin Ebers and Marta Cantero Gamito (eds), *Algorithmic Governance and Governance of Algorithms. Legal and Ethical Challenges* (Springer 2021) 26-27.
[119] Natali Helberger *et al.*, 'EU Consumer Protection 2.0. Stuctural asymmetries in digital consumer markets' (2021) BEUC 25.
[120] Teresa Rodríguez de las Heras Ballell, 'Digital Vulnerability and the Formulation of Harmonised Rules for Algorithmic Contracts: A Two-Sided Interplay' in Camilla Crea and Alberto De Franceschi (eds), *The New Shapes of Digital Vulnerability in European Private Law* (Nomos 2024) 259-291.

cyborgs are not only monitored during their online interactions and exposed to AI-driven outputs in various forms; they are also "followed" and "observed" by the AIoT devices they wear or are integrated with. Consequently, these smart Things can monitor behavioural patterns, bodily functions, and emotional states, allowing them to infer how the cyborg decides, what triggers their actions, and how they emotionally respond[121]. The level of personalisation enabled by AIoT technologies is unprecedented, as are the associated risks to autonomy of will, privacy, and cognitive exploitation. This gives rise to what can be termed **cyborg vulnerability**: the specific condition of vulnerability experienced by the human who merges with the machine, whether by wearing it or being physically integrated with it[122].

In this context, hyper-nudges represent highly personalised marketing strategies shaped by consumer profiles that are dynamically and continuously adjusted and updated through the AIoT's ongoing processes of data collection and behavioural analysis, which monitor the cyborg's responses to the hyper-nudge and refine the strategies accordingly[123]. As a result, AIoT systems not only adapt their outputs to changes in the behaviour, preferences, and desires of the individual consumer, but are also capable of creating new needs and altering existing preferences and behavioural patterns[124].

Consequently, the average consumer standard appears inadequate to ensure a high level of consumer protection, especially in the cyborg era. This paradigm assumes autonomous, informed, and rational choice as the norm. However, in digital environments and, even more so, in the cyborg world, consumers risk being placed in a position of powerlessness in the face of sophisticated, data-driven, AIoT-powered hyper-nudges[125].

A potential solution to these issues could involve shifting the normative standard from the average consumer to the vulnerable consumer. This shift would move away from the current binary approach – adopted by both the UCPD and DMCCA – that distinguishes between these two paradigms. Instead, it would embrace a monistic approach, positioning the vulnerable consumer as the sole consumer paradigm. This normative strategy would highlight, as Fineman explains, that the vulnerable condition is universal and ontological, a shared trait that unites all humans[126]. However, in the age of highly personalised digital and cyborg practices, considering vulnerability as a singular, uniform condition may not suffice[127].

[121] Cf. (n 82) 2.
[122] Gill Haddow, *Embodiment and Everyday Cyborgs* (Manchester University Press 2021) 105.
[123] Cf. (n 2) 122.
[124] Cf. Aron Darmody and Detlev Zwick, 'Manipulate to empower: Hyper-relevance and the contradictions of marketing in the age of surveillance capitalism' (2020) Big Data & Society 7.
[125] Cf. Thomas J. Rickert, 'Ambient Engineering: Hyper-Nudging, Hyper-Relevance, and Rhetorics of Nearness and Farness in a Post-AI Algorithmic World' (2024) 54 Rhetoric Society Quarterly 5, 424.
[126] Martha Albertson Fineman, 'The Vulnerable Subject: Anchoring Equality in the Human Condition' (2008) 20 Yale Journal of Law and Feminism 1, 8-9.
[127] Cf. (n 14) 13-16. Amit Zac *et al.*, 'Dark patterns and consumer vulnerability' (2025) Behavioural Public Policy 5-7.

AIoT technologies, indeed, make one thing unmistakably clear. On the one hand, it is undeniably true that we all share a common starting point of vulnerability, whether engaging online or merging with machines. In both contexts, we are continuously monitored by the various, interconnected "Big Brothers" represented by the AIoT companies that track our every move. We are universally exposed to dark patterns, exploitative hyper-nudges, and other manipulative techniques that leverage real-time surveillance and AI's capability to efficiently gather and process data. This constitutes the shared ground on which all consumers, without distinctions, are subject to behaviourally informed marketing strategies with a high degree of personalisation[128].

On the other hand – and this is where our common ground begins to diverge – each of us is characterised by unique psychological, cognitive, physical, educational, cultural, and behavioural traits that make us more or less susceptible to manipulative strategies and aware of them[129]. In sum, exposure to personalised strategies is what we all share, while our individual characteristics are what set us apart and shape how we experience and ultimately respond to them[130].

Given this, while the current classical binary distinction between the average consumer – as the rational standard – and the vulnerable consumer – as the exception justified by factors such as age, credulity, mental and physical conditions[131], or the circumstances they are in[132] – appears insufficient to adequately address the real-world imbalances of power between traders and consumers, a complete shift to a monistic approach may not be the optimal solution either[133].

Instead, a more effective strategy for ensuring a high level of consumer protection may be to retain the binary model, explicitly enriched with insights from behavioural science. The standard consumer benchmark should be reconceptualised, grounded in our shared baseline of vulnerability, to reflect how consumers actually think and behave[134]. At the same time, the notion of the vulnerable consumer – as the binary model's exception – should be expanded to encompass those individuals whose particular characteristics render them even more susceptible to manipulative practices. A dual-layered legal framework structured in this way would aim to ensure that consumer protection remains responsive, nuanced, and genuinely effective in light of both common and individual vulnerabilities.

[128] Natali Helberger *et al.*, 'Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability' (2022) Journal of Consumer Policy 45, 175-176.
[129] Ibid. 180.
[130] Ibid. 182.
[131] Article 5(3) and Recital 19 UCPD; Section 247(4)(a)-(c) DMCCA.
[132] Section 247(4)(d) DMCCA.
[133] Federico Galli, 'Online Behavioural Advertising and Unfair Manipulation Between the GDPR and UCPD' in Martin Ebers and Marta Cantero Gamito (eds), *Algorithmic Governance and Governance of Algorithms. Legal and Ethical Challenges* (Springer 2021) 126-128.
[134] Bram B. Duivenvoorde, *The Consumer Benchmarks in the Unfair Commercial Practices Directive* (Springer 2015) 159-174.

3.3 HYPER-NUDGING AS AN OPPORTUNITY FOR CONSUMERS

In the previous subparagraphs, hyper-nudging has been examined primarily as a commercial practice that poses significant risks to consumer well-being. While the risks associated with the exploitative use of AIoT technologies should not be underestimated, they can also offer a wide range of benefits, such as tailored recommendations, harm prevention, and highly personalised user experiences. In essence, the knowledge that AIoT devices acquire about us can be used not only against us but also in our favour[135]. As with most technologies throughout history, it is the intended purpose that determines whether they serve as tools for good.

In the case of hyper-nudges, these can be designed to guide the consumer towards choices that are beneficial for their long-term well-being[136]. Returning to the earlier example of a cyborg consumer wearing an AIoT device that detects hunger and nudges them towards purchasing a cheeseburger, the nudge's value depends on its content, purpose, and effects. We supposed that the consumer has high cholesterol, has already eaten cheese at breakfast, and, according to medical advice, should limit their cheese intake. We also assumed that, without the hyper-nudge, the cyborg consumer would have followed their planned meal – baked fish and a tomato salad – aligned with their dietary needs. In this case, the nudge is detrimental, as it undermines the consumer's health goals and overall well-being.

By contrast, imagine a different scenario in which, instead, the hyper-nudge actually guides the consumer towards their optimal choice. The consumer is still very hungry and genuinely committed to following their diet. They have already bought all the ingredients to prepare the scheduled healthy meal. However, after completing a one-hour run, the cyborg passes a billboard showing a happy person eating a cheeseburger – coincidentally, their favourite food. This combination of hunger, visual triggers, and the proximity of their preferred fast-food outlet – as signalled on the billboard – clouds their judgement[137]. A consumer-centric hyper-nudge could infer these signals and gently remind the cyborg that a healthy meal awaits at home. It could also highlight the progress they have made – such as having succeeded in following their diet for two weeks – and emphasise the long-term benefits of continuing these efforts.

In this scenario, the hyper-nudge does not serve corporate profits by stimulating compulsive consumption but instead identifies the most beneficial option for the consumer's well-being and gently guides their thoughts and actions towards it. Crucially, the cyborg consumer remains free to adhere to or reject the AIoT's recommendation, in

[135] Fengjiao Zhang *et al.*, 'AIoT-enabled smart surveillance for personal data digitalization: Contextual personalization-privacy paradox in smart home' (2023) Information & Management 60, 1-2.
[136] *See* (n 82) 7. Stuart Mills, 'Into Hyperspace: An Analysis of Hypernudges and Personalised Behavioural Science' (2019) SSRN 10 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3420211> accessed 12 June 2025.
[137] Cf. George Loewenstein, 'Out of Control: Visceral Influences on Behavior' (1996) 65 Organizational Behavior and Human Decision Processes 3, 272.

line with the libertarian-paternalist principle of preserving freedom of choice – including choosing differently from the architect's suggested path.

Other examples of consumer-centric hyper-nudges that support the long-term well-being of the cyborg consumer could include the following:

- The cyborg consumer is approaching their destination while being driven by an AIoT-powered autonomous vehicle. The smart car could suggest: "It's a beautiful morning and the air quality is excellent. Your destination is just a 15-minute walk away. Walking today could save ~300g of CO_2 and help you meet your weekly step goal. Want directions for the walk?"

- It is late at night, and the consumer has been doomscrolling on a social media app for 45 minutes. Their facial expression, detected through the device's front-facing camera, indicates fatigue, and their sleep tracking shows poor sleep patterns over the past three nights. Their AIoT glasses might intervene with a prompt: "It's past your usual bedtime, and your brain needs rest to stay sharp. Want to switch to *Wind Down Mode* and continue in the morning?"

- It is payday. The cyborg consumer tends to overspend during the following weekend, often missing their monthly savings goal[138]. Their mood is low, increasing the risk of emotional spending[139]. In this context, the AIoT smartwatch could provide a timely and personalised nudge: "You've saved €250 this month – just €50 short of your monthly target! Great progress. How about transferring €50 now to lock it in before weekend expenses start piling up?"

In each of these scenarios, the hyper-nudges prioritise the consumer's well-being over corporate profits. Rather than encouraging fuel consumption, excessive digital engagement, or impulsive spending, the AIoT-powered nudges aim to promote environmentally responsible behaviour, healthier routines, and financial discipline. They illustrate how hyper-nudging, when aligned with consumer-centric objectives, can serve as a valuable tool for enhancing individual autonomy and long-term welfare.

[138] Cf. Kenneth Partridge, 'On Payday, Consumers Feel a License to Spend' (Columbia Business School, 4 March 2016) <https://business.columbia.edu/cgi-economics-policy/chazen-global-insights/payday-consumers-feel-license-spend> accessed 12 June 2025.
[139] Grant Donnelly *et al.*, 'Sadness, identity, and plastic in over-shopping: The interplay of materialism, poor credit management, and emotional buying motives in predicting compulsive buying' (2013) Journal of Economic Psychology 39, 115.

3.4 HYPER-NUDGES AND MARKET EFFICIENCY IN A CYBORG SOCIETY

While consumer-centric hyper-nudges are primarily intended to promote a high level of consumer protection, in doing so they can also advance the goal of market efficiency. In fact, a well-functioning market depends on healthy economic agents – consumers who act in a balanced, rational, and thoughtful manner. Behavioural science has shown that mental health struggles, bad moods, or elevated stress levels often lead to suboptimal economic decisions[140]. Therefore, by guiding cyborg consumers towards decisions aligned with their long-term well-being, hyper-nudges not only improve individual lives but also contribute to a robust, resilient market, and a more satisfied society.

Moreover, although hyper-nudges present significant risks of exacerbating existing manipulative commercial practices, they also hold the potential to act as a countermeasure to such concerns. When a cyborg consumer is on the verge of making an economic decision, AIoT devices – drawing on real-time data through their sensors – could promptly detect the presence of dark patterns, addictive designs, or other manipulative strategies aimed at boosting corporate profits at the expense of consumer well-being[141]. In response, the AI-powered smart Thing could suggest more suitable alternatives, if any, tailored to the consumer's actual needs, while also explaining why certain seemingly attractive options may, in fact, be misaligned with their long-term interests[142].

A well-designed hyper-nudge could leverage its high degree of personalisation to deliver outputs that optimise the cyborg consumer's economic behaviour. By doing so, AIoT technologies can empower individuals to make more informed and rational decisions by:

a) Addressing information asymmetry – highlighting the most relevant information needed for an aware decision[143];

b) Mitigating cognitive vulnerability – using behavioural profiling to prevent emotionally driven, impulsive, and stubborn choices[144];

[140] Harsh Sadhu, 'Behavioral Economics: How Emotions Influence Financial Decisions' (2025) 7 International Journal for Multidisciplinary Research 1, 1-4. Sudha Mishra *et al.*, 'Compulsive buying behavior and its association with emotional distress, depression, and impulsivity in general population: an online survey' (2023) 28 CNS Spectrums 5, 592-593. Cf. Oliver Hämmig, 'Overindebtedness, unemployment, and poor mental health – and the role of sense of control: a population-based Swiss study' (2024) Front. Public Health 12, 5-9.

[141] For example, a non-profit is currently developing a "honest" AI that aims to counteract deceptive AI systems. *See* Dan Milmo, 'AI pioneer announces non-profit to develop 'honest' artificial intelligence' (The Guardian, 3 June 2025) <theguardian.com/technology/2025/jun/03/honest-ai-yoshua-bengio> accessed 12 June 2025.

[142] Cf. Benedict G. C. Dellaert *et al.*, 'Regulating robo-advice for consumers' financial decisions: The interplay between algorithmic quality & digital choice architecture' (2024) 10 Behavioral Science & Policy 2, 1-5.

[143] On the importance of information design – focusing on how information is delivered and highlighting the elements essential for optimal decision-making, thereby counteracting information asymmetries – *see* Joasia Luzak *et al.*, 'ABC of Online Consumer Disclosure Duties: Improving Transparency and Legal Certainty in Europe' (2023) Journal of Consumer Policy 46, 307-313. Cf. Alexander J. Wulf and Ognyan Seizov, 'How to improve consumers' understanding of online legal information: insights from a behavioral experiment' (2023) European Journal of Law and Economics 56, 559-563.

[144] Sandra C. Matz and Oded Netzer, 'Using Big Data as a window into consumers' psychology' (2017) Current Opinion in Behavioral Sciences 18, 7-11.

c) Reducing digital vulnerability – providing human-friendly explanations and interfaces[145].

As a result, AIoT technologies have the potential not only to serve as highly useful assistants that enhance consumer rationality but also to reshape the dynamics of power in modern markets. Today, manipulative commercial practices – designed to increase consumption, fabricate artificial needs, and keep consumers hyper-engaged so they produce more personal data that companies can eventually exploit – have marked an era in which corporate success often depends more on traders' ability to manipulate persuasively[146] than on offering high-quality goods and services at competitive prices[147]. When used for good, hyper-nudges can help reverse this trend, by fostering market environments where a company's ability to prosper is determined by how effectively it satisfies consumers' real needs at a competitive quality-price ratio[148].

In conclusion, the cyborg era offers an unprecedented opportunity to enhance the decision-making process of economic agents[149]. A society of AIoT-enhanced humans opens the door to a more efficient economy. Indeed, if markets are inhabited by consumers who are capable of maximising their best interests[150] and are adequately protected against manipulation[151], market dynamics can shift towards rewarding those traders who truly excel at delivering the best products and services. Enhanced consumers can, indeed, effectively compare quality and price, making rational decisions based on their real – rather than artificially induced – needs. In sum, progress demands innovation, and humanity needs that innovation to be consumer-centred. A good legal framework is one that not only fosters technological advancement but also ensures its potential is harnessed to improve people's everyday lives.

[145] Cf. Koti Tejasvi *et al.*, 'Explainable Artificial Intelligence (XAI) for Managing Customer Needs in E-Commerce: A Systematic Review' in Loveleen Gaur and Ajith Abraham (eds), *Role of Explainable Artificial Intelligence in E-Commerce* (Springer 2024) 24.
[146] Ryan Calo, 'Digital Market Manipulation' (2014) The George Washington Law Review 82, 1000-1001.
[147] *See* Aron Darmody and Detlev Zwick, 'Manipulate to empower: Hyper-relevance and the contradictions of marketing in the age of surveillance capitalism' (2020) 7 Big Data & Society 1, 1-2.
[148] Ibid. 2-10.
[149] Cf. Stephen Fox, 'Cyborgs, Robots and Society: Implications for the Future of Society from Human Enhancement with In-The-Body Technologies' (2018) 6 Technologies 2, 7.
[150] Oren Bar-Gill, 'Competition and Consumer Protection: A Behavioral Economics Account' (2011) Law & Economics Research Paper No. 11-42, 1-3 <papers.ssrn.com/sol3/papers.cfm?abstract> accessed 12 June 2025.
[151] Cf. (n 146) 1027.

4 THE INTEGRATION OF AI AND IOT: PROHIBITED OR HIGH-RISK AI PRACTICE?

Unlike the EU, which has already adopted a comprehensive legal framework for the regulation of AI — the EU AI Act[152] — the UK is still in the process of developing its own[153]. The EU AI Act adopts a risk-based approach, categorising AI systems into four levels of risk: unacceptable, high, limited, and minimal, following the methodology of "the higher the risk, the stricter the rules[154]". The UK, on the other hand, has proposed an AI Bill that, although not yet enacted, adopts a principles-based approach[155]. Despite their structural differences, both jurisdictions share a human-centric regulatory vision, aiming to promote innovation[156] while ensuring that AI technologies serve human well-being[157]. Against this backdrop, this chapter examines whether AI regulations provide effective safeguards for cyborg consumers against manipulative uses of AIoT technologies such as hyper-nudges.

When AIoT technologies are used to steer consumer decision-making through hyper-nudges, it is essential to assess the effectiveness of safeguards for cyborg autonomy and human dignity[158], particularly when such technologies are designed to serve corporate interests rather than well-being. Furthermore, a regulatory framework that aims to promote both consumer protection and market efficiency must ensure adequate safeguards while fostering ethical innovation – that is, the development of cutting-edge technologies designed to enhance people's well-being and serve the broader interests of humanity[159].

The AI Act clearly articulates this objective by stating that the regulation seeks to "promote the uptake of human centric and trustworthy[160]" AI and "support innovation[161]". The AI Bill, by contrast, does not explicitly use the term *human-centric* – in fact, the current draft does not contain the word *human* at all. Nonetheless, a similar objective can be inferred from the five principles set out in Section 2(1)(a). In particular, the

[152] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024.
[153] Nathalie Moreno, 'The Artificial Intelligence (Regulation) Bill: Closing the UK's AI Regulation Gap' (*Kennedys*, 7 March 2025) <https://kennedyslaw.com/en/thought-leadership/article/2025/the-artificial-intelligence-regulation-bill-closing-the-uks-ai-regulation-gap/> accessed 12 June 2025.
[154] Martin Ebers, 'Truly Risk-based Regulation of Artificial Intelligence. How to Implement the EU's AI Act' (2024) European Journal of Risk Regulation 1.
[155] Daniel Mair *et al.*, 'AI Watch: Global regulatory tracker – United Kingdom' (*White & Case*, 25 March 2025) <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-kingdom> accessed 12 June 2025.
[156] Recitals 1-2, 8, 20, 25, 102, 139, 176, and Articles 1, 40, 57 AI Act; Articles 1 and 3 AI Bill.
[157] While the EU AI Act directly states that the regulation is meant to foster human-centric AI (*see* Recital 1 and Article 1) that acts "as a tool that serves people, respects human dignity and personal autonomy" (Recital 27), the human-centric design of the proposed UK AI regulation can be inferred by the regulatory principles set out in Article 2, which are practically meant to ensure the design of AI mitigates its risks and amplifies its opportunities, benefiting society as a whole.
[158] *See* (n 82) 5.
[159] Cf. Mark Anthony Camilleri, 'Artificial intelligence governance: Ethical considerations and implications for social responsibility' (2024) 41 Expert Systems 7, 1-12.
[160] Recital 1.
[161] Ibid.

principle of fairness should be interpreted in a human-centric manner: AI systems ought to be designed, developed, and deployed to treat people fairly by respecting their legal rights, avoiding discrimination, and preventing unfair market outcomes[162]. Moreover, the UK regulation emphasises the importance of balancing adherence to these principles with the promotion of innovation by requiring the AI Authority – the central body responsible for monitoring and coordinating the implementation of these principles across sectors – to assess the extent to which these principles support innovation[163].

As a result, both EU and UK regulations are conceived to leave no room for manipulative practices. Where AIoT devices are deployed in ways that manipulate cyborg consumers to the detriment of their well-being, such technologies could be deemed prohibited AI practices under Article 5 AI Act. This provision explicitly bans AI's "subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques" that have the objective or the effect of "materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision", thereby steering their decision-making towards choices they would not otherwise have made[164]. Similarly, the exploitation of vulnerabilities caused by AI systems "with the objective, or the effect, of materially distorting the behaviour of that person" is also prohibited[165].

In both cases, to be prohibited the AI practice should:

a) cause significant harm, or

b) be reasonably likely to cause significant harm.

Accordingly, if an AIoT-powered hyper-nudge materially manipulates the consumer or exploits their vulnerability, and causes – or is reasonably likely to cause – a significant harm, it would pose an unacceptable risk and, thus, qualify as a prohibited AI practice under Article 5[166].

Moreover, AIoT technologies may also fall under the category of high-risk AI practices under Article 6 and Annex III AI Act, if they are used for biometric categorisation[167] and/or

[162] Department for Science, Innovation & Technology, 'Implementing the UK's AI regulatory principles: initial guidance for regulators' (*Policy paper*, 6 February 2024) 17 <https://assets.publishing.service.gov.uk/media/65c0b6bd63a23d0013c821a0/implementing_the_uk_ai_regulatory_principles_guidance_for_regulators.pdf> accessed 12 June 2025.
[163] Section 1(2)(e) AI Bill.
[164] Article 5(1)(a) AI Act.
[165] Article 5(2)(a) AI Act.
[166] Cf. Mark Leiser, 'Psychological Patterns and Article 5 of the AI Act: AI-Powered Deceptive Design in the System Architecture and the User Interface' (2024) AIRe 1, 20-22. Huixin Zhong *et al.*, 'Regulating AI: Applying Insights from Behavioural Economics and Psychology to the Application of Article 5 of the EU AI Act' (2024) The Thirty-Eighth AAAI Conference on Artificial Intelligence 20001-20007.
[167] Annex III(1)(b) AI Act.

emotion recognition[168] and "pose a significant risk of harm to the health, safety or fundamental rights" of consumers, including by "materially influencing the outcome" of their decision-making process[169]. Additionally, where an AI system performs consumer profiling, it "shall always be considered to be high-risk".

Although the UK AI Bill does not set out a direct equivalent of these provisions, the use of AIoT technologies to manipulate or exploit the vulnerabilities of the cyborg consumer would be incompatible with the proposed British regulatory framework. In particular, such practices would violate the following core principles:

- **The principles of safety, security, and robustness**[170], which demand the identification and mitigation of risks associated with AI systems, to guarantee a safe, secure, and robust deployment of these technologies and ensure that consumers can "make informed decisions about the safety of AI products and services[171]". AIoT devices that are designed, developed, and deployed with the objective or the effect of manipulating the consumer, who wears or is integrated with them, pose a significant risk of harm, which must be mitigated and neutralised to comply with this principle;

- **The principle of fairness**[172], which requires that AI must respect consumers' rights, treating them fairly and avoiding the exacerbation or creation of new vulnerabilities[173]. As a result, AIoT devices must be designed to align with a consumer-centric vision, thereby ensuring that these technologies create an environment that respects and cares about users' well-being and rights, and guarantees that cyborg consumers are adequately safeguarded against vulnerability exploitation practices;

- **The principles of appropriate transparency and explainability**[174] that call for clear and simple explanations of AI systems' outcomes and purposes[175]. Therefore, AIoT devices shall be developed to be transparent or, when intrinsically opaque, they shall integrate explainable AI (XAI) mechanisms that deliver consumer-friendly explanations of the AIoT system's functionalities and objectives. Within this framework, AI practices intended to manipulate consumers or exploit their vulnerabilities have no room, since a transparent explanation would

[168] Annex III(1)(c) AI Act.
[169] Article 6(3) AI Act.
[170] Section 2(1)(a)(i) AI Bill.
[171] *See* (n 162) 13.
[172] Section 2(1)(a)(iii) AI Bill.
[173] *See* (n 162) 17.
[174] Section 2(1)(a)(ii) AI Bill.
[175] *See* (n 162) 15.

instantaneously highlight the manipulation and/or exploitation risk, thereby protecting the consumer.

In conclusion, AIoT-enhanced hyper-nudges, by virtue of their high degree of personalisation and their unprecedented capability to steer consumer decisions, may fall under the prohibition of the AI Act or be considered non-compliant with the proposed AI Bill, depending on their design, development, deployment, and associated purposes and risks. Moreover, under EU law, they can be deemed high-risk whenever they profile the cyborg consumer. At the same time, if the AIoT device uses emotion recognition and biometric categorisation to profile the cyborg who wears or is integrated with it, it is labelled as high-risk under the AI Act, except when it does not pose a significant risk of harm to consumers' health, safety, or fundamental rights and does not materially influence the outcome of their decision-making process.

5 THE PRIVACY CHALLENGE IN THE CYBORG ERA

AIoT technologies and their capacity to intrude into every aspect of our lives – even the most intimate ones – pose significant challenges for the right to privacy. As consumers increasingly interact with, wear, and even integrate intelligent systems into their daily routines – ranging from smartwatches and AI-powered glasses to autonomous vehicles – our bodies, choices, and emotions turn into sites of data extraction, and we become "constituent parts of the infosphere"[176]. In this *cyborg era*, where human beings and machines are functionally intertwined, the classical understanding of privacy faces an existential challenge. What, then, does privacy mean in a world where the self is always tracked – even when offline – and increasingly cyborg?

Traditionally, the right to privacy – rooted in notions of dignity, personal liberty, and informational self-determination[177] – has been conceived as a sphere of autonomy in which individuals can retreat from surveillance and intrusion – a zone of control over personal information. However, AIoT technologies increasingly collapse the boundaries between public and private, online and offline, internal and external, voluntary and imposed. These technologies do not merely observe our actions; they predict, profile, and, in some cases, pre-empt them[178].

Both the EU and UK GDPR frameworks rest on the foundational assumption that individuals are capable of making informed and autonomous decisions regarding their

[176] *See* (n 80) 75.
[177] Tobias Naef, *Data Protection without Data Protectionism. The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law* (Springer 2023) 34.
[178] *See* (n 80) 202.

personal data[179]. However, in the AIoT era, this assumption often fails. Cyborg consumers, constantly connected and embedded within AI-driven systems, routinely provide consent either without full comprehension of what they are agreeing to or as a necessary trade-off to access tailored digital services, personalised experiences, or enhanced AI-powered functionalities[180]. In practice, such consent is frequently automatic, unreflective, and shaped by interface design rather than genuine understanding[181] – a phenomenon exacerbated by unfair data practices[182].

This chapter contends that the classical understanding of privacy is no longer sufficient to protect individuals – particularly cyborg consumers – from the persistent, pervasive, and intimate forms of capitalist surveillance enabled by AIoT devices[183]. Rather, a fundamental rethinking is required – one that recognises the structural and behavioural transformations brought about by the fusion of AI-powered Things and humans.

The cyborg consumer is no longer a passive subject of data collection but a living node in a constant feedback loop between human behaviour and machine learning systems[184]. In this context, where cyborgs give up on their privacy for a more personalised experience, smart devices continuously harvest physiological data (e.g., heart rate, movement, sleep cycles), behavioural patterns (e.g., purchasing choices, driving habits), and even emotional cues (via facial recognition or tone analysis) to tailor and adapt their outputs to the individual cyborg. This data is then processed in real time by opaque algorithms that inform nudging strategies, behavioural predictions, and targeted interventions[185].

Therefore, the cyborg is, on the one hand, a consumer who uses AIoT services, and, on the other hand, a worker continuously providing these technologies with the data that fuels their functioning[186].

In this context, consent – the legal linchpin of privacy protection – becomes increasingly hollow. Users may click or say "accept" on a privacy policy, but the scope, granularity, and temporal continuity of the data collected far exceed what is reasonably understood or voluntarily embraced. The illusion of control persists while behavioural data fuels profiling systems that create consumers' choice environments and, consequently, shape their decisions. Therefore, the distinction between manipulation, influence, and coercion becomes increasingly blurred[187].

---

[179] *See* Florent Thouvenin, 'Informational Self-Determination: A Convincing Rationale for Data Protection Law?' (2021) 12 JIPITEC 4, 248-250. Cf. Monica C. Jones *et al.*, 'Navigating data governance associated with real-world data for public benefit: an overview in the UK and future considerations' (2023) BMJ Open 13, 6.
[180] *See* (n 80) 202.
[181] *See* (n 14) 19.
[182] *See* (n 80) 76.
[183] Cf. Dean Curran, 'Surveillance capitalism and systemic digital risk: The imperative to collect and connect and the risks of interconnectedness' (2023) 10 Big Data & Society 1, 2-3.
[184] *See* (n 14) 11.
[185] Ibid. 2.
[186] *See* (n 80) 10.
[187] *See* (n 14) 10.

In the cyborg era, the self becomes an entity continuously updated and evaluated by predictive models. The idea of a "post-privacy" society, once theoretical, is becoming an empirical reality in the age of post-humanism[188]. While privacy as a right remains enshrined in EU and UK regulations such as the GDPR, the lived experience of many consumers reflects a different truth: constant surveillance is the default, and opting out of this system is practically impossible[189]. Within this context, traditional legal remedies focused on transparency and consent are ill-equipped to counter the structural asymmetry created by real-time, predictive AI systems embedded in the objects we wear and inhabit – ultimately demanding a rethinking of the right to privacy in the AI era[190].

Consequently, it becomes vital to ensure that, while AIoT technologies must be designed and employed following the privacy-by-design approach – to ensure compliance of the AI-powered Thing with the GDPR – another fundamental safeguard is that the technology itself must be designed to serve only the individual consumer's best interests. This would constitute a fundamental strategy to ensure AIoT technologies foster the individual consumer's well-being and the broader interest of an efficient market, promoting the flourishing of a human-friendly society.

6 THE FAIRNESS-BY-DESIGN APPROACH

On 3 October 2024, the European Commission published the *Digital Fairness Fitness Check*, which assessed whether current EU consumer protection regulations are adequate to safeguard consumers in online environments, fostering a high level of consumer protection[191]. The findings demonstrated that consumers face unprecedented challenges online, such as dark patterns[192], addictive designs[193], and personalised targeting[194], all of which aim to exploit their vulnerabilities to the detriment of their well-being[195]. Furthermore, the President of the European Commission, Ursula von der Leyen, highlighted in her Mission Letter the importance of addressing commercial practices that

[188] *See* Thomas A. Bass, 'Our Post-Privacy World' (*The American Scholar*, 1 September 2020) <https://theamericanscholar.org/our-post-privacy-world/> accessed 12 June 2025.
[189] Finn Brunton and Helen Nissenbaum, 'The Fantasy of Opting Out' (*The MIT Press Reader*, 25 September 2019) <https://thereader.mitpress.mit.edu/the-fantasy-of-opting-out/> accessed 12 June 2025.
[190] Cf. Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) Columbia Business Law Review 2, 497-499.
[191] European Commission, 'Commission evaluation shows the benefits and limitations of online consumer protection laws' (*Press Release*, 3 October 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4901> accessed 12 June 2025.
[192] European Commission, *Commission Staff Working Document Fitness Check of EU consumer law on digital fairness* (2024) 18-20.
[193] Ibid. 20-21.
[194] Ibid. 21-22.
[195] Ibid. 164-169.

– through dark patterns, addictive designs, and online profiling – exploit consumer vulnerabilities[196].

While the Fitness Check did not analyse AIoT applications or the associated opportunities and risks for cyborg consumers[197], it proposed a fairness-by-design approach that would impose on traders a duty to incorporate "consumer protection considerations at all stages of the product or service development[198]". In the context of AIoT, this implies that the design of such technologies and their practical applications must primarily foster consumers' well-being, ensuring that consumer rights, human dignity, and ethical considerations are integrated into the core of AI-powered Things and their components.

The Fitness Check states that such an approach would represent the explication of a positive duty for traders to *trade fairly* and that, even in the absence of an explicit obligation, the existence of this duty should be inferred from the existing standard of professional diligence and the general principle of good faith[199], which imposes on contractual parties a standard of conduct inspired by an ideal of loyal cooperation.

That duty – particularly in the context of B2C commercial practices – is even more pressing on traders due to the structural asymmetries of power, which are further exacerbated by the integration of AI, with its capabilities to process vast amounts of data in real time, and IoT, with its inherent tendency to function as a surveillance technology. Traders should behave in a manner that addresses this power imbalance by designing their products and services in ways that anticipate and mitigate risks to consumers, rather than exploit them.

In the AIoT ecosystem, this means embedding fairness, transparency, and accountability into the very architecture of connected devices and the algorithms that govern them. This proactive orientation reflects a shift from a reactive, enforcement-based model of consumer protection to a preventative, design-based one – where harm is addressed not *after* it occurs, but *before* it materialises.

To operationalise the fairness-by-design approach, traders must engage in an iterative and interdisciplinary process throughout the conception, development, and deployment of AIoT systems. This includes conducting *ex ante* impact assessments that account for the potential effects of the product on different categories of consumers – especially those who are more vulnerable due to age, digital literacy, or socioeconomic conditions. For instance, an AI-powered smartwatch that monitors mental health must be designed in a way that supports users' autonomy and well-being, avoids manipulation through

[196] Ursula von der Leyen, Mission Letter (Brussels, 17 September 2024) <https://commission.europa.eu/document/download/907fd6b6-0474-47d7-99da-47007ca30d02_en?filename=Mission%20letter%20-%20McGRATH.pdf> accessed 12 June 2025.
[197] Even though the Digital Fairness Fitness Check does not explicitly address AIoT technologies, it acknowledges that emerging and increasingly adopted technologies are likely to affect the relevance and adequacy of existing consumer protection laws. *See* (192) 82.
[198] Ibid. 152.
[199] Ibid. 53.

behavioural profiling, and ensures that alerts or nudges are grounded in clinically sound principles rather than mere engagement maximisation.

Moreover, fairness-by-design should guide not only the design of the consumer-facing interface but also the background architecture and business logic of AIoT systems. For example, if a voice assistant prioritises product recommendations, it must do so in a way that is not solely driven by commercial interests or opaque targeting, but rather by a consideration of the consumer's needs, preferences, and best interests. This also implies that algorithmic decision-making should be explainable: consumers should be able to understand *why* a certain suggestion was made or a specific functionality triggered[200].

In this context, fairness-by-design intersects with and reinforces the GDPR's principles of data protection by design and by default, yet it goes beyond mere data governance. It imposes an overarching normative vision: the design and deployment of AIoT technologies must respect the consumer not merely as a data subject or a user, but as a person with dignity, rights, and inherent vulnerabilities. This aligns with interpretations of consumer law as a branch not only of economic regulation, but also as a form of human-centric governance[201].

However, a fairness-by-design approach cannot be fully effective without parallel efforts to enhance consumer digital literacy[202]. As AI-driven environments become increasingly complex and opaque, consumers often lack the knowledge and skills necessary to recognise manipulative design[203], understand how their data is used, or exercise meaningful control over algorithmic decisions[204]. Therefore, legislative support for educational initiatives is essential to empower individuals to engage critically with AIoT technologies. Digital literacy should be promoted not only through formal education but also via accessible public campaigns and tools that clarify how AI systems operate, what rights consumers have, and how to assert them. By fostering a more informed consumer base, such efforts can serve as a structural complement to fairness-by-design, reinforcing resilience against exploitation and enabling active participation in the digital marketplace.

7 CONCLUSION

The rise of AI and the Internet of Things is reshaping not only consumer markets but also the very notion of consumer identity. In this new cyborg era – where technology is

[200] Serge Gijrath, 'Consumer Law as a Tool to Regulate Artificial Intelligence' in Hans-W. Micklitz *et al.* (eds), *Constitutional Challenges in the Algorithmic Society* (Cambridge University Press 2021) 293.
[201] Jie Ouyang, '"Embedded Consumer": Towards a Constitutional Reframing of the Legal Image of Consumers in EU law' (2024) Journal of Consumer Policy 47, 403-404.
[202] Antonios Kouroutakis, 'Rule of law in the AI era: addressing accountability, and the digital divide' (2024) 4 Discover Artificial Intelligence 115, 8-9.
[203] *See* Amit Zac *et al.*, 'Dark patterns and consumer vulnerability' (2025) Behavioural Public Policy, 27.
[204] Cf. Afrilia Cahyani *et al.*, 'Consumer Legal Protection Against Decoy Effects Through Digital Literacy' (2022) 5 Substantive Justice International Journal of Law 2, 195-196.

seamlessly embedded into everyday life and decision-making – traditional legal frameworks are increasingly strained. Consumers are now in constant interaction with adaptive systems that personalise, influence, and, at times, manipulate their choices. This paper has argued that, to safeguard consumer rights, dignity, privacy, and autonomy – while also ensuring market efficiency – legal systems in the UK and EU must evolve to reflect the realities of this technological transformation.

Everyday experience confirms that we are living at the dawn of the cyborg era, as human beings become even more dependent on technologies that are worn or integrated into their bodies. While this phenomenon introduces novel risks and exposes consumers to unprecedented forms of vulnerability, it also holds immense potential to enhance individual well-being and promote societal progress. Within the existing UK and EU legal frameworks, it is therefore vital to ensure that AI and consumer protection laws are not only fit for purpose but also "cyborg-proof": capable of addressing the challenges of human-machine integration while fostering ethical innovation – conceived as a means of advancing human flourishing.

The fairness-by-design approach may offer a promising pathway to achieving this balance. It responds to the urgent need for AI and consumer law to evolve in tandem, cultivating a legal environment that protects autonomy, dignity, and privacy without stifling innovation.

As the consumer becomes increasingly cyborgian, the law must rise to meet the complex, interdisciplinary demands of this new reality. Only then can we envision a future in which technological advancement and consumer dignity are not in conflict, but in harmony.