THE POWER OF THE "INTERNET OF THINGS" TO MISLEAD AND MANIPULATE CONSUMERS: A REGULATORY CHALLENGE

Kate Tokeley

THE POWER OF THE "INTERNET OF THINGS" TO MISLEAD AND MANIPULATE CONSUMERS: A REGULATORY CHALLENGE

Kate Tokeley[*]

The "Internet of Things" revolution is on its way, and with it comes an unprecedented risk of unregulated misleading marketing, and a dramatic increase in the power of personalized manipulative marketing. IoT is a term that refers to a growing network of internet-connected physical "smart" objects accumulating in our homes and cities. These include "smart" versions of traditional objects such as refrigerators, thermostats, watches, toys, light bulbs, cars, and Alexa-style digital assistants. The corporations who develop IoT are able to utilize a far greater depth of data than is possible from merely tracking our web browsing in regular online environments. They will be able to constantly collect and share real-time data from inbuilt IoT sensors and trackers such as microphones, cameras, GPS sensors, and temperature sensors. Artificial intelligence (AI) can be used to analyze this raw data in order to gain insights into consumer preferences and behavior, and deliver individualized marketing messages via our IoT devices. The persuasiveness of these marketing messages is likely to be further enhanced if future IoT household assistants are developed to have human-like mannerisms and appearances. This article explains how current laws that prohibit businesses from misleading and deceiving consumers will struggle to operate effectively in an IoT marketing landscape, where questions of who can be held liable, who should be held liable, what communication should be prohibited, and how to ensure enforcement, all become more complicated. It argues that current legal frameworks will need to be re-formulated in order to maintain the ability to prevent deceptive and misleading communication. It also tackles the wider question of whether legal frameworks should be re-formulated so as to add in protections against excessively manipulative marketing. The article points to several potential ways to achieve such re-formulations. Redesigning legal regimes to effectively protect consumers in a new IoT marketing landscape will no doubt be a challenge. The starting point is to confront the fact that there are genuinely difficult problems for which existing regulatory toolkits are ill-equipped to handle.

INTRODUCTION

In a not-so-far-off future, many of the objects that we interact with on a day-to-day basis will have internet-connected functionality and communicate with each other.[1] Your smart fridge might tell you when you are low on butter and suggest a brand that it can order for you and have delivered to your door.[2] It might one day ask you if you would like it to take care of all your grocery shopping based on its knowledge of your food preferences, health goals and the state of your fridge.[3] Your smart mirror might advise you on what style of jeans will flatter your figure, and execute the purchase of these jeans at the sound of your spoken command. On a particularly hot day, your self-driving smart car might let you know that you are about to pass an ice cream shop. Or it might have eye-tracking sensors that detect that you are getting tired and tell you the coordinates of the nearest coffee shop.[4]

Collectively, these smart objects are known as "The Internet of Things" (IoT). In combination with artificial intelligence (AI) innovations, IoT is likely to open up unprecedented opportunities for businesses to collect and analyze consumer data and communicate directly with consumers.[5] The development of IoT is already well

[*] Associate Professor, Faculty of Law, Victoria University of Wellington. I wish to thank Graeme Austin, Shmuel Becher and Marcin Betkier for their insightful comments on earlier drafts.

[1] According to some predictions there will be over 30 billion connected devices on Earth by 2025. *See* Knud Lasse Lueth, *State of the IoT 2018: Number of IoT Devices Now at 7B – Market Accelerating*, IOT ANALYTICS (Aug. 8, 2018), https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/.

[2] The LG Instaview ThinQ refrigerator is a smart fridge that already has the technology to order Amazon groceries via an Alexa command. *LG LNXS30996D: InstaView ThinQ™ Refrigerator*, LG USA, https://www.lg.com/us/refrigerators/lg-LNXS30996D-door-in-door (last visited Mar. 15, 2021).

[3] Amazon already provides technology that allows compatible smart appliances to monitor supplies of consumables such as ink and detergent and then automatically place an order when they run low. This Amazon service is called the Amazon Dash Replenishment. *Amazon Dash Replenishment*, AMAZON, https://developer.amazon.com/en-US/alexa/dash-services (last visited Mar. 15, 2021).

[4] For a detailed example of the kinds of targeted advertising that passengers and drivers of smart cars might expect to receive in the future when entering a smart city, see Hidayet Aksu et al., *Advertising in the IoT Era: Vision and Challenges*, IEEE COMM. MAG. 138 (Nov. 2018).

[5] *Chips With Everything: How the World Will Change as Computers Spread Into Everyday Objects*, ECONOMIST (Sept. 12, 2019), https://www.economist.com/leaders/2019/09/12/how-the-world-will-change-as-computers-spread-into-everyday-objects; Internet of Things is distinct from "artificial intelligence," which is a combination of advanced algorithms, machine learning, and other emerging technologies that utilize raw data to achieve various outcomes. See

underway in the form of items such as wearables,[6] electric toothbrushes,[7] baby monitors,[8] thermostat systems,[9] coffee machines,[10] toys,[11] and home security systems.[12] Many homes now have voice-activated virtual assistants, such as *Google Home* and *Amazon Echo* that have internet connectivity and can be linked to other smart devices in the home.[13] Interestingly, smartphones are not generally thought of as IoT devices themselves. Yet, they play a large role in IoT ecosystems, since most IoT devices can be controlled through an app on a smartphone.[14]

POSSIBLE MINDS: TWENTY-FIVE WAYS OF LOOKING AT AI (John Brockman ed., 2019) for an exploration about what AI is and where it might be taking us.

[6] "Wearables" is a category of hands-free IoT devices that are worn close to or on the skin. They can track personal information such as steps, sleep quality, heart rate, and distance covered. See, e.g., the activity tracker, Fitbit: *Fitbit*, FITBIT, https://www.fitbit.com/ (last visited Mar. 15, 2021). See also the Apple Watch, which tracks various information and also connects to the user's iPhone to run apps, deliver notifications, send messages, and make calls. *Apple Watch*, APPLE, https://www.apple.com/watch/ (last visited Mar. 15, 2021).

[7] *See* Nicole Van Zanten, *9 Smartest Electric Toothbrushes on the Market*, IDEAING (May 12, 2019), https://ideaing.com/ideas/smartest-toothbrushes-on-the-market/. Smart toothbrushes combine a variety of sensors to track in real time how you brush your teeth. The data is synced to an app for both iOS and Android.

[8] See, e.g., the Nanit Plus Camera Smart Baby Monitor, which has a night-vision camera that hangs over a cot, using computer vision and AI deep-learning to monitor your baby's sleep. *Nanit Plus*, NANIT, https://www.nanit.com/products/nanit-plus (last visited Mar. 15, 2021).

[9] See, e.g., the Nest Learning Thermostat, which can be controlled from a smartphone and works with a multitude of other Nest products such as lightbulbs, heating, door locks, home security cameras, and dryers. *Nest Learning Thermostat*, GOOGLE STORE, https://store.google.com/us/product/nest_learning_thermostat_3rd_gen (last visited Mar. 15, 2021).

[10] *See* Mikah Sargent, *Best Smart Coffee Maker in 2021*, IMORE (Dec. 6, 2020), https://www.imore.com/best-smart-coffee-maker.

[11] *See* Marie-Helen Maras, *4 Ways "Internet of Things" Toys Endanger Children*, SCI. AM. (May 10, 2018), https://www.scientificamerican.com/article/4-ways-internet-of-things-toys-endanger-children/ ("Such toys wirelessly connect with online databases to recognize voices and images, identifying children's queries, commands and requests and responding to them.").

[12] John R. Delaney, *The Best Smart Home Security Systems for 2021*, PCMAG AUSTRALIA (Jan. 9, 2021), https://au.pcmag.com/home-security/41818/the-best-smart-home-security-systems.

[13] As this article is concerned with issues around misleading consumer information, it will focus on IoT devices intended for personal or household use, not those intended for business use. By the end of 2023, consumer spending on smart home systems is projected to rise to $157 billion. *Consumer Spending on Smart Home Systems Worldwide from 2014-2023*, STATISTA (Aug. 27, 2020), https://www.statista.com/statistics/693303/smart-home-consumer-spending-worldwide/.

[14] *See* David Nield, *The Best Smart Home Systems 2021: Top Ecosystems Explained*, AMBIENT (Dec. 23, 2021), https://www.the-ambient.com/guides/smart-home-ecosystems-152.

Looking further into the future, IoT objects may become more human-looking, express emotions, and communicate in a human-like way.[15] This subset of IoTs is commonly referred to as robots and could undoubtably be used for a range of commercial communications. The future might be populated by robots that will function as caregivers,[16] housekeepers, companions,[17] and shop assistants.[18] Robot financial advisors are already operating in the marketplace, helping consumers to make financial decisions, and so too are rudimentary robot waitresses.[19] Robots can also be in animal form–there already exists a Japanese-made cuddly seal invented to soothe and engage people with Alzheimer's.[20]

IoT devices have potential for doing much good in the world. They can increase convenience, enhance the quality of life, and even improve our health.[21] Indeed, a disease-detecting smart toilet is currently under

[15] Several research groups are already producing prototypes of unnervingly human-like robots. *See* Celine Ge, *Meet Jiajia, the Realistic 'Robot Goddess' Built by Chinese Researchers*, S. CHINA MORNING POST (Apr. 18, 2016, 2:15 PM), https://www.scmp.com/news/china/society/article/1936834/meet-jiajia-realistic-robot-goddess-built-chinese-researchers (a robot named Jiajia built at the University of Science and Technology in China.) *See also Geminoid HI-2*, HIROSHI ISHIGURO LAB., http://www.geminoid.jp/en/robots.html (last visited Mar. 15, 2021) (a robot called Geminoid designed by Hiroshi Ishiguro at Osaka University in Japan.)

[16] Health care technology has resulted in Charlie, a medical robot currently in experimentation at Bichat Hospital in France. *See* John Harris, *Robots Could Solve the Social Care Crisis - but at What Price?*, GUARDIAN (July 2, 2018, 1:00 PM), https://www.theguardian.com/commentisfree/2018/jul/02/robo-carers-human-principles-technology-care-crisis.

[17] A companion robot for children called Moxie will be available on the market from Fall 2020. *See Moxie,* EMBODIED, https://embodied.com/products/moxie-reservation (last visited Mar. 15, 2021).

[18] *See* ROBOTICS, AI AND THE FUTURE OF LAW (Marcelo Corrales et al. eds., 2018).

[19] *See* Miriam Rozen, *Why Robot Advisers Do Not Always Add Up*, FIN. TIMES (Apr. 17, 2019); *Amy Waitress*, SERVICE ROBOTS, https://www.servicerobots.com/amy-waitress/ (last visited Mar. 15, 2021). In 2018, global sales of service robots rose nearly 60% from the previous year to 16.6 million robots, according to the International Federation of Robotics. *Executive Summary World Robots 2019 Service Robots*, INT'L FED'N OF ROBOTICS, https://ifr.org/downloads/press2018/Executive_Summary_WR_Service_Robots_2019.pdf (last visited Mar. 15, 2021).

[20] *See* Andrew Griffiths, *How Paro the Robot Seal Is Being Used to Help UK Dementia Patients*, GUARDIAN (July 8, 2014, 9:01 AM), https://www.theguardian.com/society/2014/jul/08/paro-robot-seal-dementia-patients-nhs-japan.

[21] In 2018, Apple launched a new "Movement Disorder API" IoT device, which allows Apple Watches to monitor Parkinson's Disease symptoms. *ResearchKit and CareKit*, APPLE, http://www.apple.com/researchkit/ (last visited Mar. 15, 2021). It might be possible one day to wear a smart device that has the capability to detect and inform you when a blood clot is about to cause a stroke. *See* Eunjeong Park et al., *Use of Machine Learning Classifiers and Sensor Data to Detect Neurological Deficit in Stroke Patients*, 19 J. MED. INTERNET RSCH. E120 (2017).

development.[22] The toilet can sense multiple signs of illness through automated urine and stool analysis.[23] However, IoT also holds plenty of potential for consumer harm. Legal scholars examining the impact of IoT on consumers have thus far been concerned primarily with consumer harms related to privacy and data security.[24] This article throws light onto a novel, but equally important consumer harm. That is the harm caused by misleading and excessively manipulative marketing in an era of pervasive IoT.

This type of consumer harm already exists in the regular online world but will be greatly exacerbated in a world of ever-present IoT objects. IoT dramatically expands the times and places where it is possible for businesses to communicate to consumers and potentially mislead them.[25] It also allows businesses to utilize and share a far greater depth of data than is possible from merely tracking our web browsing in regular online environments. Artificial intelligence (AI) can analyse the mass of real-time data collected from IoT systems in order to understand individual consumer behaviour and deliver targeted, persuasive marketing messages.[26] The persuasion becomes more powerful if some of the IoT objects of the future begin to look more human-like, talk to us with a natural-sounding voice, display human-like mannerisms, express emotions, and mimic friendship.[27]

This article demonstrates where and why the current legal regimes that protect consumers from misinformation will struggle to operate effectively in a future of ubiquitous IoT. It also offers some suggestions for the way forward. Current laws prohibit a person from engaging in

[22] *See* Seung-min Park et al., *A Mountable Toilet System for Personalized Health Monitoring via the Analysis of Excreta*, 4 NATURE BIOMEDICAL ENG'G 624 (2020).

[23] *Id.*

[24] *See, e.g.*, Steven I. Friedland, *Drinking From the Fire Hose: How Massive Self-Surveillance From the Internet of Things Is Changing the Face of Privacy*, 119 W. VA. L. REV. 891 (2017); Kathryn McMahon, *Tell the Smart House to Mind Its Own Business: Maintaining Privacy and Security in the Era of Smart Devices*, 86 FORDHAM L. REV. 2511 (2018); Andrew Guthrie Ferguson, *The Smart Fourth Amendment*, 102 CORNELL L. REV. 547 (2017); Terrell McSweeny, *Consumer Protection in the Age of Connected Everything*, 62 N.Y. L. SCH. L. REV. 203 (2017) (discussing the challenges of privacy and data collection in an IoT environment); Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805 (2016).

[25] This future of pervasive connectivity has been described as the "third wave" of the internet. STEVE CASE, THE THIRD WAVE: AN ENTREPRENEUR'S VISION OF THE FUTURE 187 (2016). Case suggests that the first wave can be thought of as the years between 1985 and 1999 when the internet was built, and that the second wave was from 2000 to 2015 when the App economy and the mobile market flourished. The third wave is from 2016 onwards and encompasses the revolution of IoT. This period in the digital age has also been described as the fourth revolution. *See also* KLAUS SCHWAB, THE FOURTH INDUSTRIAL REVOLUTION (2016).

[26] *See* Part II(C) *infra*.

[27] For further discussion on the topic of the persuasive power of human-like IoT robots, see *infra* notes 150–153 and accompanying text.

misleading or deceptive practices in commerce, or from using false advertising.[28] In an IoT future there might not be a "person" doing the misleading (it could be a robot driven by black-box AI systems), and there might not be any obvious "advertising" (the messages might be delivered by a cuddly pet IoT dinosaur chatting to your child.) The communication might not even be "misleading" or "deceptive" so much as surreptitiously manipulative. For example, your IoT robot companion might seem like a friend; she might know how to push your emotional buttons, know your deepest desires and be able to automate your purchases by your mere utterance of assent. Currently, manipulation of this kind is not subject to any legal limits.

In an IoT future, it is going to become increasingly difficult to identify who can be held liable under current laws and who should ideally be held liable. The new ways of marketing may also lead us to question what types of communication should be prohibited and raise issues as to how to effectively enforce laws. These "who," "what," and "how" questions are relevant worldwide, and no jurisdiction has yet fully identified the span of problems, let alone begun to reframe the laws to tackle them. The questions are of relevance to the regulation of regular internet advertising on our computers and smart phones. However, it makes sense to tackle the questions through the lens of a future envisioned IoT advertising environment where the seriousness and scale of the problems is likely to be so much greater. Much of this paper deals with problems that are difficult to predict exactly and are futuristic in nature. For that reason, the call for law change is not urgent. However, recognizing the problems and beginning to think about solutions is a vital first step.

Part I of the article examines how IoT is likely to transform advertising and commercial communication. Part II gives an overview of the current legal approach to protecting consumers from being misled, deceived and manipulated. Parts III to V of the article examine the "who," "what," and "how" questions that arise when contemplating the challenges of regulating communication to consumers in an age of IoT.

[28] Section 5 of the Federal Trade Commission Act (FTC Act) prohibits unfair or deceptive acts or practices in or affecting commerce. 15 U.S.C. § 45. The FTC interprets the phrase "unfair or deceptive acts" in section 5 as including representations, omissions, or practices that are likely to mislead the consumer. *See FTC Policy Statement on Deception*, FED. TRADE COMM'N (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf. Most states have adopted versions of the Uniform Deceptive Trade Practices Act (UDTPA), which prohibits deceptive trade practices and false advertising. For example, in California, the law provides that the crime of false advertising occurs when "a person or company makes false or misleading statements to consumers about the nature of a product or service." *See* CAL. BUS. & PROF. CODE § 17500 (1999). Similarly, in Texas, the legislation provides that "false, misleading, or deceptive acts or practices in the conduct of any trade or commerce" are unlawful. TEX. BUS. & COM. CODE ANN., § 17.46(a) (West 2019).

They also offers some tentative ideas for reformulating legal regimes to more readily meet these challenges.

I. HOW IOT WILL TRANSFORM ADVERTISING AND COMMERCIAL COMMUNICATION

A. Sheer Volume and Scope for Engagement

The most obvious way that IoT will transform commercial communication is that the number of IoT devices that surround us in our daily lives will become so vast and interconnected that businesses will be able to engage with us around the clock.[29] No longer will the advertising be limited to the arena of our screen lives. The current dominant method of online advertising relies on capturing our attention at those times when we visually access our screens (a phone, a laptop or a computer.) Admittedly, the portion of our lives that is devoted to screens is becoming frighteningly large.[30] Nevertheless, there remain plausible options in our day for disconnecting. In the future, the very notion of an offline world may seem increasingly meaningless. As the former Google Chairman, Eric Schmidt, put it when asked about the future of the internet:

> I will answer very simply that the internet will disappear . . . There will be so many IP addresses … so many devices, sensors, things that you are wearing, things that you are interacting with that you won't even sense it. It will be part of your presence all the time. Imagine you walk into a room, and the room is dynamic.[31]

When the internet floats above and out of our screens and seeps into many of the human-made things we constantly interact with, then it is going to be difficult to escape connection. All this connectivity is accompanied by more opportunities for businesses to engage with us, learn about us, and advertise to us.[32]

[29] Some scholars predict that there will be over 30 billion connected devices by 2025. *See* Lueth, *supra* note 1.

[30] *The Nielsen Total Audience Report: Q1 2018*, NIELSEN (July 31, 2018), https://www.nielsen.com/us/en/insights/report/2018/q1-2018-total-audience-report (finding that Americans spend over eleven hours a day interacting with their screens.) *See also* Nicole Fisher, *How Much Time Americans Spend in Front of Screens Will Terrify You*, FORBES (Jan. 24, 2019, 2:24 AM), https://www.forbes.com/sites/nicolefisher/2019/01/24/how-much-time-americans-spend-in-front-of-screens-will-terrify-you/#6be4381c1c67.

[31] Dave Smith, *Google Chairman: 'The Internet Will Disappear'*, BUS. INSIDER AUSTL. (Jan. 27, 2015, 8:45 AM), https://www.businessinsider.com.au/google-chief-eric-schmidt-the-internet-will-disappear-2015-1.

[32] *See generally* Otto Petrovic, *3.3 The Internet of Things as Disruptive Innovation for the Advertising Ecosystem*, *in* COMMERCIAL COMMUNICATION IN THE DIGITAL

B. Communications Beyond the Keyboard

The traditional way that consumers and businesses interact over the internet is by way of a keyboard and a screen. The advertisements are often in the form of pictures and typed words. If adverts, such as the ones on YouTube, have an audio element they can usually be skipped over in a couple of seconds or muted by default. Consumers generally conduct their online shopping by using the keyboard.[33]

In the expanding world of IoT, consumers will bypass the keyboard and rely on their voice to activate the device.[34] Eventually the keyboard may seem antiquated and clunky. Many of our future IoT devices will also be able to communicate back to us via a computer-generated human-sounding voice.[35] Devices such as *Google Home* and *Amazon Echo* already communicate in this way. Being able to listen and talk to all future IoT incarnations–some of which might eventually be robots that look human-like–will revolutionize how businesses communicate with consumers. Professor Stuart Russell, a leading AI researcher, predicts a future in which each person will have their own unique personal assistant that can listen to them and talk to them.[36] Indeed, human-like IoT robots could one day connect with us in ways that might even be described as friendship.[37]

AGE 183 (Gabriele Siegert et al. eds., 2017). *See also The Internet of Things Will Bring the Internet's Business Model into the Rest of the World*, ECONOMIST (Sept. 12, 2019), https://www.economist.com/technology-quarterly/2019/09/12/the-internet-of-things-will-bring-the-internets-business-model-into-the-rest-of-the-world.

[33] The dominant trading platform is Amazon.com. Close to two-thirds of Americans say they have purchased something on Amazon, according to an NPR/Marist poll conducted in April through May 2018. *See* Alina Selyukh, *What Americans Told Us About Online Shopping Says A Lot About Amazon*, NPR (June 6, 2018), https://www.npr.org/2018/06/06/615137239/what-americans-told-us-about-online-shopping-says-a-lot-about-amazon.

[34] A recent report by Juniper research suggests that the number of voice assistant devices in use will overtake the world population by 2024, reaching 8.4 billion. *Number of Voice Assistant Devices in Use to Overtake World Population by 2024, Reaching 8.4BN, Led by Smartphones*, JUNIPER RSCH. (Apr. 28, 2020), https://www.juniperresearch.com/press/press-releases/number-of-voice-assistant-devices-in-use.

[35] *Id.*

[36] STUART J. RUSSELL, HUMAN COMPATIBLE: ARTIFICIAL INTELLIGENCE AND THE PROBLEM OF CONTROL 67–74 (2019).

[37] *See* John Danaher, *The Philosophical Case for Robot Friendship*, 3 J. POSTHUMAN STUD. 5 (2019) (arguing that future robots will plausibly be able to be viewed as our friends.). *See also* Claus Emmeche, *Robot Friendship: Can a Robot Be a Friend?*, 3 INT'L J. SIGNS & SEMIOTIC SYS. 26 (2014). A commercial for the robot companion "Moxie" shows a lonely young boy finding what appears to be friendship with his robot companion. Urdesign, *Embodied Moxie*, YouTube (Apr. 29, 2020), https://www.youtube.com/watch?v=7YRNjclHTHg.

We don't need to go as far as the human-like robot to understand the impacts of moving away from keyboard communication. All voice-driven communication, whether via a human-like robot or a more mundane IoT device, has the advantage of both persuasive powers and the ability to make buying products a frictionless experience. The mere words "yes please" could trigger a purchase, with the payment and delivery instructions all taken care of automatically. Friction in the purchasing process might be inconvenient, but it does have the advantage of giving consumers a moment to reflect.

In order to appreciate the power of voice-driven communication, take a moment to visualize a pillow that delivers targeted advertising in your first waking moments of the day. There are already smart pillows on the market: such pillows play restful music, measure whether you are snoring, vibrate to make you roll over, and provide daily updates on your sleep quality.[38] Imagine a future in which your Dream Pillow gently whispers to you in the morning, via a tiny speaker in your ear. Perhaps first up your pillow delivers your favorite meditation or recites morning affirmations recommended especially for you. Then it gently points out that your sleep statistics have been extremely poor this week and you would perform better with more sleep. The voice goes on to tell you how you will sleep far better if you indulge in some expensive lavender oil, take calming magnesium tablets, use a snorer's nose clip on your partner, or invest in the premium version of the smart pillow (which will deliver scientifically proven sleep-inducing dream music). Suppose that all you have to do to dramatically improve your life is to say, "YES Dream Pillow, place my order." There might even come a time when we give our IoTs general consent to place automatic orders on our behalf within parameters that we choose in advance, such as for the purpose of improving our health up to a certain price limit. Concerns about the potential for marketing manipulation via voice-activated IoTs that have human-like characteristics are discussed further in Parts IV(C) and IV(D).

C. AI Machine Learning Used to Frame Advertising Through IoT Devices

Traditionally, internet advertising uses AI to analyse people's web browsing habits in order to optimize advertising so as to improve sales outcomes.[39] IoT advertising will be able to utilize a far greater depth of data than just our web browsing. It will be able to use all of the data

[38] *Smart Pillow - Track Sleep, Stream Audio, Smart Home Connected for Home Automation (ZEEQ Smart Pillow)*, AMAZON, https://www.amazon.com/ZEEQ-Smart-Pillow-Connected-Automation/dp/B06XG7G5SC (last visited Mar. 15, 2021).

[39] *See* David Z. Morris, *How Marketers Are Increasingly Using A.I. to Persuade You to Buy*, FORTUNE (Jan. 31, 2020, 6:30 AM), https://fortune.com/2020/01/31/ai-marketing-persuade/.

collected by the various inbuilt sensors on our IoTs including microphones, cameras, GPS sensors and temperature sensors. The data becomes richer, deeper and more integrated as all the IoT devices we interact with talk to each other and share data. All this raw data can then be analysed by AI to not only improve the functionality of the IoT devices but could also be used to deliver targeted marketing messages via the IoT device directly into our everyday lives.[40] In the eyes of those excited about the opportunities for advertising in the age of IoT, this is seen as a huge advantage.[41]

The more data that AI collects, the better it can understand our individual personalities and manipulate our behavior.[42] Technology companies already have enormous power to use current consumer data in ways that help to both serve our preferences and manipulate our preferences. The data available from IoT devices of the future will expand this power. One day, we might have IoT devices not only in our homes, cars, and cities but also inside our bodies.[43] AI will be able to analyze all the data streaming from the sensors on IoT devices both inside and outside our bodies and use AI-learning to recognize our desires and needs before we are even explicitly aware of them.[44]

[40] Your IoT thermostat can gather data about your movements, your home, and the weather, so that it can automatically adjust the temperature settings of your home to match your preferences. *See supra* note 9. Data analyzed by AI can also be used to improve advertising. *See* Thomas Davenport et al., *How Artificial Intelligence Will Change the Future of Marketing*, 48 J. ACAD. MKTG. SCI. 24 (2020); Hairong Li, *Special Section Introduction: Artificial Intelligence and Advertising*, 48 J. ADVERT. 333 (2019); Sonia K. Katyal, *Artificial Intelligence, Advertising, and Disinformation*, 20 ADVERT. & SOC'Y Q. (2019).

[41] *See* Aksu et al., *supra* note 4, at 143 ("IoT advertising would go further [than online advertising] by tracking user behaviour based on day-to-day activities. Here, dataveillance becomes more valuable considering that IoT user data is much more diverse if compared with regular web browsing data.").

[42] *See* Wu Youyou et al., *Computer-based Personality Judgments Are More Accurate than Those Made by Humans*, 112 PROC. NAT'L ACAD. SCI. U.S. 1036 (2015) (study shows that "computers' judgments of people's personalities based on their digital footprints are more accurate and valid than judgments made by their close others or acquaintances[.]").

[43] In 2017, the first pill containing a digital tracking system was approved by the U.S. Food and Drug Administration. It is used to monitor medicine ingestion in patients suffering from mental disorders. *See FDA Approves Pill with Sensor that Digitally Tracks if Patients Have Ingested Their Medication*, U.S. FOOD & DRUG ADMIN. (Nov. 13, 2017), https://www.fda.gov/news-events/press-announcements/fda-approves-pill-sensor-digitally-tracks-if-patients-have-ingested-their-medication.

[44] *See generally* Yuval Noah Harari, *Liberty - Big Data is Watching You*, *in* 21 LESSONS FOR THE 21ST CENTURY 34, 46 (Jonathan Cape 2018) (discussing the idea that big data algorithms, along with biometric sensors, will come to know us so well that they will be able to assert precision-guided manipulation. In Harari's words, technology will gain the technological ability to "hack and manipulate the human heart."). *See also* Michal S. Gal & Niva Elkin-Koren, *Algorithmic Consumers*, 30 HARV. J. L. & TECH. 309, 311 (2017) (examining the next generation of e-commerce which will be increasingly facilitated by digital agents using a succession of algorithms) ("Will it still make sense,

The use of AI to precisely *target* commercial communications delivered through IoT devices is probably inevitable.[45] What is as yet unknown is the extent to which AI might also play a role in the creation of the *content* of that targeted communication. In other words, is it possible that AI will one day be able to create the ads itself rather than simply choose where to place the human-designed ads or tell advertisers which human-designed ad will be most effective?

There are already early indications that AI holds much promise in this arena.[46] For example, Microsoft Corporation is currently working on its own conversational AI which they claim will open "an amazing new channel for companies to interact with their customers."[47] The digital marketing company Persado Inc. has begun to experiment with using AI to not only target the ad but to create the ad itself. In 2019, Persado teamed up with the financial services company JP Morgan Chase & Co. to test the potential for AI ad-creation. It found that ads written by the AI platform got far more clicks than ads written by humans.[48] Persado describes its ad-writing AI as having the power to "engage consumers like never before, one by one, moment by moment, across every marketing channel, driving improvements in brand engagement and revenue performance."[49] The use of AI in writing commercial communications is

for example, to speak about consumer choice when preferences are defined, predicted, and shaped by algorithms?").

[45] AI is already used extensively to target online advertisements. *See* Davenport et al., *supra* note 40; Li, *supra* note 40. One way AI improves advertising is by experiment using A/B ad testing to determine which form of ad leads to the best sales outcomes. A/B Testing is where a small change in an ad is tested against a current ad to determine which one gives the best result. A is the control ad and B is the variation ad. Both ads are run simultaneously for a certain time. The process can be repeated by testing the winning ad against a new variation.

[46] *See* David Cox, *The Beginnings of Advertising Created by Artificial Intelligence*, GUARDIAN (June 8, 2015, 6:56 AM), https://www.theguardian.com/media-network/2015/jun/08/artificial-intelligence-ai-created-adverts-computers; Rhoda Sell, *The Future of Advertising: Artificial Intelligence & Creativity*, BECOMING HUMAN (June 25, 2018), https://becominghuman.ai/the-future-of-advertising-artificial-intelligence-creativity-522e969d194b.

[47] *Responsible Conversational AI*, MICROSOFT, https://www.microsoft.com/en-us/ai/ai-lab-conversational-ai (last visited Mar. 15, 2021).

[48] Nat Ives, *JPMorgan Chase Taps AI to Make Marketing Messages More Powerful*, WALL ST. J. (July 30, 2019, 6:30 AM), https://www.wsj.com/articles/jpmorgan-chase-taps-ai-to-make-marketing-messages-more-powerful-11564482606. ("In one test, a headline written by humans urged consumers to 'Access cash from the equity in your home,'" and asked consumers to "'Take a look.'" The AI came up with an alternative that stated: "'It's true–You can unlock cash from the equity in your home'" and suggested that consumers "'Click to apply.'" The AI version generated forty-seven weekly applications for home equity lines of credit, compared with twenty-five for the original version.).

[49] *Persado*, PERSADO, https://www.persado.com/gb/ (last visited Mar. 15, 2021).

likely to increase as the technology improves.[50] The combination of IoT and AI creates extraordinary opportunities for advertisers.

D. IoT Communication Might Not Seem Like Advertising or Commercial Speech

Traditional old-style advertisements, such as intrusions into television viewing or promotions in print newspapers, are easily identifiable as adverts. Online advertising is more camouflaged. It might masquerade as an Instagram post or look like an online news article. But IoT advertising might not feel anything like advertising at all. Perhaps an illustration might clarify this further. Imagine you are walking around a shopping mall. Your smart watch and your smart headphones are communicating with each other, combining data such as your predilection for diet coke, the humidity of the air, and your biometrics. At the exact moment when your data shows a level of dehydration that is likely to be impinging on your conscious awareness, your headphones might say, "Hey there Kate, you need a drink and a zap of energy. There is an ice-cold coke at a vending machine around the next corner." Another consumer might be more health-conscious and prefer orange juice. This consumer is instead prompted to increase her vitamin C and visit the juice bar. This type of communication might not feel like advertising. Indeed, it might simply feel like a good friend making helpful suggestions to improve your life.

E. Emergence of Different Business Models

In an IoT environment, it is likely that new entities and business models will emerge. Recognizing the uncertainty surrounding the types of corporate players that could evolve in the future is important for understanding subsequent discussions about how to effectively regulate IoT misinformation. Currently, when a consumer buys a regular non-smart fridge, printer, car, soft toy or electric toothbrush, the transaction is relatively straight forward and one-dimensional. The supplier sells the product and the consumer pays a price to cover manufacturing costs, plus a mark-up to enable the supplier to make a profit. The unique nature of IoT products to collect data and communicate with consumers creates new funding opportunities. This means that the physical IoT devices themselves and the services provided by the devices might end up being relatively cheap if they are "paid" for by way of consumers sacrificing data and accepting advertising messages.

The very nature of an IoT product means that the consumer will sign up for some level of data collection, without which the IoT will not function effectively. The initial sales contract is likely to include lengthy

[50] *See generally supra* note 46.

and unreadable online terms of service.[51] Consumers do not read these privacy terms, so meaningful consent is unlikely.[52] They might be "agreeing" to share data with both the supplier of the IoT and multiple third parties. Much of this data is likely to be extremely valuable.[53] There remains uncertainty about which kind of companies might be the ones to tap into the value of this data. There are various potential types of companies that might be involved - software engineering companies, AI creators, manufacturers of the physical IoT objects, advertising content creators, platform companies, advertising network companies, etc.

Since consumers will benefit from one central hub or app to control all their IoT devices, there is the potential for power to concentrate in one company that is able to coordinate the whole IoT network in our homes. It is possible that this one company might rise as the dominant player and achieve a "winner takes all" status in the same way that Google became the winner of the battle for the online search engine market.[54] Indeed, one of the current tech giants could become the dominant company in IoT world. Amazon and Google are already in the data extraction business, and each is in the initial stages of building a cluster of IoT products operated via their voice activated home

[51] For an interesting discussion of the extent to which consumer sign-in-wrap contracts are unreadable, see Uri Benoliel & Shmuel I. Becher, *The Duty to Read the Unreadable*, 60 B.C.L. REV. 2255 (2019).

[52] Many scholars have discussed this problem of unread boilerplate terms that consumers are offered on a take-it-or-leave-it basis. *See, e.g.*, Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1173 (1983); Russell B. Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. CHI. L. REV. 1203 (2003); MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2013); Yannis Bakos et al., *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1 (2014); OREN BAR-GILL, SEDUCTION BY CONTRACT: LAW, ECONOMICS, AND PSYCHOLOGY IN CONSUMER MARKETS (2012). Even with the well-intended European Union General Data Protection Regulation (GDPR), which requires consumer consent to data collection, most consumers do not give any meaningful consent in the face of unreadable privacy policies and limited time. Consumers are likely to skim past the "we've updated our privacy" notices, and rush to the "I accept" button that needs clicking before the service operates. *See, e.g.*, Kate Fazzini, *Europe's Sweeping Privacy Rule Was Supposed to Change the Internet, but so far It's Mostly Created Frustration for Users, Companies, and Regulators*, CNBC (May 5, 2019, 6:00 AM), https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-regulators.html. *See also* Benoliel & Becher, *supra* note 51 (showing that in spite of the GDPR requirements to use plain language, even post-GDPR policies are generally unreadable).

[53] *See Big Data Market Size Revenue Forecast Worldwide from 2011 to 2027*, STATISTA (Mar. 2, 2020), https://www.statista.com/statistics/254266/global-big-data-market-forecast/ (the global big data market is forecasted to grow to 103 billion dollars by 2027). *See also* Gilad Rosner & Erin Kenneally, *Privacy and the Internet of Things: Emerging Frameworks for Policy and Design*, CTR. FOR LONG-TERM CYBERSECURITY 6 (2018).

[54] For an examination of the power of this kind of digital dominance, see DIGITAL DOMINANCE: THE POWER OF GOOGLE, AMAZON, FACEBOOK, AND APPLE (Martin Moore & Damian Tambini eds., 2018).

assistants.[55] Other companies are also vying for the dominance in the IoT market. For example, Samsung has created what it calls the Family Hub Fridge.[56] The by-line for the promotion of this fridge is that it is "more than a fridge, it's the Family Hub."[57]

II. THE CURRENT LEGAL APPROACH TO PROTECTING CONSUMERS FROM BEING MISLED, DECEIVED, AND MANIPULATED

In most countries, regulators protect consumers by prohibiting misleading and deceptive representations or practices in the marketplace. In the United States, Section 5 of the Federal Trade Commission Act (FTC Act) prohibits unfair or deceptive acts or practices in or affecting commerce.[58] In addition, the Lanham Act imposes civil liability for using false or misleading representations in advertising.[59] Most States have also adopted versions of the Uniform Deceptive Trade Practices Act (UDTPA) which prohibits deceptive trade practices and false advertising.[60] Other jurisdictions have similar legislation that prohibits misleading or deceptive representations, and misleading or deceptive conduct in trade.[61]

Laws that prevent consumers from being misled or deceived have long been considered essential to ensure the efficient and fair operation of the market. The advantages of these rules are well-established under

[55] In 2019, Google joined forces with Nest, the creator of the Nest smart thermostat, with the vision of creating a smart home where all the Nest products work together and are bundled together in your Google account. Nick Statt & Dieter Bohn, *Google Nest: Why Google Finally Embraced Nest as its Smart Home Brand*, Verge (May 7, 2019, 2:49 PM), https://www.theverge.com/2019/5/7/18530609/google-nest-smart-home-brand-merging-hub-max-rebrand-io-2019. *See also Nest*, *supra* note 9.

[56] *The Family Hub™ Refrigerator*, SAMSUNG, https://www.samsung.com/nz/family-hub/ (last visited Mar. 15, 2021). This fridge can create shopping lists, integrate family member's calendars, control music, and connect with other IoT devices so users can set the lights, see who is at the front door, adjust the thermostat, or check the monitor in the baby's bedroom, all from the refrigerator.

[57] *It's More than a Fridge, It's the Family Hub™*, SAMSUNG, https://www.samsung.com/au/b2btest/family-hub-refrigerator/ (last visited Mar. 15, 2021).

[58] 15 U.S.C. § 45.

[59] The Lanham Act § 43(a), 15 U.S.C. § 1125(a)(1)(B). Consumers do not have standing under the Lanham Act; only competitors or indirect competitors who are harmed by the false advertising have standing. Lexmark Int'l, Inc. v. Static Control Components, Inc., 572 U.S. 118 (2014).

[60] *See supra* note 28, discussing the UDTPA.

[61] *See*, *e.g.*, The Consumer Protection from Unfair Trading Regulations 2008, SI 2008/1277 arts. 3, 5, 9 (UK); The Australian Consumer Law set out in chapter 2 of the *Competition and Consumer Act 2010* (Cth) § 18 (Austl.); The Fair Trading Act 1986, § 9-14 (N.Z.); Competition Act, R.S.C. 1985, c C-34, § 74.01(1)(a) (Can.). Each of the Canadian provinces also has a statute prohibiting false or misleading representations in trade that uses similarly human-centric language.

classical economic theory.[62] Under this theory, once consumers are fully and truthfully informed about products in the market place, they will make rational choices to maximise their utility.[63] As far back as 1976, the United States Supreme Court embraced the view that, while the First Amendment grants protection to advertising because a "free enterprise economy" requires "informed" consumers, states still retain the power to prohibit false or deceptive advertising.[64] While behavioral economists have more recently questioned the assumption of consumer rationality, there is no disagreement about the importance of consumers not being deceived or misled about the characteristics of a product or service.[65] As of yet, laws do not extend to prevent sellers from using advertising to manipulate consumers. So long as sellers do not deceive or mislead, there will be no illegality for persuasion or behavioral manipulation.

Most jurisdictions also have some additional specific prescriptive requirements to disclose information–e.g. financial product information, calorie disclosures, ingredient lists.[66] These prescriptive laws are designed to balance out asymmetries in information between the consumer and trader.[67] These laws are not the focus of this article because they do not cause problems in an IoT environment in the same way as do the more general rules that prohibit misleading and deceiving consumers. They do not give rise to the complex "who," "what," and "how" problems that are the focus of the rest of this article. Their prescriptive nature

[62] *See, e.g.*, Gillian K. Hadfield et al., *Information-Based Principles for Rethinking Consumer Protection Policy*, 21 J. CONSUMER POL'Y 131 (1998).

[63] *See* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 17 (Wolters Kluwer Law & Business 7th ed. 2007). *See also* Richard A. Epstein, *The Neoclassical Economics of Consumer Contracts*, 92 MINN. L. REV. 803 (2008). *See also* Martin H. Redish, *The First Amendment in the Marketplace: Commercial Speech and the Values of Free Expression*, 39 GEO. WASH. L. REV. 419, 432–33 (1971) (arguing that advertising plays an important role in keeping consumers informed about their choices in the marketplace so that they can make rational welfare-maximizing decisions about what to purchase).

[64] Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, 425 U.S. 748, 749–50, 765, 770–773 (1976).

[65] See the seminal work by Phillip Nelson, *Information and Consumer Behavior*, 78 J. POL. ECON. 311 (1970); George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q. J. ECON. 488, 489 (1970). Many consumer protection laws address the importance of consumers being well-informed. *See, e.g.*, Consumer Credit Protection Act, Pub. L. 90-321, 82 Stat. 146 (1968); Pure Food and Drug Act, Pub. L. 59–384, 34 Stat. 768 (1907).

[66] In the United States, a state may enact a law that compels advertisers to provide certain factual and uncontroversial speech without violating the advertiser's First Amendment rights, if it can be shown that the law is reasonably related to the State's interest in preventing deception of consumers. *See* Zauderer v. Office of Disciplinary Counsel, 105 U.S. 626 (1985).

[67] The debate about when the law should remedy information problems in consumer markets has been discussed in the legal literature for some years. *See, e.g.*, Alan Schwartz & Louis L. Wilde, *Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic Analysis*, 127 U. PA. L. REV. 630 (1979).

means that they clearly require certain people to take specific actions. IoT technology is unlikely to challenge their application.

The regulatory regimes that prohibit misleading and deceiving consumers are designed to operate smoothly in the world of face-to-face shopping and, to a large extent, they are also useful in controlling misinformation in the current online world.[68] On the face of it, the current laws should be sufficient for regulating IoT commercial communication. Certainly, the broad principles make sense and should theoretically apply equally to both traditional communications and all forms of digital communication.[69] One would think that a tech-neutral law based on a general principle such as "businesses should not mislead consumers" would be flexible enough to adapt to the ever-evolving ways in which businesses use technology to communicate to consumers.[70]

However, when looked at more closely, the *operation* of the broad principles might not be so straightforward in an age of pervasive IoT devices. Indeed, current legal frameworks may inadvertently shield corporations from liability. The next Parts of the article examine the questions of "who" can be held liable under current law, "who" should be liable, "what" communication should be prohibited, and "how" to ensure enforcement.

III. THE "WHO" QUESTION

This Part canvases the "who" questions that arise when contemplating liability for misinformation in an IoT environment. It first

[68] However, the online world is more difficult to regulate because, for example, it is global in nature which results in choice of law and jurisdiction issues. In addition, there are new opportunities for consumer deception caused by commercial messages stealthily masquerading as online news, online entertainment, or social media messaging.

[69] As Geraint Howells points out, as digitization changes the market, "[c]ore consumer values should be maintained. . . . Consumers have been granted rights to information and expect not to be misled, including by omissions." Geraint Howells, *Protecting Consumer Protection Values in the Fourth Industrial Revolution*, 43 J. CONSUMER POL'Y 145, 147–48 (2020). In other words, the general principles are the same regardless of the medium of the communication.

[70] *See, e.g.*, Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 MD. L. REV. 785 (2015) (arguing that robots are nothing special and that the Federal Trade Commission is the preferable agency to protect consumers from unfair and deceptive robots). The choice between rules versus standards is relevant here. Rules are specific and determinate, whereas a standard states a more general principle that requires interpretation and involves an element of discretion. For a discussion of these different legal forms, see Russell B. Korobkin, *Behavioral Analysis and Legal Form: Rules vs. Standards Revisited*, 79 OR. L. REV. 23 (2000). Note also that tech-neutral laws also have the advantage of not needing to be re-written when the technology inevitably changes. For example, United States copyright law is drafted using generalized language to allow the law the flexibility to accommodate new media without extensive legislative revision. *See* 17 U.S.C. § 101, 102. *See also* Brad A. Greenberg, *Rethinking Technology Neutrality*, 100 MINN. L. REV. 1495 (2016) (examining the problems inherent in tech neutral law, using copyright laws as an analytical lens).

considers who can be held liable under the current laws and how landing liability might be challenging in an IoT context. It then examines the wider public policy question of "who" *should* be held liable for misleading commercial communications in an IoT future.

A. The Deceptive AI

In most legal systems, the legislation that prohibits misleading or deceptive commercial communication refers to human actors and human activity. The only non-human entity that can be held liable is a company. The law does this by deeming the conduct of the human employee or director, when acting on behalf of the company, to be the conduct of the company.[71] The language of the current laws works well in scenarios where a human seller speaks misleading words directly to a consumer, or where a seller writes or approves of misleading words on labels, in adverts, or on packaging. Indeed, in simple cases of a seller approving of the communication of deceptive marketing through an IoT device, the human-centric language of the law will still work perfectly well. Both the employees engaging in the deception, and the company itself, can be held accountable for the deception. But what happens when it is an AI and not a person that is making the decisions?

If we take a look at the specific wording of consumer misinformation law, we can see that it is envisaging that there is a human, not an AI algorithm, that is doing something that misleads or deceives. For example, the language used in the laws in the United States is human-centric. It refers to a "person" who uses false or misleading representations in advertising[72] or "engages" in deceptive and unfair "acts or practices[.]"[73] Other jurisdictions around the world use similarly human-centric language.[74]

The problem with leaving the laws as they are currently written is that future IoT companies may be able to avoid liability for misinformation by claiming that the human-centric statutory language does not easily encapsulate misinformation created by an AI system without any direct input from a person or a company. The idea of a future AI that can work with this degree of independence might seem far-fetched

[71] Modern commercial laws will also allow for a company to be held liable by defining a company as a legal "person" and deeming the conduct of an individual employee or director, when acting on behalf of the company, to be the conduct of the company. The United States version of this rule is specified in 1 U.S.C. § 1, which states that in determining the meaning of any Acts of Congress, unless the context indicates otherwise, the words "person" and "whoever" include corporations, companies, associations, firms, partnerships, societies, and joint stock companies, as well as individuals.

[72] The Lanham Act § 43(a), 15 U.S.C. § 1125(a)(1)(B).

[73] *See supra* note 28, discussing the UDPTA and the Federal Trade Commission Act.

[74] *See*, *e.g.*, *supra* note 61.

and the analysis that follows unnecessary. But in an article about the regulation of an IoT future, it would be remiss to not at least consider the possibility that AI will one day be at the helm of commercial communication decisions. Indeed, some commentators have predicted that AI-powered speakers might at some point "be disconnected enough and smart enough to say that the speech they produce is *theirs,* not *ours,* with no human creator or director in sight."[75] The AI could one day, via black box algorithms, be able to make autonomous decisions about both the ideal targeting and the ideal content of ads so as to maximize sales outcomes.[76]

Obviously, the AI is created by human labor, but it sounds grammatically odd to say that a "person" or a "company" has "engaged in misleading conduct or deceptive practices" when it is the AI running the show and the IoT device is producing the speech. Statutory words such as "person," "acts," "making a statement," "making a representation," "conduct," and "practice" were written into the law at a time when there was no conception of an AI targeting or writing the content of commercial communication. This human centric language presents a problem regardless of whether the AI-created advertising occurs on our current screens or emanates from an IoT device. However, the influence and reach of AI-created ads is likely to be far greater in an IoT environment.

AI deception might occur by way of targeting errors, or content errors. Targeting errors might occur in cases where the AI-delivered information is time-sensitive. For example, information to a consumer about the best rates, the most efficient solution, or the safest or most effective product might become obsolete and therefore misleading over time. If the AI design is not calibrated to handle the complexities of these timing issues then deception is possible. AI deception in the future might also occur due to content errors. As has been pointed out, there is already a move toward more AI involvement in the creation of the content of ads.[77] The nuances of human language are likely to present a significant challenge to this area of AI development. For example, one can envisage a scenario where designers of an AI advertising system add in some kind

[75] Toni M. Massaro & Helen Norton, *Siri-ously? Free Speech Rights and Artificial Intelligence*, 110 NW. U. L. REV. 1169, 1172 (2016). Nick Bostrom has gone as far as to posit that AI may reach a point where it is capable of improving itself, resulting in a feedback loop that significantly advances its own intelligence, perhaps beyond that of its human creators. *See* NICK BOSTROM, SUPERINTELLIGENCE: PATHS, DANGERS, STRATEGIES 124–25 (2014).

[76] The term "black box" is used to describe the idea that the constantly evolving nature of complex AI systems means that even their creators cannot explain exactly how they work. *See, e.g.*, FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 34–35 (2015) (describing use of software and online data to make hiring decisions).

[77] *See supra* Part II(C) and accompanying footnotes.

of truth-telling limitation that fails to filter out literally true statements that are nevertheless misleading.[78]

The problematic human conduct here would not be an act of deception, but rather it would lie in the development and monitoring of the AI. Perhaps the data input is flawed, the programmed objectives have unintended consequences, there is insufficient testing, or unreasonably low levels of human intervention to monitor outcomes. While the human conduct might be troubling, it is not in itself easily described as misleading. The software programmers who design the AI cannot be said to have engaged in the act of misleading consumers. They are instead engaged in unwittingly creating a system which ends up misleading consumers. Unless the law is reworded, this subtle difference could allow the IoT software company to escape liability for the consequences of their actions by virtue of the fact that the deception is in some senses perpetrated by a non-human.

B. AI Legal Personhood

The law has not yet prepared for a future where AI-driven IoT devices replace humans as the producer of spoken and written information to consumers.[79] Some scholars have suggested that one solution to problems of AI liability (such as problems of liability when a self-driving car causes an accident), is to impose legal personhood on AI.[80] The theory goes that if the law has already imposed liability onto inanimate things such as companies, then it should be possible to impose

[78] Thus, for a claim of false advertising under the Lanham Act, a plaintiff may show that while the advertisement is literally true it is nevertheless likely to mislead or confuse consumers. Lanham Act § 43(a), 15 U.S.C. § 1125(a).

[79] Similar issues around algorithmic AI liability have arisen in the area of defamation law. *See*, *e.g.*, Robinson Meyer, *Did Facebook Defame Megyn Kelly? Which is a Different Way of Asking: Can a Bot Commit Libel?*, THE ATLANTIC (Aug. 30, 2016), https://www.theatlantic.com/technology/archive/2016/08/did-facebook-defame-megyn-kelly/498080/ (discussing Facebook's potential liability for a shift in the algorithm for its trending feature, which promoted a fake story that claimed Megyn Kelly endorsed Hillary Clinton for President). *See also* Bruce E. Boyden, *Aereo and the Problem of Machine Volition*, 2015 MICH. ST. L. REV. 485, 499–505 (2015) (discussing how technology muddies issues of responsibility in copyright infringement cases).

[80] *See* Robert van den Hoven van Genderen, *Do We Need New Legal Personhood in the Age of Robots and AI?*, *in* ROBOTICS, AI AND THE FUTURE OF LAW 15 (Marcelo Corrales et al. eds., 2018). There is also an EU proposal to create legal status for robots. Committee on Legal Affairs of the European Parliament, *Report with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))*, Nos. A8-0005/2017, 64 (Jan. 1, 2017). The Committee is also working generally on the issue of regulating artificial intelligence. Madiega Tambiama, *EU Guidelines on Ethics in Artificial Intelligence: Context and Implementation*, EUROPEAN PARLIAMENTARY RES. SERV. (Sept. 2019). This general idea of AI legal personhood was postulated as far back as 1992, when the problem of AI liability was purely speculative. *See* Lawrence B. Solum, *Legal Personhood for Artificial Intelligences*, 70 N.C. L. REV. 1231 (1992).

legal personhood onto AI. Indeed, the law has also granted legal personhood to inanimate objects such as the Whanganui River in New Zealand and several rivers in India.[81] An entity that is granted legal personhood is subject to legal rights and duties.[82] Imbuing the AI system with legal personhood might be seen as treating the AI as an autonomous intelligent being so that it can be made responsible for its actions like a natural person.

It is not clear that creating AI legal personhood is a workable solution in the case of AI-created consumer misinformation. For one thing, the idea that an AI is intelligent in such a way that it should be culpable seems odd without any correlating consciousness. No current AI creator is even trying to make machines conscious.[83] A further difficulty with AI legal personhood is that the concept of AI is an ever-moving target that might prove too difficult to define in enough detail for any personhood law to be workable.[84] Unlike the concept of a company, the concept of AI, while generally understood in broad terms, might not be understood well enough to form a basis for new AI personhood laws. Imposing AI legal personhood would require the law to define AI in such a precise way that it is easily understood and does not lead to endless litigation about its parameters.

The second reason that the AI personhood approach might be unsatisfactory relates to the difficulty of translating AI personhood into a system where liability falls onto humans. It is the humans that have the money that can compensate for harm caused by AI or pay fines for offending behavior. Punishing a corporation ultimately results in punishment of the human owners of the corporation. Likewise, holding a corporation liable to compensate aggrieved individuals results in the human owners of the corporation losing money. The legal fiction works because there are easily identifiable people and money behind the fiction.

A workable mechanism for AI personhood would need to both define AI and identify the relevant human owners behind the AI who

[81] *See* Te Awa Tupua (Whanganui River Claims Settlement) Act 2017, § 14 (2017) (N.Z.).

[82] For a historical overview of the concept of the corporation, *see* John Dewey, *The Historic Background of Corporate Legal Personality*, 35 YALE L. J. 655 (1926). *See also* Richard Tur, *The Person in Law*, *in* PERSONS AND PERSONALITY 116 (Grant Gillett & A. R. Peacocke eds., 1987) (providing a concise summary of the concept of the person within several areas of the law).

[83] RUSSELL, *supra* note 36, at 16.

[84] AI pioneers Stuart Russell and Peter Norvig point out the history of artificial intelligence has produced several different definitions of AI, each variously emphasizing four possible goals: "[s]ystems that think like humans, [s]ystems that act like humans, [s]ystems that think rationally, [s]ystems that act rationally." STUART J. RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH 5 (1995). The discussion about "what is AI?" takes over four pages, which indicates the potential difficulties in giving a concise definition. In his latest book, Stuart Russell undertakes an exploration of what is meant by artificial intelligence in machines by characterizing "machines as intelligent to the extent that their actions can be expected to achieve their objectives." RUSSELL, *supra* note 36, at 9.

should be responsible for the harm caused by the misleading information. In some ways the proposal to create AI legal personhood might be a distraction from the real task at hand which is for the law to be re-drafted so as to allow responsibility, or perhaps shared responsibility, to fall on the individuals or companies who are undertaking activities that ultimately lead to the misinformation. The next section explores this task.

C. Who Should be Responsible for AI-Automated Deception and Under What Theory of Liability?

Let's imagine that an IoT personal assistant robot, called Jack, tells his owner something that is misleading about a product and this causes her harm. The miscommunication is caused by automated AI decision-making and not a human act of deception. Rather than try to solve the liability issue by giving Jack, or parts of Jack, some kind of legal personhood and make him liable for the misleading conduct, a more straightforward approach might be to simply update the law so that it catches a wider range of human conduct than just misleading conduct. For example, liability could be imposed on conduct such as negligent or intentionally poor design of the AI systems (that ultimately produce deceptive speech.)

Expanding the law beyond the human-centric language of a *person* doing the misleading seems like an obvious approach to avoiding the difficulties posed by misinformation caused by AI. It gets straight to the heart of the matter, which is to hold accountable the companies and individuals behind the consumer harm. The problem of defining AI would be less acute under this legal framework than it would be under an AI personhood framework. AI could be defined broadly as any combination of advanced algorithms, machine learning, and other emerging technologies that utilize raw data to achieve a defined outcome.

If a misleading or deceptive message has emanated from an IoT, then either a person has misled the consumer, or a person has created an AI system that has misled the consumer. If a defendant wanted to argue that there was no AI involved, then that means there must be a person who is responsible. We already have laws prohibiting *people* from engaging in unfair or deceptive acts, so that is no problem.[85] Expanding the law to cover people who negligently or intentionally design an AI system that misleads consumers is less cumbersome than creating AI legal personhood. Nevertheless, there are a couple of issues to think through when re-formulating the law in this way. I will divide these into issues related to fault-based liability, issues related to strict liability, and issues related to a pre-sale approval regime.

[85] Federal Trade Commission Act § 5, 15 U.S.C. § 45.

1. Fault-based liability. – Let us first assume that the AI design liability is fault-based. One potential problem under a fault-based regime is that it might be difficult to pinpoint exactly what, or who, caused the faulty outcome of a misleading commercial communication. This could result in companies avoiding liability due to the difficulties of tracing any failures back to any one individual or company. Jack is powered by AI processes. He might be a combination of the result of the work of human labour that might span across the different companies responsible for various stages of the system initiation, analysis, and design of the AI products and systems that work within Jack. In cases where it is easy to identify the company that designed the relevant AI, difficulties might remain with using fault-based liability rules that require proof of intention or negligence.[86]

Proving intent might be challenging if the black box architecture of the AI environment makes it impossible to assess what exactly what went wrong and why.[87] AI operates by way of providing the AI system with a desired outcome. In the case of advertising, the desired outcome is improved sales. It would be easy for the designers of the AI system working within Jack to claim they never intended for the system to use the strategy of allowing Jack to produce misleading statements. They might say that they had no idea the deception would occur; they merely gave the AI system within Jack the broad and lawful objective of communicating to each individual robot owner in a way that improves sales of the advertised product.

If the rule instead required proof of negligence rather than intent, this might also be a difficult hurdle for plaintiffs. Where a black box environment makes AI decision-making impenetrable, the creator will not know what strategy the AI will choose to achieve the desired outcome. If there is no ability for the creator of the AI to foresee how the AI will choose to achieve the outcome, it is difficult to prove negligence.[88] Unless, of course it is decided that unleashing black box type AI systems into IoT devices for the purposes of advertising is in itself a negligent action. There is also the possibility that inputs can unintentionally lead to a benign program producing undesired outputs. This is what happened with Microsoft's AI Twitter chatbot, Tay, who was designed to have a

[86] *See* Jon Kleinberg et al., *Discrimination in the Age of Algorithms*, 10 J. LEGAL ANALYSIS 113, 148–51 (2018) (discussing problems of proof for plaintiffs in cases of AI discrimination versus discrimination carried out by humans).

[87] *See generally* Yavar Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, 31 HARV. J. L. & TECH. 889 (2018). Bathaee discusses the problems of proving fault and causation in cases where AI is making decisions. *See also* Matthew U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, 29 HARV. J. L. & TECH. 353, 362–69 (2016).

[88] *See* Scherer, *supra* note 87, at 363–66 (explaining the problem of AI systems and foreseeability).

teenage millennial persona and use slang. However, soon after it was launched it began posting offensive and racist tweets.[89]

It might be more workable to impose liability for negligent failure to *monitor* the outcomes of an AI system, rather than negligent *design* of the AI system. Under this approach, liability would fall on AI creators who fail to exercise reasonable care in the monitoring of an AI system and this then causes ongoing, unchecked consumer deception. This approach would recognize the importance of the human oversight of AI automated decision-making.

2. Strict liability. - An alternative to any kind of negligence/intent approach is to retain strict liability but widen the range of prohibited conduct. The law could be reframed so as to hold liable any creator of an AI system that deceives or misleads a consumer, and any advertiser that uses such a system. After all, it is the advertiser and the AI creators who financially benefit from using the AI-powered marketing strategies in order to increase sales, so it seems unfair for them to be free from the consequences of deception that result from these strategies.[90] The advertiser and the AI creator are also in a better position than the consumer to both bear the loss caused by the misinformation (by spreading the costs via price adjustments) and prevent misinformation (by abandoning a black box AI system if it is too unpredictable).[91] Ultimately, such a strict liability approach might have the effect of stifling the use of advanced AI in advertising. However, it is debatable whether using the power of AI to continually improve advertising is the best use of AI in a world where more pressing problems need to be solved.

3. Pre-sale approval approach. - A different approach would be to create a pre-sale approval system.[92] Under this kind of system there would be obligations imposed on IoT companies to prove that the AI systems underpinning our IoTs have a low risk of causing deception before

[89] Caitlin Dewey, *Meet Tay, the Creepy-Realistic Robot Who Talks Just like a Teen*, WASH. POST (Mar. 23, 2016 1:32 PM), https://www.washingtonpost.com/news/the-intersect/wp/2016/03/23/meet-tay-the-creepy-realistic-robot-who-talks-just-like-a-teen/.

[90] *See* Gregory C. Keating, *The Idea of Fairness in the Law of Enterprise Liability*, 95 MICH. L. REV. 1266 (1997) (arguing that accidental losses should be borne according to the degree to which people benefit from a profit-making enterprise.)

[91] This is an approach that is in line with the theory proposed by Guido Calabresi that liability should fall on the "cheapest cost avoider." *See* GUIDO CALABRESI, THE COST OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS (1970).

[92] *See* Deven R. Desai & Joshua A. Kroll, *Trust But Verify: A Guide to Algorithms and the Law*, 31 HARV. J. L. & TECH. 1 (2017) (discussing some of the difficulties of requiring post-event transparency as a solution to mitigating possible undesired outcomes from opaque automated decision-making. The authors suggest ex ante regulation of algorithms that encompasses technically informed solutions such as requirements that software be built to certain specifications that can be tested or verified, and requirements that software is built to allow for analyzability and technical accountability.).

they are approved for the market. This kind of pre-sale approval system exists in current regulations such as those that prevent unsafe pharmaceuticals or unsafe food from entering the market.

This approach does have its own challenges.[93] It could prove very difficult to flesh out the obligations with enough detail or clarity to form the basis of a feasible system. Moreover, if the AI creators are not transparent about their design, or if the system works within a black box environment, it might be impossible for regulators to detect potentially risky features of the AI system. In addition, as has already been pointed out, any regulation that applies specifically to AI is complicated by the difficulties in coming up with a workable definition for "artificial intelligence." If lawmakers are to have any chance of creating a meaningful and workable set of pre-sale obligations they would need to work with AI experts to devise the details. Obligations in the future might include the requiring of pre-sale evidence of the use of specified software templates, detailed mechanisms for reporting problems, and requirements that AI creators use updating and monitoring programs that follow certain design templates.[94]

D. Should Any Responsibility Fall on the Companies Monetizing the Data?

The previous section considered liability for AI deception. Let us now turn to the more familiar scenario of a human seller delivering a misleading or false advertisment to consumers via an IoT device. In these cases the seller will be liable under the current laws against misleading and false advertising. But there is another critical player in modern advertising, who may also feature in the IoT future, who is not currently responsible for misleading or false advertising. This player, named the "surveillance capitalist" by Shoshana Zuboff, is the corporation who monetizes the data.[95]

These corporations own the data and the AI power to aggregate and analyse this data to offer a way to target adverts, based on models of behavioural prediction.[96] Understandably, they hold enormous power because the advertising sector wants to tap into the predictive power of the data to improve the effectiveness of their advertising. In the current online world these players are companies such as Facebook, Google and

[93] *See* Scherer, *supra* note 87 (discussing some of the practical challenges of using ex ante regulations to control AI systems).

[94] Stuart Russell discusses this kind of technical detail forming part of future AI legal obligations. RUSSELL, *supra* note 36, at 252.

[95] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR THE FUTURE AT THE NEW FRONTIER OF POWER (Profile Books 2019). *See also* MARCIN BETKIER, PRIVACY ONLINE, LAW AND THE EFFECTIVE REGULATION OF ONLINE SERVICES 58-74 (INTERSENTIA 2019) (discussing the nature of the power that is held by the controllers of our personal data and the detriments that flow from unconstrained use of this data).

[96] *See generally* ZUBOFF, *supra* note 95.

Twitter. There is fierce public debate these days about whether these digital companies should be legally responsible for removing misleading advertising, particularly misleading or fake political ads, from their sites.[97] A legal requirement to remove content could be seen as unfair given that the platforms are the hosts or the conduit of content, rather than being the creators of the content.[98] Indeed, in the United States this notion is reflected in section 230 of the Communications Decency Act 1996, which gives online platforms broad legal immunity, with some exceptions, from being sued for content posted by a user.[99]

The alternative view is that platform-based information intermediaries cannot continue to plausibly be understood as neutral players in the marketplaces of ideas, given the intentional decisions that they make about moderation and the algorithms they use to curate what information each of us receive.[100] The fundamental problem lies in the fact that all the money that these platforms make comes from targeted advertising. This incentivizes them to make design choices to curate our information flow in a way that targets our interests, in order to keep us online, watching more ads and allowing more data collection to further refine the targeting algorithms. It is a vicious cycle. For example, an algorithm might gauge that misinformation about a bogus alternative health remedy is likely to be popular and then drive the reach of the message by targeting it to people who are most likely to share it, and thus

[97] For an in-depth discussion about the challenges of regulating platforms, see Julie E. Cohen, *Law for the Platform Economy*, 51 U.C.D. L. REV. 133 (2018).

[98] Mark Zuckerberg's initial resistance to the pressure on Facebook to remove misleading posts made by President Trump in 2020 is indicative of this hands-off approach to content posted on its site. *See* Mike Isaac et al., *Zuckerberg Defends Approach to Trump's Facebook Posts*, N.Y. TIMES (Jun. 2, 2020), https://www.nytimes.com/2020/06/02/technology/zuckerberg-defends-facebook-trump-posts.html. In January 2021, Facebook reversed this approach by indefinitely banning Trump from its site after rioters stormed Capitol Hill to protest the election results. Zuckerberg was concerned that Trump's posts were intended to undermine the transfer of power to President-elect Joe Biden. *See* Kate Conger & Mike Isaac *Facebook Bars Trump Through End of His Term* NEW YORK TIMES (Jan. 7, 2021) https://www.nytimes.com/2021/01/07/technology/facebook-trump-ban.html. Twitter followed suit by permanently banning Trump from its site "due to the risk of further incitement of violence," see Kate Conger & Mike Isaac, *Twitter Permanently Bans Trump, Capping Online Revolt*, NEW YORK TIMES (Jan. 8, 2021) https://www.nytimes.com/2021/01/24/business/media/trump-facebook-oversight-board.html https://www.nytimes.com/2021/01/08/technology/twitter-trump-suspended.html.

[99] 47 U.S.C. § 30 ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

[100] *See, e.g.*, Anupam Chander & Vivek Krishnamurthy, *The Myth of Platform Neutrality*, 2 GEO. L. TECH. REV. 400 (2018).

influence the viewpoints of thousands or even millions of people.[101] The AI is not designed to promote truth, it is designed to promote popularity.

In response to pressure to conduct some monitoring of misinformation on its site, Facebook instigated a new policy in 2019 of paying third-party fact checkers to check for false advertising (but not political advertising).[102] The policy, however, fails to adequately tackle misinformation given that it is under-funded and any false advertisements that are discovered merely get flagged as such but generally do not get removed from view entirely.[103] Unsurprisingly, companies, such as Facebook, that rely on advertising for revenue are unlikely to adequately police ads when they are not legally required to do so. Even if they were legally required to monitor this information there remains the problem of scale. There is a massive amount of content on the social media platforms, and once the information is out there it can be shared. Controlling misinformation is a daunting task. One day the task might be made easier by the use of AI to aid the detection of misleading advertisements.[104] It is hard to imagine, however, that AI will be able to completely take over the task any time soon given that it requires weighing conflicting sources of information and giving appropriate consideration to context and nuance.

[101] *See* Nathalie Maréchal & Ellery Roberts Biddle, *It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge*, Ranking Digital Rights, Open Technology Institute, NEW AM. (last updated Mar. 17, 2020) http://newamerica.org/oti/reports/its-not-just-content-its-business-model/ (arguing that content-driving algorithms are responsible for much of the spread of misinformation.).

[102] *See Fact-Checking on Facebook*, FACEBOOK BUSINESS HELP CENTER, https://www.facebook.com/business/help/2593586717571940?id=673052479947730 (last visited Mar. 15, 2021). Google has similarly instigated policies to remove misleading advertising. *See* Davey Alba, *Google Goes After Bad Ads and Bad Sites That Profit from Them*, WIRED (Jan. 25, 2017, 9:00 AM), https://www.wired.com/2017/01/google-goes-bad-ads-bad-sites-profit/; Jon Porter, *Facebook Confirms Ban on Misleading Coronavirus Ads*, VERGE (Feb. 26, 2020, 5:22 AM), https://www.theverge.com/2020/2/26/21154069/facebook-coronavirus-advertising-ban-misinformation-sense-of-urgency. *See also* Kang-Xing Jin, *Keeping People Safe and Informed About the Coronavirus*, ABOUT FACEBOOK (Dec. 18, 2020), https://about.fb.com/news/2020/07/coronavirus/.

[103] Chris Mills Rodrigo, *Critics Fear Facebook Fact-Checkers Losing Misinformation Fight*, HILL (Jan. 20, 2020, 7:30 AM), https://thehill.com/policy/technology/478896-critics-fear-facebook-fact-checkers-losing-misinformation-fight. In 2020 Facebook agreed the policy would, however, extend to removing advertisements that make misleading claims promote fake cures for Covid-19. *See* Porter, *supra* note 102.

[104] The Australian Securities and Investments Commission (ASIC) has announced plans to develop artificial intelligence technology to detect misleading online advertising for financial products. *See* James Eyers, *ASIC to Use AI to Target Misleading Advertising*, FINANCIAL REVIEW (Mar. 3, 2019, 11:00 PM), https://www.afr.com/companies/financial-services/asic-to-use-ai-to-target-misleading-advertising-20190303-h1bx8f.

As the IoT era expands, there will be new opportunities for "surveillance capitalists" to take advantage of an IoT-based adverting model in the same way that is happening on our screens.[105] Exploring the possibility of imposing obligations on these companies for consumer misinformation is likely to be a hot topic for debate in the future.[106] As has already been discussed, it is not clear yet who the main players in this developing IoT world will be. Indeed, the dystopian vision of the future would feature one or two giant monopoly companies owning all aspects of our IoT smart-homes, smart-cars and smart-wearables and selling behavioral predictions and targeted advertising.

It seems fair that these IoT corporations should bear at least some of the risks of conveying false information to consumers. However it is debateable whether it is appropriate to legally require private corporations to be the deciders of what is misleading and what is truthful, and what information should and should not be out in the market-place.[107] Perhaps we would prefer these decisions to be made by public enforcement agencies whose mission is to protect consumers from misleading and deceptive advertising. But public enforcement agencies might find the task overwhelming given current funding restraints, a lack of tech expertise and no access to the algorithms used by the industry to amplify and target information. Increasing the funding levels and the technical expertise of public enforcement agencies is discussed further in Part VI(A) and (B) below. It is vital that lawmakers wanting to reformulate the law to protect consumers from misinformation in the era of IoT explore options for placing some responsibilities on the corporations that enter the business of monetizing the data that the IoT environment produces.

[105] *See generally* ZUBOFF, *supra* note 95.

[106] *See* Howells, *supra* note 69, at 149 (suggesting that one key area for new regulatory solutions lies in the area of platform liability). For a discussion on the challenges of applying consumer law in a platform economy in the travel industry, see Margherita Colangelo & Vincenzo Zeno-Zencovich, *Online Platforms, Competition Rules and Consumer Protection in Travel Industry*, 2 J. EUR. CONSUMER & MKT. L. 75 (2016). Germany has already introduced legislation to make digital hosting platforms responsible for removing hate speech and fake news. *See* Netzdurchsetzunggesetz [Network Enforcement Act], Jul. 7, 2017, [BR] 536/17 (Ger.), which came into force in 2018. The Act penalizes the digital platform and not the person posting the fake news or hate speech.

[107] *See* DAVID KAYE, SPEECH POLICE: THE GLOBAL STRUGGLE TO GOVERN THE INTERNET (Columbia Global Reports 2019) (arguing that giving private companies the job of policing speech on the internet gives them a massive power over the future of freedom of expression worldwide).

E. Summary

In summary, the current consumer laws prohibiting misleading and deceptive communication are focused on the human conduct of misleading or deceiving. This poses a problem when applied to black box AI-automated misinformation emanating from IoT devices. Creating AI legal personhood is a poor solution to this problem and only distracts from the task of re-formulating the laws to target those companies and individuals who design the AI systems. The better approach would be to re-word the laws so as to refer to the kinds of human conduct that ultimately lead to the deception or misleading communication. Under such an approach, consideration would need to be given to the best way to deal with concepts of causation, intent and fault when it is an automated AI that is the source of the misinformation.

Any reform of traditional legal rules about misleading and deceptive information (whether it is coming directly from a human, or via an AI system), will need to grapple with questions such as who is in the best position to bear the loss, who is in the best position to prevent the misinformation, and how best to apply the principle that holds that the person who profits from an activity should also bear the risks. What is safe to say is that consumers who are harmed by misinformation are not the ones in the best position to prevent this harm, and they should not be the ones to bear the loss. It may be that the big winners in the IoT future, if incentivised by regulation, will be able to use effective monitoring tools to avoid the propagation of misinformation to consumers via IoT devices.

IV. THE "WHAT" QUESTION

This section moves on from the question of "who" to the question of "what." Namely: what kinds of consumer information should be covered by consumer protection laws in an IoT era? The aim here is to discuss current gaps and weaknesses in the current laws that will allow companies to avoid responsibility for communicating to consumers via IoT devices in ways that are misleading, deceptive or manipulative.

A. "But this isn't advertisement or a trade practice."

Let us assume that an IoT has produced some kind of speech that is misleading. One of the hurdles of applying current regulatory frameworks to IoT speech is that the speech might not seem like an advertisement. It might not even seem like communication in a trade setting. Currently consumer protection laws around the world are phrased so as to limit their scope to misleading communication that happens "in trade or commerce"[108] or is a "trade practice" or "commercial practice"[109] or amounts to false "advertising."[110] In the United States at the federal level, the FTC Act prohibits deceptive unfair or deceptive acts or practices "in or affecting commerce."[111] Most States in the USA have adopted versions of the Uniform Deceptive Trade Practices Act (UDTPA) which refers to a person engaging in a deceptive "trade practice."[112] These limiting phrases are necessary to ensure that only misleading *commercial* speech is controlled by governments, and not other types of misleading speech.[113] We are generally free to mislead or lie to people, but businesses are not permitted to mislead or lie to consumers.

Future IoT corporations might try to avoid liability for misleading communication by claiming that the communication emanating from an IoT device was not an advertisement, and was not taking place in trade or commerce. Consumers might also fail to even be aware that they are being exposed to advertisements.[114] Advertising in its broadest sense is simply speech intended to make consumers spend money to buy more goods and services. It is likely that some of the information that flows out of IoT devices to the consumer will be designed to influence purchasing decisions. The commercial messages might be in the form of the chatty voice of your child's soft toy, the familiar reassuring voice of your AI personal assistant, or a friendly smart car. The lines between when your IoT assistants are in an entertainment-chatty mode, and when they are in an "in trade" mode, might be hard to draw.

Imagine you are elderly and have a robot dog companion. The robot dog asks you, in its doggy voice and with its big pleading puppy eyes, for a dog friend that will make it less lonely. Is this an advertisement for robot dogs? Or is it just a chatty dog making conversation? Presumably the communication is intended to make you buy another dog, but there

[108] This is the phrase used in the Australian Consumer Law set out in Schedule 2 of the *Competition and Consumer Act 2010* (Cth) s 18 (Austl.). The New Zealand law uses the phrase "in trade." Fair Trading Act 1986, ss 9-14 (N.Z.).

[109] *See* Consumer Protection from Unfair Trading Regulations, *supra* note 61.

[110] Advertising Industry Codes are also limited to regulating communication that can be considered advertising. Industry self-regulation organizations include the Australian Association of National Advertisers (AANA), the Advertising Standards Authority (ASA) in the United Kingdom, the Advertising Self-Regulatory Council (ASRC) in the United States and Ad Standards in Canada.

[111] *Supra* note 58.

[112] *Supra* note 73.

[113] In the United States, a ban on deceptive or misleading *commercial* speech does not impinge on the First Amendment's prohibition against governmental restrictions on speech. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 562-64 (1980).

[114] Even if they become aware of the deception it is unlikely to evolve into a legal claim. This idea of only a small number of grievances ever maturing into disputes is discussed in William L.F. Felstiner et al., *The Emergence and Transformation of Disputes: Naming, Blaming, Claiming* 15 LAW & SOC'Y REV. 631 (1980).

seems to be some shades of gray here. Imagine you also have a robot personal assistant/housekeeper. She has been with you for years and because of AI learning, she knows everything about you and your preferences. One day she looks you in the eyes and tells you in a sad voice that she is tired. She further suggests that her work would be done a lot quicker with another robot housekeeper on board. Is there any communication "in trade" happening at this point? Your robot might deceive you by failing to tell you about the hidden fees in a robot-housekeeper contract, or she might misrepresent the new model's features and abilities. Worse still, she might show you a *deepfake* video of your favorite celebrity telling you that it is far better to have two robot housekeepers than one, or for that matter, recommend any product.[115] Suppose too that your robot assistant and your robot dog are able to make a purchase for you simply by hearing your voice command. What we have here is a conflation of what behavioural scholars call "market norms" (or "exchange relationship") and "social norms" (or "communal relationship").[116] The nature of the exchange and the communication is blurred in a way that makes it hard for the consumer to properly realize what is going on.

In developing effective laws to regulate an IoT world, lawmakers will need to include more expansive definitions and understandings of the concepts of advertising and commercial communication. The functions of advertising are likely to be performed in a different way. The communications via IoT devices will not look like what we have historically considered an advertisement, nor will they look like the current online advertisements. It is arguably not even helpful to use the word "advertisement" as it conjures up images of a limited and old-style of commercial communication. The commercial messaging of the future might not have any obvious characteristics of an "advertisement," a "trade practice" or conduct "in trade or commerce."

Legislation should be extended so that it covers all communication (including that emanating from an IoT device) that is paid for by a brand with the aim of increasing sales. Sometimes this communication might be subtle, relying more on improving brand awareness than specifically

[115] Deepfake technology is a form of AI that allows realistic video and audio content of anyone to appear to be saying anything. *See* Ian Sample, *What Are Deepfakes – and How Can You Spot Them?*, THE GUARDIAN (Jan. 13, 2020), https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them. *See also* Sonia K. Katyal, *Artificial Intelligence, Advertising, and Disinformation*, Keynote Address at the Third Annual *Advertising & Society Quarterly* Colloquium 20 ADVERT. & SOC'Y Q. (2019).

[116] DAN ARIELY, PREDICTABLY IRRATIONAL: THE HIDDEN FORCES THAT SHAPE OUR DECISIONS 68–69 (Harper Collins 2008); Margaret S. Clark & Judson Mills, *Interpersonal Attraction in Exchange and Communal Relationships*, 37 J. PERSONALITY & SOC. PSYCHOL. 12 (1979).

plugging of a product.[117] Canadian false advertising legislation provides a possible model for wording that covers a broad range of communication. Under the Canadian Competition Act, materially false or misleading representations are reviewable if made to the public "for the purpose of promoting, directly or indirectly, the supply or use of a product or for the purpose of promoting, directly or indirectly, any business interest, by any means whatever."[118] This wording avoids limiting the scope to the content in traditional advertisements. Nevertheless, the concept of "promoting" would need to be interpreted in its widest sense when applied to communication from IoTs, which will work by way of increasingly personalized persuasion and behavior modification. A message through your IoT headphones, as you walk past an outdoor pool, that tells you that it is the hottest day so far this summer, is not obviously "promoting" the swimming pool. It might not even mention the word "pool." But if this message is paid for by the pool owners, then it should be a reviewable representation as its purpose is to change your behavior so that you pay for a swim.

In short, legislation should apply to a broad category of promotion activities, not just some old-fashioned view of an advertisement. It should be drafted in such a way as to include all forms of communication, where the ultimate goal is to modify a consumer's purchasing behavior in any way. If any of *that* kind of communication is in any way misleading, then the assumptions underlying neoliberal economics model fall apart. Accurate, non-misleading information is needed for consumers to make free and informed choices.

B. Disclosure Requirements

The discussion in the last section has identified the challenge of landing liability in cases where a defendant may argue that the misleading speech from an IoT device was not an "advertisement" and did not occur "in trade or commerce." This leads on to a further interesting point. Even if the content of the information being delivered to consumers is not itself misleading, there may still be a level of deception in cases where advertisers are hiding from consumers the fact that the speech is paid for by a brand to influence sales, and so is essentially an advert. A failure to disclose the fact that an accurate message is an advertisement is misleading and has the potential to distort consumer behavior.

As pointed out above, businesses already hide advertising in regular online content such as online entertainment, news, or social

[117] Rong Huang & Emine Sarigöllü, *How Brand Awareness Relates to Market Outcome, Brand Equity, and the Marketing Mix*, 65 J. BUS. RES. 92 (2012).

[118] Competition Act, R.S.C. 1985, c C-34, §74.01(1)(a) (Can.). *See also* the criminal provision on misleading advertising, which is substantially similar to §74 but also requires mens rea of intention. *Id.* §52.

media posts. These adverts, often called "native advertising," are designed to match the appearance and form of the online environment in which they are placed. They are effective at persuading people to buy more products.[119] This is at least in part because consumers lack the knowledge of the persuasive intent of the communication and therefore fail to experience scepticism or resistance to the messaging.[120] One can only imagine the ways in which advertisers will use the IoT of the future to more stealthily insert advertising messages into consumers lives. The previous sections have given some illustrations of how it might work. Even if these suggestions turn out to be off the mark, it is undeniable that marketers will be looking for innovative ways to seamlessly integrate marketing messages into consumers lives via IoT.

Communication that blurs the lines between advertising and media content has raised the concern of regulators and scholars over the past few years.[121] There is as of yet no specific United States federal offence of camouflaging advertising, but there is the general prohibition on "unfair or deceptive acts or practices in or affecting commerce" in §5 of the FTC Act.[122] The FTC has expressed the view that advertising messages that are not identifiable as advertising are deceptive if they mislead consumers into believing they are independent, and are therefore a breach of §5 of the FTC Act.[123] The FTC is envisaging native advertising on a mobile or computer screen. Nevertheless, the principle should apply equally to voice messages from an IoT device. Whether the ad is disguised as regular media content, or as general chit-chat from an IoT personal assistant, it should be treated the same.

The European Union takes a more direct approach by explicitly referring to the deception of embedded marketing. The E-Commerce EU Directive requires all commercial communications to be clearly

[119] *See* Seunghyun Kim et al., *Consumers' Responses to Native vs. Banner Advertising: Moderation of Persuasion Knowledge on Interaction Effects of Ad Type and Placement Type*, 38 INT'L J. ADVERT. 207 (2019); Chiang I-Ping et al., *Do Native Advertisements Attract More Attention from Facebook Users?*, 9 INT'L J. ELECTRONIC COM. STUD. 191 (2018).

[120] Kim et al., *supra* note 119; Chiang et al., *supra* note 119.

[121] *See*, *e.g.*, Lili Levi, *A "Faustian Pact"?: Native Advertising and the Future of the Press*, 57 ARIZ. L. REV. 647 (2015); Dipayan Ghosh & Ben Scott, *Digital Deceit: The Technologies Behind Precision Propaganda on the Internet*, NEW AMERICA (Jan. 23, 2018), http://newamerica.org/public-interest-technology/policy-papers/digitaldeceit/.

[122] Federal Trade Commission Act §5, 15 U.S.C. §45. In addition, the Communications Act forbids the undisclosed acceptance of payment for promotion of a product, but this only applies to on-air TV and Radio. Communications Act of 1934, 47 U.S.C. §§ 151, 317 & 507 (1934).

[123] *See* Federal Trade Commission, Enforcement Policy Statement on Deceptively Formatted Advertisements, 81 Fed. Reg. 22596 (Apr. 18, 2016). *See also* Federal Trade Commission, *Guides Concerning the Use of Endorsements and Testimonials in Advertising*, 16 C.F.R. § 255 (2020) (similar rules around endorsements.).

identifiable as such and the person on whose behalf the commercial communication to be also identifiable.[124] Although the EU did not have IoT devices in mind when drafting this Directive, the wording is broad enough to be applied to speech from an IoT.

The United States and other jurisdictions also have statutory provisions that allow for civil remedies for misleading conduct in trade.[125] These provisions are theoretically broad enough to cover the deception of hiding advertising. However, relying on civil liability in this arena has limited impact. Consumers are unlikely to complain about an advertisement that they did not realise was an advertisement. Ideally the consumer protection laws of each country should be assessed, and where necessary reformulated, so as to explicitly require sufficient disclosure to enable consumers to recognise when marketing manipulation is the purpose of the message being delivered by their IoT devices. This at least gives consumers a chance to approach the message with a degree of scepticism.[126]

[124] European Parliament and Council Directive 2000/31, art. 6, 2000 O.J. (L 178) 1 ('EU Directive'). The United Kingdom has developed regulations based on the EU model. The Consumer Protection from Unfair Trading Regulations prohibits unfair commercial practices, such as misleading omissions. 2008, SI 2008/1277, art. 6 ¶1(d) (UK). The regulations specifically include failing to identify the commercial intent of a commercial practice as a category of misleading omission. Note also that the EU has prohibited surreptitious advertising in broadcasting media since 1989. *See* Council Directive 89/552 1989 O.J. (L 298) 23 (EC).

[125] All states have "Unfair and Deceptive Acts and Practices" legislation (or "UDAP statutes") which provide civil remedies for consumers misled by advertising. Nevertheless, the effectiveness of UDAP statutes varies widely from state to state and in many states there are serious gaps or weaknesses in the level of consumer protection offered. *See Consumer Protection in the States: A 50-State Evaluation of Unfair and Deceptive Practices Laws*, NAT'L CONSUMER L. CTR. (Mar. 2018) https://www.nclc.org/issues/how-well-do-states-protect-consumers.html. False advertising claims can also be bought by competitors under the federal Lanham Act. Lanham Act §43(a), 15 U.S.C. §1125(a)(1)(B) (2012).

[126] There is some scholarly criticism of the use of disclosure as a regulatory tool. *See, e.g.*, Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647 (2011). However, in respect of sponsorship disclosures there is evidence that disclosure can be effective if framed appropriately. *See, e.g.*, Eva A. van Reijmersdal et al., *Effects of Disclosing Influencer Marketing in Videos: An Eye Tracking Study Among Children in Early Adolescence*, 49 J. INTERACTIVE MKTG 94 (2020) (showing that commercial content disclosures prior to videos can indirectly evoke in children and adolescents a skepticism and resistance toward the content and the brand); Sophie C. Boerman et al., *"This Post Is Sponsored" Effects of Sponsorship Disclosure on Persuasion Knowledge and Electronic Word of Mouth in the Context of Facebook*, 38 J. INTERACTIVE MKTG 82 (2017) (showing that the recognition of advertising increases distrusting beliefs about a sponsored post); Bartosz W. Wojdynski et al., *Measuring Sponsorship Transparency in the Age of Native Advertising,* 52 J. CONSUMER AFF. 115, 134 (2018) (developing a scale to measure sponsorship transparency and arguing that "where emerging formats challenge our expectations of and familiarity with 'what is advertising,' the ability to have a means by which to assess

C. Puffery

It does not take much imagination to see that your IoT personal assistant of the future might use exaggerated vague claims for the purpose of commercial gain. When you ask her whether she knows of any products on the market that will make you look better, she suggests a moisturiser that will "make you look a decade younger." When she hears that you are feeling unwell, she might mention a nutritional supplement that will "completely reboot your immune system and rebalance your chakras." These kinds of statement are sometimes called puffs.

In general terms, puffery can be described as vague, exaggerated marketing claims. In most legal systems, claims that are considered "mere puffs" will not attract liability.[127] The theory is that consumers do not take these claims seriously and so are not misled by them. For example, the court in *Martin v. Living Essentials, LLC* held that exaggerated claims were non-actionable puffery because there was "no danger of consumer deception and hence, no basis for a false advertising claim."[128] It is interesting to consider whether this reasoning holds in a world of IoT communication.

There has always been something paradoxical about the way firms approach puffs. On the one hand, sellers spend large amounts of money using puffery, in the hopes of influencing consumers. At the same time, they defend themselves against complaints by arguing that consumers are not misled by puffery. It is difficult to see how puffery can be both effective and of no effect, at the same time.[129] It is difficult to understand why firms invest large sums of money in these puffs if they do not influence consumers.

Sellers are, no doubt, well aware that puffery is often more powerful in the new and expanding digital marketing landscape, than it was in old-style ads. When a consumer hears a radio jingle or a paid actor in a TV ad tell them something is "the best product ever," they might not believe it. However, consumers are far more likely to subconsciously believe the puffery when the message is not directly from the seller, but

the extent to which a consumer can make this assessment is paramount"). The concept of "emerging formats" brings to mind the emerging IoT phenomenon.

[127] For example, the FTC does not pursue subjective claims of puffery–in one of its guidelines it states that claims like "this is the best hairspray in the world" are acceptable. Roscoe B. Starek, III, *Myths and Half-Truths About Deceptive Advertising*, FED. TRADE COMM'N (Oct. 15, 1996), https://www.ftc.gov/public-statements/1996/10/myths-and-half-truths-about-deceptive-advertising. *See also* Pizza Hut, Inc. v. Papa John's Int'l, Inc., 227 F.3d 489, 497 (5th Cir. 2000).

[128] Martin v. Living Essentials, LLC, 160 F. Supp. 3d 1042,1049 (N.D. Ill.), *aff'd*, 653 F. App'x 482 (7th Cir. 2016).

[129] *See* David A. Hoffman, *The Best Puffery Article Ever*, 91 IOWA L. REV. 1395 (2006) (discussing the drawbacks of the puffery defense to society and arguing that courts are incapable of satisfactorily drawing a line between harmful and innocuous puffery, and that sellers use puffery to exploit buyers' cognitive vulnerabilities.)

from a journalist working for their favourite newspaper, or their favourite travel blogger raving about her new hiking boots, or a glowing Instagram star recommending a special detox tea to lose weight. Just imagine how much more powerful the marketing messages will be when they are in the form of familiar, friendly speech from an IoT personal assistant; where the tone, content and timing of the speech is calibrated by AI algorithms to be the most persuasive to us as an individual.

The idea that we will not be misled by exaggerated, impliedly untrue claims because we will see them as "mere puffery" has always been dubious.[130] Behavioural economics studies have shown that consumers are not as rational as traditional economic theory would have us believe.[131] We will explore consumer irrationality further in relation to manipulation in the following section. At this point it is enough to suggest that with the power of IoT, big data, and AI, combined together and geared towards persuading us, it is naive to think we will act rationally and see through all the puffery. It is more likely that we will, on some level, be misled. The justifications for allowing puffery begin to break down when it is accepted that consumers are susceptible to its influence. Any attempt to reform the law to prevent deception in an era of IoT advertising will need to re-consider and update the legal rules surrounding puffery. Certainly, the assumptions that underlie the current approach to regulating puffery need to be revisited.

D. Manipulation

1. How we are manipulated. - Understanding that modern consumers have a limited resistance to puffery leads on to the more general question about how tolerant we, as a society, want to continue to be about the use of manipulation as a method of selling more products.[132] This is a "what" question, in that it asks what types of communication the law should be prohibiting in an IoT future.

Modern advertisers have, of course, been attempting to manipulate consumer preferences for the past hundred years or more.[133]

[130] *Id.*at 109.

[131] *See*, for example, Colin F. Camerer & George Loewenstein, *Behavioral Economics: Past, Present, Future*, *in* ADVANCES IN BEHAVIORAL ECONOMICS (Colin F. Camerer et al. eds., 2004).

[132] Ramsi A. Woodcock, *The Obsolescence of Advertising in the Information Age*, 127 YALE L. J. 2270 (2018) (questioning the benefit to society of persuasive, manipulative advertising). He takes the extreme position of recommending that the FTC should treat all advertising, beyond the minimum required to ensure that product information is available to online searchers, as monopolization in violation of section 2 of the Sherman Act.

[133] Tobacco advertising started back in the 1920s. One of the classic books on the persuasive powers of advertising was written in 1957 by Vance Packard. VANCE PACKARD, THE HIDDEN PERSUADERS (Longmans 1957). *See also* Dan Ariely et al., *"Coherent*

Indeed this is the entire point of advertising. David Foster Wallace in his novel *Infinite Jest* nicely sums it up when he states: "It did what all ads are supposed to do: create an anxiety relievable by purchase."[134] Consumers are susceptible to market manipulation because we are, as behavioural economist Dan Ariely puts it, "predictably irrational."[135] Our judgments are often subject to systematic biases and heuristics.[136] Sometimes we do not have the self-control to sacrifice short-term gratification for long-term benefits.[137] We are also easily influenced by framing effects and context.[138]

In the past, advertisers could combine art and psychology to exploit our biases and manipulate our fears and needs. The combination of big data and AI gives advertisers a new capacity to exploit our weaknesses and to actively influence behaviour. We saw the power of these new technologies to manipulate people in the realm of political advertising in 2018 when the consulting firm, Cambridge Analytica, used millions of Facebook users' data to change the voting behavior of Americans.[139]

Arbitrariness": Stable Demand Curves Without Stable Preferences, 118 Q.J. ECON. 73, 103 (2003). Ariely shows that consumer preferences can be deliberately manipulated. *See also* Kyle Bagwell, *The Economic Analysis of Advertising*, *in* HANDBOOK OF INDUSTRIAL ORGANIZATION 1701, 1724 (Mark Armstrong & Rob Porter eds., 2007); BAR-GILL, *supra* note 52; Gaëlle M. Bustin et al., *Who Does Red Bull Give Wings to? Sensation Seeking Moderates Sensitivity to Subliminal Advertisement*, 6 FRONTIERS IN PSYCHOL. 825 (2015); Johan C. Karremans et al., *Beyond Vicary's Fantasies: The Impact of Subliminal Priming and Brand Choice*, 42 J. EXPERIMENTAL SOC. PSYCHOL. 792 (2006).

[134] DAVID FOSTER WALLACE, INFINITE JEST 284 (2011).

[135] *See* ARIELY, *supra* note 116. *See also* Christine Jolls et al., *A Behavioral Approach to Law and Economics*, 50 STAN. L. REV. 1471 (1998) (arguing that the neoclassical economic idea that informed consumers will act to maximize their own welfare is flawed and that evidence points to people not always behaving rationally in their own best interests); Colin F. Camerer & George Loewenstein, *Behavioral Economics: Past, Present, Future*, *in* ADVANCES IN BEHAVIORAL ECONOMICS (Colin F. Camerer et al. eds., 2004).

[136] Lucia A. Reisch & Min Zhao, *Behavioural Economics, Consumer Behaviour and Consumer Policy: State of the Art*, 1 BEHAV. PUB. POL'Y 190 (2017); Camerer & Loewenstein, *supra* note 135.

[137] *See* Shane Frederick et al., *Time Discounting and Time Preference: A Critical Review*, 40 J. ECON. LITERATURE 351, 352 (2002); Shahram Heshmat, *Behavioral Economics of Self-Control Failure*, 88 YALE J. BIOLOGY & MED. 333 (2015).

[138] *See generally* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (Yale University Press 2008). For example, people are influenced by the presentation of default choice, as they will tend to take the default option over making an active choice. Gabriel D. Carroll et al., *Optimal Defaults and Active Decisions*, 124 Q.J. ECON. 1639 (2009).

[139] *See The Cambridge Analytica Files*, GUARDIAN, https://www.theguardian.com/news/series/cambridge-analytica-files (last visited Mar. 15, 2021). *See also* Concordia, *Cambridge Analytica - The Power of Big Data and Psychographics,* YOUTUBE (Sep. 27, 2016), https://www.youtube.com/watch?v=n8Dd5aVXLCc (Alexander Nix, former CEO of Cambridge Analytica, discussing how his company's psychological profiling techniques

AI-driven marketing strategies aim to manipulate consumers by sending the right information, at the right time, so as to maximise the chances of a consumer making a purchase.[140] In other cases the manipulation might occur through the use of "filter bubbles" to distort each consumer's reality in ways that lead to commercial outcomes.[141] Our personal network of IoT devices might one day understand our behaviors, desires, and motivations better than we understand ourselves. Once they understand us, they can nudge us toward profitable outcomes.[142]

This ability to aggressively manipulate behaviour for profit via IoT computing is especially concerning for vulnerable consumers. For example, data from IoT devices could be used to pinpoint those with gambling or alcohol addiction, or those on a low income. These people can then be manipulated toward spending money on alcohol, casinos, or pay-day lending. The ability for technology to target the vulnerable is super-charged by the power of AI-driven IoT to pin-point not just the individual's general characteristics, but to use real-time data, to identify the time, place, mood, facial and other subliminal cues that can predict the optimal time to deliver the marketing message, and the exact way to present the message so as to maximise a commercial outcome.[143]

were revolutionizing political campaigning). *See also* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014) (detailing how collected information can be used to manipulate consumer choice).

[140] Efforts to personalize the persuasion via use of technology have been in operation for many years already. *See, e.g.*, Maurits Kaptein et al., *Personalizing Persuasive Technologies: Explicit and Implicit Personalization Using Persuasion Profiles*, 77 INT'L J. HUMAN-COMPUTER STUD. 38 (2015).

[141] ELI PARISER, THE FILTER BUBBLE: WHAT THE INTERNET IS HIDING FROM YOU (2012).

[142] The term "nudge" was popularized by behavioral economists Richard H. Thaler and Cass R. Sunstein in their 2008 book, where they discuss techniques that governments can use to nudge citizens toward smarter choices. *See generally* THALER & SUNSTEIN, *supra* note 138. Corporations also use these insights to nudge us to buy products. *See* ZUBOFF, *supra* note 95 at 8. Zuboff describes how this new way of advertising works by way of the acquisition of ever more predictive sources of behavioral data and uses that data to "nudge, coax, tune, and herd behavior toward profitable outcomes."

[143] The drive toward designing AI to automatically read spontaneous emotional cues and use this for marketing purposes is already underway. *See, e.g.*, *The Automatic Sentiment Analysis in the Wild* (SEWA), a European Union research project which aims to use algorithms for machine analysis of facial, vocal, and verbal behavior to read emotions. *SEWA Project*, SEWA, https://sewaproject.eu/ (last visited Mar. 15, 2021); *Brands*, REAL EYES, https://www.realeyesit.com/solutions/brand/ (last visited Mar. 15, 2021) (a company which provides an AI platform that uses computing power and sensors to read emotion and offers this technology to brands in order to help them to drive up sales outcomes.); Adam D. I. Kramer et al., *Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks*, 111 PROC. NAT'L. ACAD. SCI. U.S. 8788 (June 17, 2014) (In 2014 Facebook proved it could manipulate users' emotions in a controversial newsfeed experiment.); Vindu Goel, *Facebook Tinkers with Users' Emotions in News Feed Experiment, Stirring Outcry*, N.Y. TIMES (Jun. 29, 2014),

Determining the right time might be as simple as assessing the time of day when the consumer has the least self-control. This will vary depending on factors such as whether the consumer is a morning or a night person.[144] We already have evidence of Facebook using technology to target the vulnerable when it directed ads at 6.4 million younger users, some only fourteen years old, during moments of psychological vulnerability, such as when they felt "worthless," "insecure," "stressed," "defeated," "anxious," and like a "failure."[145] Laws that prohibit misleading advertising do not prevent preying on the vulnerable in this way. Current formulations of the doctrine on undue influence and unconscionable bargains are also not applicable, given that it is "business as usual" and so not yet viewed as contrary to public policy or good conscience.[146]

The aim of an IoT advertising model will be to keep us engaged with our IoT devices, keep us absorbed in subtle forms of marketing, and keep us making new purchases. All these behaviors are likely to feel to us like we are simply exercising our free will, which may be far from the truth.[147] Some commentators have begun to ask if the AI behaviour modification will eventually become so prevalent and extreme that we will be

https://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html. *See also* Cathy O'Neil, *Propaganda Machine: Online Advertising*, *in* WEAPONS OF MATH DESTRUCTION (2017) (describing the current ways that AI is used to micro-target advertising.).

[144] *See* DANIEL KAHNEMAN, THINKING FAST AND SLOW 41 (2011).

[145] Nitasha Tiku, *Welcome to the Next Phase of the Facebook Backlash*, WIRED (May 21, 2017, 7:00 AM), https://www.wired.com/2017/05/welcome-next-phase-facebook-backlash/ (quoting a leaked confidential document prepared by Facebook that revealed that the company had offered advertisers the opportunity to micro-targeted ads down to "moments when young people need a confidence boost."). The concept of protecting the vulnerable from advertising is not new. Many countries already recognize the vulnerability of children by banning advertising on TV during children's television programming.

[146] The doctrine on unconscionability and undue influence has never been used to overturn an agreement entered into merely because manipulative advertising was effective at modifying behavior. This is despite the doctrine being seemingly applicable, given that it addresses unequal bargaining power, taking advantage of vulnerability, and in the words of J. Skelley Wright, the "absence of meaningful choice." Williams v. Walker-Thomas Furniture Co., 350 F.2d 445 (App. D.C. 1965). The doctrine envisages particular vulnerability such as age, illness, and lack of education. The problem with the future of marketing is that we are *all* vulnerable to its manipulation.

[147] This idea of our behavior being dictated by algorithms without us realizing we are being controlled is explored by the scholar Yuval Noah Harari in YUVAL NOAH HARARI, 21 LESSONS FOR THE 21ST CENTURY (2018). *See also* Yuval Noah Harari, *The Myth of Freedom*, GUARDIAN (Sept. 14, 2018 7:00 AM), https://www.theguardian.com/books/2018/sep/14/yuval-noah-harari-the-new-threat-to-liberal-democracy; DANIEL M. WEGNER, THE ILLUSION OF CONSCIOUS WILL (2d ed. 2002) (arguing more broadly that the feeling of having free will is created by the brain, giving us the illusion of having free will).

interested in a reverse of the Turing test.[148] So instead of asking if computers can become human-like, we will be asking "can humans become machine-like and pervasively programmable?"[149]

This kind of behaviour modification via IoT could become even more successful if human-like robots were ever to come on to the consumer market as household helpers or companions. A human-like robot, that grows to know our individual personality the more it interacts with us, could become very good at persuasion. It might operate in a way that side-steps the part of our brain that is conscious and deliberate, and appeals more to the unconscious part of our brain that is emotional, automatic, and intuitive. These two modes of thinking are described by Daniel Kahneman, and other psychologists, as System 1 (the automatic and often unconscious system) and System 2 (the controlled and deliberative system).[150] System 1 operates quickly and impulsively and is more focussed on present needs and desires than long term goals.[151] It is the state of mind likely to generate the most sales. A robot with the ability to tap into the System 1 part of consumers' brains would open up enormous possibilities for manipulative marketing.

The persuasive power of IoTs that have human-like mannerisms, facial expressions, and voices is likely to be formidable. Early studies on human-robot interaction have indeed shown that humans respond to robots on an emotional level even though they realise they are dealing with a machine.[152] Some studies suggest that humans are wired to unconsciously interact with robots as if they were human and perceive

[148] Alan Turing developed what is now known as the "Turing Test" in 1950. It is a test of a machine's ability to exhibit intelligent behaviour that is indistinguishable from human behaviour. A. M. Turing, *Computing Machinery and Intelligence*, 59 MIND 433 (1950).

[149] Evan Selinger & Brett Frischmann, *Will the Internet of Things Result in Predictable People?*, GUARDIAN (Aug. 10, 2015, 11:56 AM), https://www.theguardian.com/technology/2015/aug/10/internet-of-things-predictable-people. *See also* DOUGLAS RUSHKOFF, TEAM HUMAN, 63-94 (2019); ZUBOFF, *supra* note 95, at 339-40. Part II of the book covers the advance of technology to go beyond predicting existing preferences to predicting the future by creating the future.

[150] See KAHNEMAN, *supra* note 144, at 20-24.

[151] *Id.* at 20.

[152] *See* Elizabeth Broadbent, *Interactions with Robots: The Truths We Reveal About Ourselves*, 68 ANN. REV. PSYCHOL. 627 (2017) (reviewing the findings of human-robot interaction research that suggest humans are wired by both nature and nurture to unconsciously interact with robots as if they were human and perceive humanlike characteristics in them, including thoughts and emotions). *See also* Mikey Siegel et al., *Persuasive Robotics: The Influence of Robot Gender on Human Behavior*, 2009 IEEE/RSJ INT'L CONF. ON INTELLIGENT ROBOTS & SYS. 2563 (Oct. 2009) (showing that people in a museum were more likely to donate money to a robot research lab when the robot asked with a female voice than when it asked with a male voice).

human-like characteristics.[153] Indeed, to some extent, the personification of a computer is in itself a kind of deceit.

One further point worth mentioning here is that the conditions of ubiquity might make it difficult to escape the manipulation conducted via IoTs. Already the services of platforms like Facebook, Twitter, and Instagram are hard for a consumer to replace given that they are "free" and have become the way that members of society communicate with each other. As the IoT industry builds, it might also develop the kind of architecture whereby a few dominant players lock us into a system which works by way of some kind of central IoT hub. Even if we were to become truly aware of the extent to which we are being manipulated, the convenience of the IoT network might make it difficult to disconnect from.

2. Legal intervention to reduce manipulation. - The use of advertising to mold human preferences and behavior is not currently illegal, and is generally seen as an accepted form of doing businesss.[154] With the rise of AI in combination with IoT, we might want to question whether we are happy to continue with this view. Certainly, without some form of government intervention, corporations propelled by the profit motive will continue to drive this form of manipulation in ways that were not possible pre-digitization and pre-IoT.

It might be argued that consumers are okay with being persuaded and maybe even enjoy being seduced by brand imagery. However, mass consumerism has harmful side effects. Overconsumption is the key cause of the worsening levels of ecological destruction and a key contributor to climate change.[155] Perhaps more surprising is the evidence that this consumption does in fact not make consumers happy. Research suggests that when a person's value system is oriented around materialistic goals (that relate to status and external validation), rather than intrinsic goals (that focus on personal psychological growth and connection), they report lower levels of well-being.[156] The decrease in well-being may arise

[153] Broadbent, *supra* note 152.

[154] Although manipulative advertising is generally accepted by society, it has been criticized by some scholars over the years. *See, e.g.*, JOHN KENNETH GALBRAITH, THE AFFLUENT SOCIETY (1958) (contending that manipulative advertising creates wants for people, which makes them consume more without increasing their well-being). *See also* Calo, *supra* note 139.

[155] Diana Ivanova et al., *Environmental Impact Assessment of Household Consumption*, 20 J. INDUS. ECOLOGY 526 (2016); Thomas Dietz et al., *Reducing Carbon-Based Energy Consumption Through Changes in Household Behavior*, 142 DAEDALUS 78 (2013). *See also* The UK Environmental Audit Committee report on clothing consumption and sustainability. HOUSE OF COMMONS ENVIRONMENTAL AUDIT COMMITTEE, FIXING FASHION: CLOTHING CONSUMPTION AND SUSTAINABILITY, 2017-19, HC 1952.

[156] *See* Monika A. Bauer et al., *Cuing Consumerism: Situational Materialism Undermines Personal and Social Well-Being*, 23 PSYCH. SCI. 517 (2012). *See also* TIM KASSER, THE HIGH PRICE OF MATERIALISM (2002). For a discussion on the difficulties in defining well-being, see Sandra Carlisle & Phil Hanlon, *Well-Being and Consumer Culture: A Different Kind of Public Health Problem?*, 22 HEALTH PROMOTION INT'L 261

from a sense of being continuously dissatisfied relative to individuals who own more, and from decreased social engagement, leading to a diminishment of one's sense of belonging.[157] In addition, since consumers who are making purchasing decisions on the basis of manipulative advertising are erroneously believing that the purchases will make them happier, they are also wasting their money. Finally, the continual intrusion into consumers lives in order to manipulate behaviour is in some ways an affront to our autonomy and dignity.[158]

Obviously, it is important to allow the flow of truthful information about lawful economic activities. A competitive, fair, and efficient economy requires access to product information.[159] However, we do not need invasive manipulative advertising to provide this information. In the digital information era, consumers have access to comprehensive product information by independently searching for it using a search engine and being directed to product descriptions, seller websites, product reviews, etc.

In contemplating a future where invasive manipulative advertising via AI-driven IoT is no longer tolerated, it is worth considering the possibility that new laws are not in fact needed, and instead the old laws just need to be interpreted more broadly. For example, in the United States, one might ask whether it would be possible for the FTC to treat the more extreme forms of manipulation via AI-driven IoT devices as "unfair" trade practices under Section 5 of the FTC Act.[160] Unfortunately, however, this would be challenging given that an advertisement or a business practice is only considered "unfair" under the Act if it causes or is likely to cause substantial consumer injury which a consumer could not reasonably avoid; and it is not outweighed by the benefit to consumers.[161] This harm requirement limits the FTC's authority. The harm caused by manipulative advertising is diffuse and hard to ascertain with precision. Terrell McSweeny, former Commissioner of the FTC, questions whether the FTC can adapt, within the scope of its current powers, to the growing

(2007). *See also* Leaf Van Boven & Thomas Gilovich, *To Do or to Have? That Is the Question*, 85 J. PERS. & SOC. PSYCH. 1193 (2003). This article argues that it is better to do than to have–experiences make people happier.

[157] Bauer et al., *supra* note 156 at 518.

[158] The idea of technology eroding human autonomy is examined in RUSHKOFF, *supra* note 149, at 63-94. He argues that while the technology industry's attack on human autonomy might not be conscious, it is nevertheless "reinforcing its users' role as passive consumers from whom to extract value." *Id.* at 53.

[159] Howard Beales et al., *The Efficient Regulation of Consumer Information*, 24 J.L. & ECON. 491, 492 (1981).

[160] The FTC has already given thought to using its unfairness authority to the practice of using AI in ways that leads to discriminatory outcomes, such as denying consumers credit or insurance. FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES, (Jan. 2016).

[161] 15 U.S.C. §45(n) (2006).

forces of technology in our daily lives.[162] She points out that aggressively using the FTC's unfairness authority, in an attempt to adapt, is easier said than done and that the agency is called on to defend even cautious expansions of its unfairness authority.[163]

One solution might be to enact federal legislation specifically dealing with IoT consumer manipulation. However, drafting a new law that protects consumers against manipulative marketing strategies will be challenging. The chief difficulty lies in the task of drawing a line between acceptable marketing that successfully persuades us to make a purchase, and unacceptable manipulative marketing that operates below the level of full awareness to herd us toward a behavior.

If one of the most worrying aspects of the future of IoT manipulative advertising is the persuasive power of the human voice and human mannerisms, then perhaps it is this aspect of IoTs that could be the focus for law reform. An extreme approach would be to ban the sale of consumer IoTs that have humanoid form. This way, we would at least avoid the dangers of a human-like robot living in our homes and manipulating us for commercial gain. We could still have the useful human-like functions in AI-driven IoT devices, without the need for the device to look and sound like a human. A non-anthropomorphic robot might speak in a monotone voice, have some movement capability, and help us with its AI intelligence. But ultra-realism would not be the goal. Such a ban would avoid the emotional confusion that human-like robots might cause: an emotional confusion that could be exploited for commercial gain. The essential question to ask ourselves is whether there is any good reason for an IoT device to appear human in form. If the answer is no, and the dangers of such creatures are not balanced out by the benefits, then a straightforward ban would be the simplest legal response. Perhaps there could be some exceptions to the ban for purposes such as the emotional care of the elderly.[164] Although we might want to think twice before even allowing this kind of exception given that a real human would seem preferable to a fake human.

The suggestion of a ban is, however, likely to be met with resistance. There might be concern that it would stifle innovation and

[162] Terrell McSweeny, *Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is the FTC Keeping Pace?*, 2 GEO. L. TECH. REV. 514, 517–19, 525 (2018).

[163] *Id.* at 525. McSweeny gives the example of the FTC's attempt in the late 1970s to regulate the advertising of sugary foods to children which was vehemently opposed by the food industry, advertisers, and broadcasters. The FTC was accused of being a "National Nanny" by the Washington Post. *The FTC as National Nanny*, WASH. POST, (Mar. 1, 1978), https://www.washingtonpost.com/archive/politics/1978/03/01/the-ftc-as-national-nanny/69f778f5-8407-4df0-b0e9-7f1f8e826b3b/.

[164] Although this exception would not be without its own set of challenges and ethical concerns. *See*, *e.g.*, Ipke Wachsmuth, *Robots Like Me: Challenges and Ethical Issues in Aged Care*, 9 FRONTIERS IN PSYCHOL. 1 (Apr. 2018).

limit the chances of developing useful versions of IoTs in human form.[165] Some might argue that owning any kind of IoT–whether human-like or not–is a human right. There are those who argue, for example, that human-robot friendships and love are entirely possible and that there should be freedom to own any kind of companion robot, including sex robots.[166] There are serious ethical and social implications surrounding the sex robot industry, none of which relate to consumer misinformation.[167] A full exploration of these issues is beyond the scope of this article. Nevertheless, the debate around sex robots highlights the thorny legal issues that surround attempts to limit the sale of robots.

A completely different approach to reducing the level of invasive manipulation from IoTs would be to require the providers of IoTs to offer consumers the option of a premium level of service which is free of commercial communication and is limited in its data extraction. Perhaps there could be several different levels of service on offer. If the IoT networks develop a subscription model, then there could be different subscriptions on offer, each with different terms of service. The options might range from free subscription IoTs (with wide ranging data collection, sale of data to third parties, and unlimited advertising) to mid-range subscriptions (with limited data extraction and agreed categories of personalised product recommendations) to expensive subscriptions (fully customisable with no data extraction besides what is necessary for the IoT to function, and no advertising of any kind). In other words, the law could require that IoT corporations give consumers the ability to opt-out of the advertising funding model and pay for a premium service.[168] Of course,

[165] David Hanson is a maker of humanlike robots and AI software. *See*, *e.g.*, David Hanson, *Why We Should Build Humanlike Robots*, IEEE SPECTRUM (Apr. 1, 2011, 6:48 PM), https://spectrum.ieee.org/automaton/robotics/humanoids/why-we-should-build-humanlike-robots (arguing that humanoid robots have practical applications and that developing them pushes the boundaries of biology, cognitive science, AI and engineering).

[166] DAVID NEIL LAURENCE LEVY, LOVE + SEX WITH ROBOTS: THE EVOLUTION OF HUMAN-ROBOT RELATIONS (2008).

[167] For a discussion on this topic, see John Danaher et al., *Should We Campaign Against Sex Robots?*, *in* ROBOT SEX 47 (John Danaher & Neil McArthur eds., 2017). There is a United States ban on the sale of child sex robots. *See* Curbing Realistic Exploitative Electronic Pedophilic Robots (CREEPER) Act, H.R. 4655, 115th Cong. (2017). *See also* the campaign against sex robots organized by Kathleen Richardson, UK Professor of Ethics and Culture of robots and AI. Kathleen Richardson, *About*, CAMPAIGN AGAINST SEX ROBOTS, https://campaignagainstsexrobots.org/# (last visited Mar. 15, 2021). *See also* Jenny Kleeman, *The Race to Build the World's First Sex Robot*, THE GUARDIAN (Apr. 27, 2017, 12:30 AM), https://www.theguardian.com/technology/2017/apr/27/race-to-build-world-first-sex-robot.

[168] The idea of the state protecting consumers from unwanted marketing is not entirely new–indeed in the United States, the Do Not Call Registry was set up to allow consumers a legal right to opt-out of intrusive telemarketing. FED. TRADE COMM'N,

this approach might be criticized for creating a world of second-class citizens further exploited and manipulated by IoTs, while the rich pay for peace and autonomy. But this is the model that is becoming more popular in the current online world with services such as Spotify and Netflix. It has the advantage of putting the brakes on the entire IoT environment being dragged down by ads and trackers.

No doubt some readers will be thinking that if consumers are so concerned about having these premium service options, then the free-market will provide them without the need for legal intervention. The profit motive should drive each IoT corporation to provide the products that consumers want to buy. If consumers want a product with a choice of service terms then that is what the market will provide. However, while this might turn out to be the case, it equally might not happen. The difficulty with the "the free-market will sort it out" argument is that in the tech-world there does not seem to be sufficient competition to incentivise the dominant players to move away from the big-data advertising model. If the IoT industry follows this path, whereby the power accumulates in one company, then regulation might be necessary to offer some protection to consumers.

3. Summary. – In summary, there are many things to fear in a world of pervasive powerful manipulative advertising via IoTs. There might come a time when we no longer accept the premise that being manipulated is an acceptable element of capitalism. Lawmakers who review the regulation of IoT commercial communications will need to grapple with the broad policy questions about freedom and manipulation. They will need to consider the desirability of expanding the law to restrict at least some forms of manipulative advertising. The key question will be whether it is acceptable to use the extraordinary power of technology as a manipulation tool with the intention of interfering with another person's decision-making so as to push it toward a commercial profit. Unlike autonomous vehicles, which use AI to improve the safety of the driving experience, the use of AI for IoT advertising has a less societally beneficial aim. Safe cars are good for everyone, manipulative advertising is good for corporations selling products, but it is debateable whether it is an unequivocal public good.

V. THE "HOW" QUESTION

The preceding sections have considered the "who" and "what" issues of who *can* be held liable for consumer misinformation, who *should* be held liable for consumer misinformation, and what kinds of misinformation should be prohibited in a future of ubiquitous IoT devices powered by AI. Admittedly, the analysis has in some senses already strayed into the territory of "how" in so far as it has suggested options for

National Do Not Call Registry – Telemarketer, https://telemarketing.donotcall.gov/ (last visited Mar. 15, 2021).

"how" to reframe the law to respond to the "who" and "what" questions. For example, it explored options for holding the creators of AI responsible, and options for reform that would tackle invasive manipulation. This part of the article moves on to briefly consider broader and more general "how" questions in relation to how to successfully implement any re-designed laws. For example, how do we ensure that new laws are enforced, how can we create incentives for compliance, and how do we approach the global nature of these problems?

A. Resources

The first factor to consider is increasing the resources devoted to the task. As we have seen, the opportunity to communicate directly with consumers dramatically increases in an IoT future, and so too does the risk of consumer misinformation and manipulation. It will be impossible to effectively monitor and control any of this communication without a corresponding increase in watchdog resourcing. Consumer protection enforcement agencies around the world already face serious challenges in protecting consumers from fraudulent and deceptive commercial practices due to insufficient resources.[169]

In the Unites States, the FTC is tasked with protecting consumers by stopping unfair, deceptive, or fraudulent practices in the marketplace. It receives a level of funding that has not significantly changed in a decade and FTC records indicate it has around 600 fewer workers than it had four decades earlier.[170] And yet, the workload of the FTC has substantially expanded as the internet revolution has required the FTC to respond to new consumer threats such as online scams, data privacy, and deceptively formatted online advertising. The IoT revolution will bring with it further challenges for the agency. The FTC, like other consumer protection agencies around the world, is morphing

[169] ORG. FOR ECON. CO-OPERATION & DEV., CONSUMER PROTECTION ENFORCEMENT IN A GLOBAL DIGITAL MARKETPLACE, OECD DIGITAL ECONOMY PAPERS NO. 266 (April 2018). This report identifies insufficient resources as the key constraint for consumer protection agencies attempting to control fraudulent and deceptive commercial practices in a global marketplace. *Id.* at 42.

[170] FED. TRADE COMM'N, *FTC Appropriation and Full-Time Equivalent (FTE) History*, https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation (last visited Mar. 15, 2021). The records indicate that the funding level has increased by 13% since 2010, from 292 million to 331 million dollars in 2020.

into the prime regulator of the technology industry.[171] This is a daunting task and cannot be undertaken without significant funding increases.[172]

One of the biggest challenges for enforcement agencies in an IoT era will be the increasingly difficult task of detecting the misinformation. If there are funding constraints, it is natural that the breaches that receive attention are those where there are several consumer complaints. However, relying on complaints to set in motion investigative and enforcement procedures is unsatisfactory in the arena of misinformation offences. This is so because in many instances the consumer may have no idea that they have been misled. Moreover, even if a consumer is aware that they have been misled, they are often reluctant to take the time to complain if the harm to them individually is small, even though the aggregate harm across all consumers might be large.[173] A system that only picks up on breaches in this haphazard manner will lead to repeated violations that go unchecked. An increase in funding would allow agencies to engage in more active, independent methods of investigation to pick up on breaches of the law. It would also allow continued consumer education efforts to increase awareness about AI, IoT advertising, deception, and manipulation.

However, an increase in funding will not completely solve the problem of regulating information offences in an IoT future, because of the particularized way that the information will enter private spaces. If the commercial messages are being delivered directly to consumers' ears via IoT devices in a uniquely individualized way, it will be challenging for regulatory agencies to conduct meaningful scrutiny.[174] The relevant agencies will need more than just extra funding. They will need an increase in technological expertise, and a focus on understanding and actively monitoring the advances in IoT technology, which brings us to the next element needed in the regulatory toolkit.

[171] Tony Romm, *The Agency in Charge of Policing Facebook and Google Is 103 Years Old. Can It Modernize?*, WASH. POST (May 5, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/04/can-facebook-and-googles-new-federal-watchdogs-regulate-tech/.

[172] McSweeny, *supra* note 162.

[173] *See* Meirav Furth-Matzkin & Roseanna Sommers, *Consumer Psychology and the Problem of Fine-Print Fraud*, 72 STAN. L. REV. 503 (2020) (arguing that one reason that consumers of fraud do not complain is that they assume that all contracts, even those induced by fraud, are binding.) The more general idea that only a small number of grievances ever mature into disputes is discussed in Felstiner et al., *supra* note 114.

[174] *See* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 242 (2019) (discussing the challenges of regulating "information of an astonishing variety, granularity and intimacy" intermediated by privately owned communication platforms).

B. Technological Expertise

In order to successfully regulate the IoT commercial communications of the future, regulatory agencies will need to employ technical experts in addition to legal experts. The dominant corporations of the IoT industry will attract the most qualified technological experts with financial renumerations that government-funded agencies do not currently match.[175] These corporations will consequently have a capacity for massive data-processing and elaborate AI-driven communications.

Successful regulatory agencies of the future will need the resources to employ staff with the technological expertise to undertake robust analysis of the various approaches used by these commercial entities. Expertise will also be needed to investigate technological developments that can counteract or detect wrongs. The most effective approach might be to develop a regulatory framework where technology corporations are required to work with public enforcement bodies. Under this kind of regulatory framework, corporations would be required to be more transparent about their technology, and where possible to provide insights into how their AI decision-making systems work, flag misinformation (if not remove it), share concerns about suspected misinformation with the public enforcement body and engage in developing technological solutions to the problem of misinformation. A recent UK Government report dealing with all forms of online harm, including harm caused by misinformation proposes just this kind of approach.[176] It recommends that a new statutory duty of care be imposed on technology corporations towards their users. This duty of care would be enforced by an independent regulator that would have the power to require technological transparency and proactive use of technological tools to identify, flag, block or remove illegal or harmful content.[177]

If policymakers determine that it is desirable to stem not only misleading information, but also to reduce aggressive manipulation, then the importance of technological expertise becomes an even more important part of the regulatory toolkit. New policy units that are well-informed about modern technology could be established to investigate

[175] The supply of AI talent is in short supply and "with the likes of Facebook and Google vying for top-notch talent, recruiting efforts can prove incredibly challenging." Falon Fatemi, *How to Win the War for AI Talent*, FORBES (Nov. 18, 2019, 10:47 AM), https://www.forbes.com/sites/falonfatemi/2019/11/18/how-to-win-the-war-for-ai-talent/#73f24ccc7a5b.

[176] *See* HOME DEPARTMENT, ONLINE HARMS WHITE PAPER, April 2019, CP 57 (UK). The UK government recently published a full response to the paper. *See* Rachael Astin, Gail Crawford, Katie Henshall & Alain Traill, *UK Government Publishes Full Response to Online Harms White Paper*, JD SUPRA (Feb. 24, 2021), https://www.jdsupra.com/legalnews/uk-government-publishes-full-response-2380339/.

[177] *See id.* at 44.

how these manipulative practices work and how they might be controlled. The FTC has already begun work in this area and further research is needed.[178] Without a willingness to examine the entire enterprise, there is a danger that a mass surveillance network of IoT devices designed to manipulate consumer behaviour will grow without any effective legal limits.

C. Deterrence

Effective regulation also requires hefty penalties for breach in order to improve the deterrent effect of the rules. If the penalty for breach is far lower than the profits of the behaviour then there is little incentive for companies to review practices and avoid illegal behaviour. Of course the variety of legal reforms suggested in this article means that it is difficult to make specific recommendations about the level of penalties here. The general point, however, remains important: that the penalties need to be high enough to offset the economic incentives to behave illegally. Given that there is a high cost involved in monitoring all the information flowing in an IoT network, a penalty system that deters the behaviour in the first place makes sense.

Historically, the fines imposed by the FTC have been relatively low and the most common enforcement tool has been the cease and desist order. The deterrent efficacy of this approach may be limited. However, in July 2019 the FTC imposed a historically high penalty on Facebook for misleading consumers about their privacy settings by its practice of giving third-party developers access to affected friends' data.[179] The 5 billion US dollar penalty was twenty times greater than the largest privacy or data security penalty ever imposed worldwide.[180] It is pertinent that the chairman of the FTC, Joe Simmons, explains that magnitude of the penalty was "designed not only to punish future violations but, more importantly, to change Facebook's entire privacy culture to decrease the likelihood of continued violations."[181] Critics, however, claim that the fine still was not nearly high enough, and for a company worth as much as Facebook, it will

[178] FED. TRADE COMM'N, *Data Brokers: A Call for Transparency and Accountability* (May 2014).

[179] *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FED. TRADE COMM'N, (Jul. 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

[180] *Id.*

[181] *Id.*

have had little impact.[182] In 2019 Facebook made over 70 billion dollars in revenue.[183]

D. Global Solutions

One more factor that needs to be taken into account in any reframing of legal regimes is the global nature of the marketplace. It is therefore worth exploring legal efforts to protect consumers that are more internationalized.[184] Achieving global regulatory consistency is of course very difficult and cross-border enforceability is a real challenge. Nevertheless, it is a worthy and important goal to pursue.

The alternative approach is to encourage each country to regulate IoT in its own way without global co-operation. In other words, to enter into a regulatory competition.[185] Such competition would allow each country to try to create rules that appeal to its citizens (to both consumers and industry). I would argue that consumer protection law is not an area of law that is well-suited to regulatory competition. The danger is that it devolves into a race to the bottom as each nation aims to tempt IoT development with the lure of a lack of regulation.[186] The better approach is to work together to achieve a global marketplace where consumers can trust the IoT industry to be truthful and act ethically.

As Yuval Harari argues in his book, "[g]lobal problems need global solutions."[187] Many advertisers market to a global audience and all the giant tech companies operate across the globe. If legal expectations and frameworks are fragmented, with different expectations in different countries, then confusion abounds. For some time there has been a trend

[182] Matt Stoller, a fellow at the Open Markets Institute, called the penalty a mere "parking ticket." Julia Carrie Wong, *Facebook to Be Fined $5bn for Cambridge Analytica Privacy Violations - Reports*, THE GUARDIAN (Jul. 12, 2019, 6:12 AM), http://www.theguardian.com/technology/2019/jul/12/facebook-fine-ftc-privacy-violations.

[183] *Facebook's Annual Revenue from 2009 to 2019*, STATISTA, https://www.statista.com/statistics/268604/annual-revenue-of-facebook/ (last visited Mar. 15, 2021).

[184] MATEJA DUROVIC & HANS W. MICKLITZ, INTERNATIONALIZATION OF CONSUMER LAW: A GAME CHANGER (2017).

[185] For an in-depth philosophical critique of regulatory competition theory, see JOHANNA STARK, LAW FOR SALE: A PHILOSOPHICAL CRITIQUE OF REGULATORY COMPETITION (2019) (arguing that regulatory theory is problematic from the perspective of both political theory and philosophy).

[186] The phrase "race for the bottom" in relation to regulatory competition was coined by William Cary. *See* William L. Cary, *Federalism and Corporate Law: Reflections Upon Delaware*, 83 YALE L.J. 663, 666 (1974).

[187] YUVAL HARARI, 21 LESSONS FOR THE 21ST CENTURY, *supra* note 147 at 125–26. Harari makes the point that we now live in a global economy where nations are no longer the right framework to manage many of the challenges of the age. He argues that we need to globalize our politics.

towards aiming for more globally consistent law in the area of consumer protection. For example, in 2007 OECD countries agreed to a framework for cooperation and consistency of privacy law enforcement.[188] More recently, the 2018 OECD report *Consumer Protection Enforcement in a Global Digital Marketplace* points out that consumer issues will increasingly entail an international dimension and consumer protection enforcement co-operation across borders will be an essential element for effectively addressing these challenges.[189]

CONCLUSION

The regulatory systems we have in place are based on increasingly outdated notions of how advertising and commercial communication take place. In the age of IoT, advertising will expand far beyond the old forms. The new methods of advertising will not be something we choose to interact with or even avoid. It may not even seem like advertising. In fact, it could become a soundscape that continually interacts with us and everything around us. A world of networked IoT technologies is likely to radically expand the horizon of possibilities for sellers to communicate with consumers. The communication could become frictionless, around the clock, and highly individualized. The IoT network will allow for a continual collection of data, which along with AI analysis, can be used to ensure that marketing messages have the power to manipulate consumer behavior in order to improve sales outcomes. The persuasiveness of these marketing messages is likely to be heightened if future robot personal assistants and companions are developed to have human-like mannerisms and respond to us with emotional fluency. This future version of an IoT device might develop the ability to hijack the intuitive part of our brain and nudge us at an emotional and behavioural level.

Legal systems will need to adapt to these developments in order to maintain control of misleading or deceptive commercial speech. Truth is a cornerstone of a fair and efficient market-place. The dangers of not adapting are disconcerting. Governments will also need to grapple with the wider question of whether the law should be used to keep us safe from aggressively manipulative commercial communication. Without some legal controls, we might end up in a future where we are subjected to the manipulating forces of commerce in almost every waking moment.

Redesigning legal regimes to effectively battle this new world will no doubt be a challenge. Any meaningful change will require lawmakers to first confront the fact that there are genuinely difficult problems for which existing regulatory toolkits are ill-equipped to handle. The first step in the work of improving laws is to understand where the problems lie. This article has set out some of the ways in which current laws are at

[188] ORGANISATION FOR ECON. CO-OPERATION & DEV., OECD RECOMMENDATION ON CROSS-BORDER CO-OPERATION IN THE ENFORCEMENT OF LAWS PROTECTING PRIVACY (Jan. 2007).

[189] ORG. FOR ECON. CO-OPERATION & DEV., *supra* note 169.

their weakest in their capacity to deal with the future of advertising in an IoT environment. It has also set out some of the ways forward. Now is the time to begin to a conversation about how to develop new global consumer laws in readiness for the IoT revolution ahead. Lawmakers engaged in this task will need to consider the "who," "what," and "how" questions in order to create legal systems able to effectively protect consumers in an IoT future.