DePaul Law Review

Volume 70
Issue 3 *Spring 2021*

Article 3

Personalization of Smart-Devices: Between Users, Operators, and Prime-Operators

Tomer Kenneth

PERSONALIZATION OF SMART-DEVICES: BETWEEN USERS, OPERATORS, AND PRIME-OPERATORS

*Tomer Kenneth**

Your relationships with smart-devices are about to get complicated. The ability to operate the physical functions of smart-devices from far away introduces new actors into the previously intimate relationship between the user and the device—the operators. The Internet of Things (IOT) also facilitates more complexed and nuanced use of smart-devices, most notably enabling the personalization of a specific device for a specific user. Together, remote operability and personalization of smart-devices bring forth a myriad of legal and social opportunities and challenges.

The Article explains the nature of personalization of smart-devices and teases out its significant implications. Personalization of smart-devices combines the dynamic personalization of code with the influential personalization of physical space, making it easy for operators to remotely modify the smart-device and influence specific users' behaviors. Crucially, personalization of smart-devices can affect the creation and enforcement of law: it facilitates the application of law on spaces and activities that were previously unreachable, thereby also pushing toward the way for legalization of previously unregulated spaces and activities.

The Article also distinguishes between two kinds of smart-devices operators: ordinary and prime-operators. The Article illustrates the challenges that ordinary operators bring forth by identifying different kinds of ordinary operators (users, private companies, and the state) and modes of constraints they can impose on users (notice, nudge, and prevention). It then normatively discusses the distribution of first-order and second-order legal powers between ordinary operators.

* Doctoral (J.S.D.) Candidate, New York University School of Law; Fellow, Information Law Institute, NYU. I thank Thomas Streinz, Anat Lior, Roy Cohen, Alma Diamond, Meir Yarom, and James Wilson for invaluable discussions comments on earlier versions. I am also grateful to the participants of the Yale Law School's 9th Annual Doctoral Scholarship Conference, the participants of the Privacy Research Group at NYU School of Law, and the participants of the 15th Cornell Law School Inter-University Graduate Conference, for their helpful feedback. Finally, I thank also Susan John and the law review editors for their careful editorial work.

Finally, the Article introduces the prime-operators of smart-devices. Prime-operators have informational, computational, and economic advantages that uniquely enable them to influence millions of devices and extract considerable social value from the operation of smart-devices. Prime-operators also hold unique moderating powers—they govern how different operators and users operate the smart-devices and thereby influence interactions mediated by smart-devices. The Article discusses the nature and role of prime-operators and explores paths to regulate them.

INTRODUCTION

Technological innovations turn traditional devices into smart-devices, which are digitally operated and connected to the internet.[1] Combining these two features facilitates remote operability of smart-devices, empowering operators—users and other actors—to operate the devices' functions without being in the same space and time as the device itself. In turn, remote operability introduces new actors to the previously intimate relationship between the user and the device.

The Article will use the smart-fridge as a prime example to explore the exciting possibilities and thorny challenges that smart-devices bring forth. Smart-fridges' innovative technologies facilitate various functions that traditional fridges do not. These include the digital operation of the traditional functions of the fridge, e.g., temperature setting or opening doors; various sensors that collect information from inside the fridge and its surroundings, e.g., noticing when the tomatoes rot and identifying users approaching the device; connection to personal assistants' services such as Alexa or Google Assistant, e.g., to simplify the creation of shopping lists or to find recipes according to the products in the fridge; and a connection to other internet services, e.g., social media accounts or shopping websites.[2]

Admittedly, that smart-fridges have built-in computers, sensors, or even small screens that provide various information about the device, is not likely to leave anyone with a smartphone flabbergasted. However, understanding remote operability might. It allows various operators to make the smart-fridge in the users' kitchen perform actions that affect the user without ever stepping into the kitchen. It empowers those operators to determine when the doors will be open or closed, what temperature to set for the dairy compartment, how to

1. In this article the phrase "traditional device" denotes the device that used for similar core functions without the internet connectivity of the respective smart-device. For instance, traditional fridges whose functions included cooling, thermostat control, door level, and sometime basic digital capabilities to control these functions. The relation between smart-devices and traditional devices derives from them being the same "thing" as far as the user is concerned. Michael J. Madison, *Law as Design: Objects, Concepts, and Digital Things*, 56 CASE W. RES. L. REV. 381, 389–404, 447–63 (2005) (discussing what makes a physical "thing" in law, and the expectations towards tangible things).

2. *See e.g.*, James Stables, *Chill out, it's our smart fridge buying guide*, THE AMBIENT (Jan. 11, 2019), https://www.the-ambient.com/reviews/best-smart-fridges-356; Adrian Willings, *New Alexa devices from CES 2019: AI-powered TVs, fridges, mirrors and more*, POCKET-LINT (Jan. 14, 2019), https://www.pocket-lint.com/smart-home/news/amazon/143246-the-best-new-alexa-devices-ai-powered-tvs-fridges-mirrors-and-more; Renée Lynn Midrack, *What Is a Smart Refrigerator?*, LIFEWIRE (Nov. 14, 2019), https://www.lifewire.com/smart-refrigerator-4158327; Kari Paul, *Teen claims to tweet from her smart fridge – but did she really?*, THE GUARDIAN (Aug. 13, 2019, 6:48 PM), https://www.theguardian.com/technology/2019/aug/13/teen-smart-fridge-twitter-grounded.

organize the products in the fridge, or when the beer compartment will be locked.[3]

This article will explore operators' power to personalize the use of smart-devices, and the various legal challenges that this innovative power brings to the fore. Smart-devices often celebrate their operators' ability to "personalize" these devices.[4] As we shall see, personalization refers to physically modifying the features of the smart-devices to prompt specific users to act in a specific way.[5] This is a unique, innovative, and influential feature of smart-devices. It invites operators to impose finer and more nuanced constraints on particular users, thereby pushing specific users to particular outcomes, outcomes set by the operators for those specific users.[6] As smart-devices become more abundant and the effects of personalization on users will accentuate, scholarly attention and legal responses will be required.[7]

This Article contributes to the existing literature by developing three main ideas. First, it provides a comprehensive account of personalization in the context of smart-devices, analyzing the concept and exploring the development of innovative personalized legal and market regulations that rely on this technology.[8] Second, it casts a spotlight on the new actors—the operators of smart-devices—and the changing relationships between users and their devices.[9]

Third, it singles out the *prime-operators*, specific operators that hold considerable powers regarding the operation of smart-devices.[10] Despite escaping scholarly debates so far, prime-operators are important. They have informational, computational, and economic advantages

3. *Id*.

4. The centrality of personalization can be hinted by the prominence of this function in smart-fridges ads. *See, e.g.*, *New Food AI Looks Inside Your Fridge To Help You Find The Perfect Things To Cook With What You ALREADY Have*, SAMSUNG NEWSROOM, https://news.samsung.com/us/new-food-ai-looks-inside-fridge-help-find-perfect-things-cook-already/ (last visited July 11, 2021) (featuring "personalized cooking experiences" and "personalized food recommendations"); *The Smarter Kitchen*, SMARTFRIDGE, http://smartfridge.io/ (last visited July 11, 2021) (featuring "personalized food manager features" and "personalized grocery lists"); *Home is where the Hub is*, SAMSUNG, https://www.samsung.com/us/explore/family-hub-refrigerator/overview/ (last visited July 11, 2021).

5. *See infra* Part II.B.

6. *See infra* Part II.C.1; *supra* note 4.

7. On the expected prevalence of smart-devices see, e.g., Paolo Collela, *Ushering In A Better Connected Future*, ERICSSON, https://www.ericsson.com/en/about-us/company-facts/ericsson-worldwide/india/authored-articles/ushering-in-a-better-connected-future (last visited July 11, 2021) (predicting roughly 30 billion IoT devices by 2022); *A Guide to the Internet of Things*, INTEL (Apr. 3, 2016), https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html (predicting roughly 200 billion IoT devices by 2020).

8. *See infra* Part II.

9. *See infra* Part III.

10. *See infra* Part IV.

that enable only these types of operators to extract considerable social value from the operation of smart-devices.[11] Prime-operators also hold unique moderating powers, enabling them to favor certain operators over others.[12] The Article will argue that prime-operators of smart-devices create legal challenges that resemble those posed by social media moderators and set the foundations for the regulatory and scholarly discussion about prime-operators.[13]

Part I provides a primer to the technology of smart-devices, explains how its core features facilitate remote operation, and presents the key opportunities and challenges that this technology holds. Part II focuses on personalization as a unique feature of smart-devices. It expounds upon the concept, explains the technological background, and then illustrates how personalization of smart-devices poses new possibilities for personalized legal and market constraints.

Part III is dedicated to personalization by ordinary operators. It illustrates and assesses the normative harms that ordinary operators might pose, namely by combining the types of operators and methods of constraints they could apply. It then discusses the adequate distribution of first-order and second-order legal powers to operate smart-devices. Part IV introduces the prime-operators. It explains the origin of their power, underscores the unique legal challenges that they pose, and suggests a legal path to regulating them. The Article concludes with a set of considerations about the scholarship and regulation of smart-devices.

I. Preface to Smart-Devices

A. From Traditional to Smart

Smart-devices and the Internet of Things (IoT) are notoriously tricky to define.[14] Instead of grappling with a definitive definition for this emerging technology, I shall discuss the crucial features that set

11. *See infra* Part IV.A.

12. *See infra* Part IV.B

13. *See infra* Part IV.C.

14. *See, e.g.*, Hillary Brill & Scott Jones, *Little Things and Big Challenges: Information Privacy and the Internet of Things*, 66 Am. U. L. Rev. 1183, 1186–88 (2017); Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 Cal. L. Rev. 805, 823–25 (2016). The California legislature referred to smart-devices as "connected devices" and defined them as "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address." *See* Cal. Civ. Code § 1798.91.05 (West 2018). Some early references to IoT include, see generally The Internet of Things, Int'l Telecomm. Union (2005); Kevin Werbach, *Sensors and Sensibilities*, 28 Cardozo L. Rev. 2321 (2007).

smart-devices apart from traditional ones.[15] Briefly, these two features are the digitization of smart-devices' functions and interconnectivity. Together, they enable the computers embedded in smart-devices to (1) operate (execute actions regarding) the various digitized functions of the device, and (2) connect to the Internet in order to send information and receive commands.[16] These features facilitate other important characteristics, such as multifunctionality, scalability, and remote operability. Arguably, these elements also make a smart-fridge part of the IoT.[17] Allow me to elaborate.

To begin, consider the *digitization* of the devices' functions. Most traditional fridges include both analog and digital functions. The former include the leg-lever used to open the door, the ice trays, or the drawers that could be manually opened, closed, or locked; the latter include the inner computer that regulates the temperature or notifies when the door is left open.[18] Improvements in computer technology facilitate the creation of better computers that can be embedded in mundane devices.[19] These enhanced abilities facilitate the digitization of most of the devices' functions, as well as adding innovative func-

15. I find this approach especially appealing, in light of the early stage of this technology and its numerous unknown future implications on social lives. Here, I follow the footsteps of Justice Frankfurter's holding in *Northwest Airlines, Inc. v. Minnesota*: "[T]he still more subtle and complicated technological facilities that are on the horizon, raises questions that we ought not to anticipate; certainly we ought not to embarrass the future by judicial answers which at best can deal only in a truncated way with problems sufficiently difficult even for legislative statesmanship." 322 U.S. 292, 300 (1944).

16. Thus, to be regarded as a smart-device, a device does not have to constantly use its sensors to collect information nor keep a permanent link with the server. *Cf.* 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, 894–95 (2017).

17. *See, e.g.*, ERIC A. FISCHER, CONG. RES. SERV. R44227, THE INTERNET OF THINGS: FREQUENTLY ASKED QUESTIONS 1–2 (2015). The definition of IoT and the relation between smart-devices and IoT is a complicated issue which will not be fully addressed in the article. *See, e.g.*, Manuel Silverio-Fernández et al., *What is a smart device? - a conceptualisation within the paradigm of the internet of things*, 6 VISUALIZATION IN ENG'G 1 (2018); Menachem Domb, *Smart Home Systems Based on Internet of Things*, *in* INTERNET OF THINGS (IOT) FOR AUTOMATED AND SMART APPLIANCES (2019).

18. The distinction between digital systems and analog systems and their different legal applications were discussed in the context of art and copyright, see, e.g., Jeremy Paul Sirota, *Analog to Digital: Harnessing Peer Computing*, 55 HASTINGS L.J. 759, 760–61 (2004); James Grimmelmann, *There's No Such Thing as a Computer-Authored Work — And It's a Good Thing, Too*, 39 COLUM. J.L. & ARTS 403, 404 (2016); Brian Sheridan, *The Age of Forgotten Innocence: The Dangers of Applying Analog Restrictions to Innocent Infringement in the Digital Era*, 80 FORDHAM L. REV. 1453, 1465–69, 1478–81 (2011).

19. For a more nuanced explanation on the computing scheme that supports IoT, see Sona R. Makker, *Overcoming "Foggy" Notions of Privacy: How Data Minimization Will Enable Privacy in the Internet of Things*, 85 UMKC L. REV. 895, 897–98, 900–03 (2017); Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security*, 31 BERKELEY TECH. L.J. 997, 1007 (2016).

tions that traditional devices did not provide.[20] The newly digitized functions include digitally opening or closing the doors or the internal compartments, operating ice dispensers, setting temperature, and notifying about issues like dirty filters.[21] The innovative functions include various sensors that collect information about the smart-fridge and its surroundings, including cameras that record both the inside and outside of the fridge, or heat and humidity sensors that monitor different compartments.[22]

Second, technological developments also support the devices' *interconnectivity*.[23] That is, the ability of the computer embedded in the smart-device to communicate with and connect to other computers via the Internet.[24] While communicating online, each smart-device has its own identifier, meaning its own "Internet identity" and "address," which allows other computers connected to the Internet to find and communicate with it.[25] This way, the computer embedded in the smart-device exchanges information and commands with other computers connected to the Internet.[26]

---

20. *See* Peter Swire & Jesse Woo, *Privacy and Cybersecurity Lessons at the Intersection of the Internet of Things and Police Body-Worn Cameras*, 96 N.C. L. REV. 1475, 1479–83 (2018) (explaining that alongside the computational powers of the computers of the devices, other computational improvements such as cloud computing are in order to facilitate the IoT); GAURAV TANEJA ET AL., FUTURE OF IOT 13–14 (2019) (holding that the development of IoT technology and especially its large-scale spread depend on the computing powers in the devices themselves, known as "edge-computing" or "fog-computing").

21. *See supra* note 2.

22. Makker, *supra* note 19, at 897–98, 904–06; Poudel, *supra* note 19, at 1003 ("Sensors, such as cameras, thermometers, and pedometers, lie at the heart of an IoT system. These collect varied information about the environment, such as mechanical data . . . [and] thermal data . . . Sensors can work with actuators, output devices that implement decisions . . . [and] can also combine to form useful applications.").

23. On the key role of interconnectivity and smart-devices' ability to communicate as essential to IoT, see, e.g., FTC STAFF REPORT, INTERNET OF THINGS 5–6 (2015); Laura DeNardis & Mark Raymond, *The Internet of Things as a Global Policy Frontier*, 51 U.C. DAVIS L. REV. 475, 477 (2017); Vedang Ratan Vatsa & Gopal Singh, *A Literature Review on Internet of Things (IoT)*, 2 INT'L J. COMPUT. SYS. 355, 356 (2015) ("What we mean by interconnectivity is the potential various interconnections that can be made and the information can be imparted between all objects of the IoT.").

24. *See* Vatsa & Singh, *supra* note 23. On the role of interconnectivity in IoT, see, e.g., Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 554–60 (2017); Ian Taylor Logan, *For sale: Window to the Soul Eye Tracking as the Impetus for Federal Biometric Data Protection*, 123 PENN ST. L. REV. 779, 786–87 (2019); Ronald J. Hedges & Kevin F. Ryan, *The Internet of Things*, 90 N.Y. ST. BAR ASS'N J. 30 (2018).

25. *See, e.g.*, FISCHER, *supra* note 17, at 2–3; Harris Aftab, *Analysis of identifiers in IoT platforms*, 6 DIG. COMMC'NS & NETWORKS 334, 334 (2020).

26. Technically speaking, the smart-fridge usually operates as a client, meaning that it receives commands from other computers over the internet called servers that are operated by other entities. More on servers and clients, see JAMES GRIMMELMANN, INTERNET LAW: CASES AND PROBLEMS 31–33 (8th ed. 2018). For additional background on the connection and communica-

Interconnectivity and digitization of functions work together to allow smart-fridges to perform tasks that traditional fridges cannot. One such task is gathering information. A smart-fridge can use its sensors to collect information and upload it to a server.[27] Sensors may collect information about the technical use of the fridge, such as measurements of the electricity consumption, the average temperature in different compartments, filters' status, and more.[28] These sensors, specifically the cameras, can also collect information about the users of the smart-fridge and the ways they use it.[29] This includes information about the different users' habits—tracking how often they insert products to the smart-fridge, how often they eat certain products, when they usually open the fridge, and even which products or features of the fridge they use at different times.[30]

Furthermore, the devices can also process the collected information and use it to make distinctions: either between different users that use the device or between different products stored in it.[31] In more elaborate cases, inferences like identifying users or products, or detecting features and patterns can be achieved.[32] These inferences can be conducted by the smart-device itself (i.e., "edge computing") or by other

---

tion between computers over the internet, see, e.g., Lawrence E. Evans, Jr., *Internet Overview*, 63 TEX. BAR J. 226 (2000); Gibran J. Peña-Porras, *Joinder Is Coming: Why Denying Swarm Joinder in BitTorrent Cases May Do More Harm Than Good*, 87 U. CIN. L. REV. 611, 619–21 (2018); Aric Jacover, *I Want My MP3!: Creating a Legal and Practical Scheme to Combat Copyright Infringement on Peer-to-Peer Internet Applications*, 90 GEO. L.J. 2207, 2213–14 (2002).

27. *See supra* notes 20–22.

28. These features are already available in some smart-fridges, see, e.g., the FlexZone Drawer smart-divider function and the adjustable shelves functions in some of Samsung's smart-fridges. SAMSUNG, https://www.samsung.com/us/home-appliances/refrigerators/4-door-flex/22-cu--ft--counter-depth-4-door-flex--with-21-5-in--connected-touch-screen-family-hub--refrigerator-rf22n9781sg-aa/ (last visited July 11, 2021).

29. *See* Poudel, *supra* note 19, at 1003–04; Jamie Lee Williams, *Privacy in the Age of the Internet of Things*, 41 HUM. RTS. 14, 14 (2016); Branden Ly, *Never Home Alone: Data Privacy Regulations for the Internet of Things*, 2017 U. ILL. J.L. TECH. & POL'Y 539, 541 (2017).

30. *See, e.g.*, Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 98–114 (2014) (discussing the various IoT sensors that collect information in different kinds of devices).

31. I use the term "processing" here for convenience, but the more accurate term would be "profiling," defined by the GDPR as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements." *See* 2016 O.J. (L 679) 119.

32. *See* Peppet, *supra* note 30, at 130 (discussing the identification process of IoT devices by cameras, and explaining that "sensor data capture such a rich picture of an individual, with so many related activities, that each individual in a sensor-based dataset is reasonably unique"); Nicholas D. Lane et al., *On the Feasibility of User De-Anonymization from Shared Mobile Sensor Data*, PHONESENSE, Nov. 6, 2012, at 1.

servers that have access to the smart-devices' gathered information (i.e., "cloud computing").[33]

Since interconnectivity allows smart-devices to perform various actions that were not possible in the traditional devices, some view smart-devices as multifunctional,[34] in the sense that they fulfill the traditional functions as well as many new ones. They can cool your products while also collecting data,[35] connecting to social media,[36] creating grocery lists,[37] and more. Moreover, interconnectivity theoretically allows endless connections between devices on the same network, which supports the scalability of smart-devices.[38] Smart-devices are scalable in two manners: the ability to add more digital functions and features to a single device, and the ability to cooperate with other devices to facilitate even more services.[39] This explains the potential of smart-devices technology to significantly expand—to increase the number of smart-devices and the complexity of their digitized functions, and thereby to influence more aspects of users' lives.[40]

More importantly for our purposes, combining interconnectivity and digitization also facilitates the remote operability of the smart-fridge.[41] Digitizing the smart-devices' functions enables different actors to physically operate these functions through computer code commands, and interconnectivity allows remote operators to send such commands to the smart-device via the Internet. Crucially, combining the two means that the operators' remote commands are translated to

33. *See supra* note 2.

34. Friedland, *supra* note 16, at 895 ("A key to understanding the devices within the IoT is that they are generally multifunctional, such that their form and function can be separated. In other words, they are physical devices with a separate digital function.").

35. *Id.*; Ferguson, supra note 14, at 818–23 (noting that the data collection feature is sometimes regarded as surveillance).

36. *See supra* note 2.

37. *Id*.

38. About scalability of the internet and related platforms, see Anisha Gupta et al., *Scalability in Internet of Things: Features, Techniques and Research Challenges*, 13 INT'L J. COMPUTATIONAL INTELLIGENCE RES. 1617, 1618 (2017). (discussing the scalability of IoT); Annemarie Bridy, *Is Online Copyright Enforcement Scalable?,* 13 VAND. J. ENT. & TECH. L. 695, 698 (2011) (discussing scalability of peer-to-peer platforms).

39. *See* Poudel, *supra* note 19, at 1003–08; OECD DIRECTORATE FOR SCI., TECH. & INNOVATION, THE INTERNET OF THINGS: SEIZING THE BENEFITS AND ADDRESSING THE CHALLENGES 9 (2016) (discussing the scalability of IoT's and its correlated potential as facilitating innovative technologies); On cooperation between smart-devices, see *infra* notes 61–63.

40. *See supra* note 7; *see infra* the text accompanying notes 61–63 for concrete examples.

41. Recently, Crootof discussed this feature extensively, calling it "remote interference." *See* Rebecca Crootof, *The Internet of Torts: Expanding Civil Liability Standards to Address Corporate Remote Interference*, 69 DUKE L.J. 583, 600 (2019).

physical actions executed by the device.[42] Such remote operation can be pre-programmed, making the smart-device act in a specific manner given a specific situation.[43] In turn, this means that operators can either activate the smart-devices in real-time or set instructions for the device to perform when certain conditions are met.[44]

Remote operability, the ability to remotely instigate physical changes to the smart-devices, is the single most important feature distinguishing smart-devices from traditional ones. To illustrate, imagine attempting to lock a fridge's door remotely: a traditional fridge would require stepping into the user's kitchen with a lock and a chain, whereas smart-fridge operators can achieve the same outcome by simply sending a few lines of code via the Internet.

Remote operability of smart-devices also has legal implications: two immediately come to mind. First, by allowing remote operability of the device, this technology introduces new actors to the relationship between the user and the device, namely the remote-operators. The technology empowers these actors to execute physical actions regarding the smart-device that is located in the users' homes, actions that previously required sending a person to that location. Second, as will be elaborated later remote operability also allows operators to modify the physical functions of the smart-devices and thus influence specific users' behavior—driving users to perform or refrain from actions in various ways.[45]

B. Opportunities and Challenges

The ability to remotely operate a smart-device is the technological background that facilitates most of the smart-fridges' attractive features.[46] It allows users to gain information about the content of the smart-fridge from far away—counting the number of yogurts left in the fridge, verifying the expiration date of the milk, or quickly allowing a user to get recipes based on the products inside.[47] It also allows users to close a door that was mistakenly left open, customize the temperatures of different parts, or lock the beer compartment

42. *See id.* at 595–96, 611; Ido Kilovaty, *Freedom to Hack*, 80 OHIO ST. L.J. 455, 472–73 (2019).

43. *See generally* Michal S. Gal, *Algorithmic Challenges to Autonomous Choice*, 25 MICH. TECH. L. REV. 59 (2018).

44. *See infra* Part II.B.

45. *See infra* the text accompanying notes 64, 72–75.

46. *See supra* note 2. On the advantages of smart devices generally, see Chris Jay Hoofnagle et al., *The Tethered Economy*, 87 GEO. WASH. L. REV. 783, 802–09 (2019).

47. *See supra* note 2.

before the children's house party.[48] The remote operability also allows other operators to monitor and notify about problems with the smart-fridge's features (for instance, that the filter needs to be replaced).[49] In addition, it allows operators to collect information and use it in order to refine the operation of the device and its related services, like optimizing energy consumption, creating a customized shopping list, or monitoring the freshness of products.[50]

While those features seem promising, remote operability of smart-devices is not inherently desirable. It is a tool in the hands of operators. It allows them to overcome space and time barriers to operate smart-devices' functions, as well as to mediate the relationships between smart-devices and users.[51] Setting aside possible software errors or malicious hackings, even the powers that "friendly"[52] operators hold may be used in unexpectedly harmful ways. As such, remote operability of smart-devices can be put to more or less socially desirable uses.[53]

To illustrate, consider operators' ability to remotely lock the smart-fridges' doors or some of its compartments to limit users' access. This feature can be used to prevent unwelcome guests from using the smart-fridge (or parts of it). For instance, consider shared workspaces or apartments in which multiple users use the same smart-fridge, but only specific users should be given access to some of its parts. This remote limitation operates similarly to a vending machine's limiting access only to customers that pay.

But operators can also limit users' access to the smart-fridge for more objectionable reasons. For one, operators could limit user's con-

48. These features are already available on some smart-fridges, for example, see the "Family Hub Fridge" by Samsung. SAMSUNG, https://www.samsung.com/us/home-appliances/refrigerators/4-door-french-door/28-cu--ft--4-door-french-door-refrigerator-with-21-5--connected-touch screen-family-hub--in-tuscan-stainless-steel-rf28r7551dt-aa/ (last visited July 11, 2021).

49. This service is celebrated by some smart-fridge producers, see Proactive Customer Care, LG, https://www.lg.com/us/discover/thinq/proactive-customer-support (last visited July 11, 2021) (This feature, operated by the seller allows users to "[g]et automatic diagnostic checks of newly installed appliances . . . [r]eceive alerts about possible maintenance issues before they even occur and get guidance on how to correct the issue for maximum efficiency and cost-savings . . . [and] [e]njoy detailed reports about appliance performance, notification history and current status.).

50. *See supra* note 2.

51. In that sense, smart-devices are not very different from other communication technologies, see Allen S. Hammond, *Reflections on the Myth of Icarus in the Age of Information*, 19 SANTA CLARA COMPUT. & HIGH TECH. L.J. 407, 415 (2003) ("Not only do we use our tools to mediate our relationship with the world, we use them to mediate our relationship with one another. This reliance on mediation is particularly evident in our use of communications technology.").

52. *See supra* note 26; *see supra* the text accompanying notes 149–50.

53. *See infra* note 220 and the accompanying text.

sumption based on any random criteria. Imagine the embarrassment when your guest, who already had two beers, approaches your kitchen in the middle of the game, reaching for the beer compartment only to be berated by the remote-operator for excessive drinking. Similarly, smart-fridge operators might limit underaged or unrecognized users from accessing the medicine compartment, thereby, for instance, limiting the babysitter from delivering medication to children they supervise. Even worse, more aggressive operators may use the smart-devices' limiting abilities to intentionally constrain other users—some might limit their spouse's ice cream consumption, while others might require ad-hoc approval for any treat, alcoholic beverage, or even essential dinner ingredients.[54]

The challenges posed by the remote operability of smart-devices are exacerbated by the kind of potential harm they impose. Since smart-devices operate digital functions that have physical consequences, they can also bring about physical harm.[55] The physical presence of these devices, especially combined with the vital functions that they ordinarily fulfill in our lives (e.g., nutrition or medicine in the case of smart-fridges, transportation in the case of smart-cars, etc.) translates misusing them to potential considerable physical harm.[56] So, while the problem of operators limiting users is not unique to smart-devices, its physical presence makes it particularly troubling. To illustrate, compare the harm of having one's running playlist deleted by a remote-operator as they are about to start a jog, to having a remote-operator limit access to the smart-fridge when one's blood sugar is low. Arguably, both hinder valued interests and can give rise to legal claims from the user against the operator, but the possible outcomes of the latter, namely the expected physical harm, make it more pressing.

These challenges of remote operability are broad and persistent. They cannot be brushed aside as merely false identification issues, to be remedied as technology hones.[57] That is mainly because these challenges arise especially when the identification of smart-devices works well, as the examples in previous paragraphs indicate. Moreover, these issues arise in a wide array of smart-devices, including smart-cars that enable remote operation of various aspects of car usage, such as limiting the speed for specific drivers for various reasons such as

54. *See infra* Part III.A.4–5.

55. *See, e.g.*, Crootof, *supra* note 41, at 587–88.

56. *Id.*

57. *See, e.g.*, Patrick Nelson, *How IoT devices can identify the people who use them*, NETWORK WORLD (Sept. 21, 2015, 8:31 AM), https://www.networkworld.com/article/2984805/how-iot-devices-can-identify-the-people-who-use-them.html; *see generally* Samera Batool et al., *Identification of Remote IoT Users Using Sensor Data Analytics*, *in* FOOD TOURISM IN ASIA 328–37 (2020).

age or gender;[58] or smart-modems that allow operators to remotely block Internet access from specific users, to specific websites, or at specific times, empowering operators with de-facto censorship abilities and correlating concerns.[59]

Furthermore, these challenges will only exacerbate as the scalability of IoT kicks in. As explained, no smart-device stands alone.[60] The operation of one smart-device regarding a specific user can be complemented by other smart-devices to impose more restrictive limitations.[61] For instance, a smart-toilet[62] could send the smart-fridge information about urine samples of the different users in the house, modifying the use of the smart-fridge accordingly.[63] More concretely, upon indication from the smart-toilet that Hanna is pregnant, the smart-fridge operators can impose limitations on Hanna, stopping her from consuming refrigerated alcohol or reaching for the leftover sushi, all before she even decides to take the pregnancy test.

The examples of misusing smart-fridges' remote operability surveyed above showcase operators' ability to limit users or at least modify users' possible enjoyment from smart-devices or some of their parts. Armed with the capability to operate the device in ways that only users with physical access could before, those operators complicate the relationships between the user and the smart device. Simply put, smart-device operators' suddenly gain power over the users.[64]

---

58. *See, e.g.*, European Commission Press Release, Road safety: Commission welcomes agreement on new EU rules to help save lives (Mar. 26, 2019).

59. AT&T recently started promoting parental control of smart-modems, which allow administrators to create users, block internet access, and schedule time restrictions for specific users, see *Use parental controls with Smart Home Manager*, AT&T, https://www.att.com/esupport/article.html#!/u-verse-high-speed-internet/KM1336815?gsi=7zteup (last visited July 11, 2021).

60. *See supra* notes 38–39.

61. Realistically, this concern would likely be materialized only by operators that have power over multiple smart-devices regarding the same person, those that operate all the smart-home devices, or sellers that sell multiple smart-devices. *See infra* Part IV.A.

62. *See* Bernard Marr, *Artificial Intelligence In Your Toilet. Yes, Really!*, FORBES (May 20, 2019, 12:23 AM), https://www.forbes.com/sites/bernardmarr/2019/05/20/artificially-intelligent-toilets-yes-they-are-here/#46bf4175626d; Kate Baggaley, *Here's how smart toilets of the future could protect your health*, NBC (Jan. 23, 2019, 9:45 AM), https://www.nbcnews.com/mach/science/heres-how-smart-toilets-future-could-protect-your-health-ncna961656.

63. *See supra* notes 34–39.

64. *See* Crootof, *supra* note 41, at 600–10; SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 293–99 (2019). *See* Gal, *supra* note 43, at 76–93 (discussing some of the autonomy deficits caused by algorithmic decision-making); Michal Lavi, *Evil Nudges*, 21 VAND. J. ENT. & TECH. L. 1, 18–19 (2018) (discussing how operators' nudging might change users' behavior).

* * *

This Part presented the emerging technology of smart-devices and underscored one crucial aspect: the remote operability of the devices' physical functions. This remote operability introduces additional actors to the relationship between the user and the device, namely the remote-operators, and allows those actors to limit users in ways that were until recently only imaginable. The rest of this Article will focus on a particular aspect of remote operation of smart-devices—operators' application of personalized policies on specific users.[65] As we shall see, this important phenomenon takes a unique form within the realm of smart-devices. It allows various operators to limit specific users in order to drive them to perform or refrain from performing specific actions. It thus raises a myriad of interesting legal queries that have not yet been discussed in legal scholarship about the regulation of smart-devices and their operators.[66]

II. Personalization – Specific Constraints on Specific Users

This Part will analyze the concept of personalization in the context of smart-devices' operation. It will define the concept of personalization, explain the technicalities of how operators personalize smart-devices, and explore the application of different personalized constraints using smart-devices.

A. Personalization Smart Devices

Earlier, I explained that remote operability of smart-devices empowers operators to control the devices' monitoring functions as well as to alter its physical functions.[67] As hinted, this allows operators to influence users by customizing the operation of the device.

Customization of smart-devices' operation often takes one of two forms: personalization or general optimization.[68] General optimization of the smart-devices refers to operating the digital functions of the smart-fridge for the benefit of all users indiscriminately, for instance, by enhancing energy efficiency.[69] Conversely, personalization refers to operating smart-devices differently per user, according to the

65. *See infra* Part II.

66. *See infra* Part III–IV.

67. *See supra* the text accompanying notes 27–33; *see supra* Part I.B.

68. *Cf.* Sofia Grafanaki, *Drowning In Big Data: Abundance Of Choice, Scarcity Of Attention And The Personalization Trap, A Case For Regulation*, 24 Rich. J.L. & Tech. 1, 20 (2017).

69. *Id.*

attributes and characteristics of a specific user.[70] Optimization is a process used by many devices, traditional and smart alike, while personalization is an innovative feature of smart-devices.[71]

In the smart-devices framework, I define personalization as the *limitations, adaptations, or modifications that operators of smart-devices apply, intended to facilitate, limit, or prompt a specific user to act in a specific way, based on information gathered on that specific user*.[72]

In other words, operators distinguish between different users and adapt the operation of the different functions of the smart-device for that specific user, limiting some options and allowing others, in order to reach a particular desired outcome.[73] This point is worth reiterating: by personalizing, operators remotely bring about physical changes to smart-devices in order to *drive users to alter their behavior*; to make users perform or refrain from performing physical actions that they would not have taken otherwise.[74] Scholars already noticed that for-profit companies might attempt to exploit these powers to gain eco-

70. *Id.*

71. As we shall see later, personalization also requires information that allows identifying the users, which traditional devices lack, see *infra*, notes 199–200 and accompanying text.

72. The definition is mine, but related ideas can be found in other literature. *Cf.* the notion of personalization as was discussed in the legal health scholarship: Mollie Roth, *The Warfarin Revised Package Insert: Is the Information in the Label "Too Thin"?*, 9 HOUS. J. HEALTH L. & POL'Y 279, 286–87 (2009) ("'[P]ersonalized medicine' is an umbrella term encompassing the idea that now information about a specific patient's genotype or gene expression profile may be used to even more closely tailor medical care to an individual's needs. Such information can be used to help stratify disease status, select between different medications, and tailor their dosage or provide a specific therapy for an individual's specific disease."); W. Nicholson Price II, *Black-Box Medicine*, 28 HARV. J.L. & TECH. 419, 425–30 (2015) ("Although there are many slightly varying definitions of personalized medicine, the heart of it is this: All patients are different, and treatment can and should be tailored to the individual patient to the extent possible."). Others use two different phrases to explain what I regard as the process of personalization: one is personalization, referring to understanding the specific desires of some individual; another is customization, referring to acting to fulfill these specific desires. *See, e.g.*, Phil Davis, *What is the Difference Between Personalization and Customization?*, TOWERDATA (Nov. 5, 2018), https://www.towerdata.com/blog/what-is-the-difference-between-personalization-and-customization.

73. Roth, *supra* note 72, at 286–87; Davis, *supra* note 72.

74. ZUBOFF, *supra* note 64, at 293–99. She referred to this call to action instigated by the operation of the smart-device, "actuation." *See also* Steve Woolgar, *Configuring the user: the case of usability trials*, *in* A SOCIOLOGY OF MONSTERS: ESSAYS ON POWER, TECHNOLOGY AND DOMINATION 58, 68–69 (John Law ed., 1991) (discussing how the context of technology limits users); Yochai Benkler, *Degrees of Freedom, Dimensions of Power*, 145 DÆDALUS J. AM. ACAD. ARTS & SCIS. 18, 23 (2016); JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 71 (2019) (explaining that the data driven companies "are designed to offer powerful, high-speed techniques for matching populations with particular strategies calibrated for surplus extraction. The techniques operate on 'raw' personal data to produce 'refined' data doubles and use the data doubles to generate preemptive nudges that, when well executed, operate as self-fulfilling prophecies, eliciting the patterns of behavior, content consumption, and content sharing already judged most likely to occur").

nomic surpluses.[75] However, those are not the only actors nor the only concerning motives that the personalization of smart-devices invokes.

Arguing that personalization limits users or prompts them towards specific outcomes does not imply it is undesirable.[76] Indeed, tailoring the use of products and services for specific needs of specific users is often celebrated as a great boon to users.[77] The view that personalization policies are objectionable simply because they limit users wrongly assumes that without such personalization users would be "free" to use the functions that the smart-device facilitates and therefore would be better off.[78] However, the reality is more complicated.[79] Freedom to access all available functions does not necessarily translate to easier or better user experience, especially when there is an abundance of possibilities and the user is humanely limited.[80] Many of the services and devices we use would not have been appealing had the operators not personalized use of them for us.[81] To see this, just imagine what searching for videos on YouTube would have been like had its operators not personalized the content for you.[82]

Similar arguments supporting personalization could be applied to smart-fridges: personalization of ordering milk frees users from reviewing all the alternatives for each purchase, and personalizing the fridge's arrangement could make the products for the next meal more accessible. For now, we can set aside the normative arguments for or against personalization.[83] My claim here is descriptive, namely that personalization is a form of limitation initiated by operators and aimed at specific users.

---

75. ZUBOFF, *supra* note 64, 293–328; Crootof, *supra* note 41, at 593–605.

76. *Cf. infra* note 220.

77. Julien Boudet et al., *The future of personalization—and how to get ready for it*, MCKINSEY & CO. (June 18, 2019), https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/the-future-of-personalization-and-how-to-get-ready-for-it#.

78. On the freedom argument and its problems, see, e.g., Grafanaki, *supra* note 68, at 26.

79. *Id*.

80. *See* Gal, *supra* note 43, at 84–87 (explaining the psychological burdens of choices and how algorithms may assist).

81. Woolgar, *supra* note 74, at 75 (suggesting that the technology's design has to predicts what the user will want to do, which makes its designers "define[ ] users' future requirement"). This point is also valid in information moderation, see, e.g., Tim Wu, *Is the First Amendment Obsolete?*, 117 MICH. L. REV. 547, 562–63 (2018) (arguing that the abundance of information makes the challenge of mediating proper information more pressing than the challenge of supporting creation of content).

82. On YouTube's personalization and video suggestions, see YOUTUBE HELP, https://support.google.com/youtube/thread/1456096?hl=EN&msgid=1532143 (last visited July 11, 2021).; *s*ee also Grafanaki, *supra* note 68, at 26–37.

83. *See infra* Part III.C.6–7. Arguably, empowering operators to allow users to perform specific actions or to limit them from performing others are two faces of the same coin—both are an exertion of power on the user.

Note, with the necessary modifications, the aforementioned definition of personalization can apply to numerous instances of personalization by various operators—including operators of smart-devices, of software, of physical spaces, etc.[84] This Article only discusses personalization of smart-devices, which makes for a particularly interesting case because it combines the personalization of code and the personalization of physical space.[85]

B. How to Personalize

Moving on to the technicalities: how do operators personalize? The first step is identifying the individual that is about to use the smart-device.[86] To do so, smart-devices' operators often apply various sources of data to create specific profiles for each individual that interacts with the device.[87] At this stage, the only identification necessary is one that allows operators to distinguish between the different users of the smart-device.[88] This distinction does not have to refer to any external identification methods, such as name, social security number, or social media account.[89] Rather, the point is simply to create a virtual representations of an individual user that can be distinguished from other users.[90]

Once users are identified, the operators will determine whether the user fits some set criteria.[91] These criteria can be general and predetermined, such as age, gender, or weight; or specific and ad-hoc, such as the number of beers or chocolate bars that this user had in the last hour.[92] Once the operators identified that the user fits a criterion, they

84. *See infra* Part II.B–D.

85. *See infra* Part II.C.

86. *See supra* notes 29–30 and accompanying text.

87. The GDPR coined the term profiling for this part of the personalization process: "'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person . . ." *see* 2016 O.J. (L 679) 119.

88. *E.g.*, user 1, user 2 . . . user n.

89. Daniel H. Kahn, *Social Intermediaries: Creating a More Responsible Web Through Portable Identity, Cross-Web Reputation, and Code-Backed Norms*, 11 COLUM. SCI. & TECH. L. REV. 176, 206 (2010) (discussing signing in to different web services using specific users); *see also Use your Google Account to sign in to other apps or services*, GOOGLE, https://support.google.com/accounts/answer/112802?co=GENIE.Platform%3DDesktop&hl=EN (last visited July 11, 2021).

90. *Cf.* COHEN, *supra* note 74, at 67 (explaining the notion of "data doubles," virtual representations of individuals based on data sets about those particular individuals. Data doubles are designed to enable operators to construct and manage the actions of that individual).

91. *Cf.* Davis, *supra* note 72.

92. Other personalization criteria discussed in the literature include those based on capacity, resources, skills, or risk, see Omri Ben-Shahar & Ariel Porat, *Personalizing Negligence Law*, 91 N.Y.U. L. REV. 627, 636–55 (2016).

would apply the limitations set for this specific criterion.[93] Setting the criteria and determining whether a user fits some criterion is based on data about the user, thus, collecting more information about users is helpful for better personalization.[94] More available information facilitates the creation and application of more criteria, which could be applied more specifically to smaller and more nuanced groups of users, thus creating higher resolution customization.[95] Theoretically, however, basic personalization can be achieved with very little information about the user, namely, information that allows distinguishing one user from another.

To illustrate, a smart-fridge can use its sensors to identify that the user that is about to approach is "User 1," part of the criterion "User 1 and User 2," and operate the set limitation of locking the beer compartment. Alternatively, the smart-fridge may identify that Joe is approaching the smart-fridge, retrieve that Joe's Facebook profile indicates that he is fifteen years old and thus fit the criteria of being underage, and accordingly operate the limitation of locking the beer compartment. Both cases involve personalization, the situations differ by the volume of information and thus sophistication and details-resolution applied by the operator.

C. Modes of Personalization

Lawrence Lessig famously introduced four sources of constraints or regulations that can be imposed to affect behavior: laws, norms, architecture (physical and code), and market.[96] This construct has interesting implications for personalization of smart-devices. Namely, personalization of smart-devices relies on personalization of code and physical architecture,[97] and can be used to further develop law and market constraints.

1. Physical & Code Architecture

Computer code imposes constraints on users by defining what the user can and cannot do at different interactions with the relevant code.[98] James Grimmelman neatly captured this idea, noting that by

93. Grafanaki, *supra* note 68, at 20–22; *see infra* note 205.

94. *See infra* notes 204–08 and accompanying text.

95. *See infra* notes 199–200 and accompanying text.

96. LAWRENCE LESSIG, CODE: VERSION 2.0 121–25 (2006). For analysis and criticism of this view, see James Grimmelmann, *Regulation by Software*, 114 YALE L.J. 1719, 1723 (2005).

97. *See infra* Part I.A.1.

98. LESSIG, *supra* note 96, at 124–25; *supra* Part I.A. For reservations to seeing code as architecture see, e.g., Grimmelmann, *supra* note 96, at 1721–22 (criticizing Lessig and suggesting that software is its own form of regulation).

providing a limited set of possible actions, codes exclude every action that is not in the set.[99] Think about a desktop computer shared by several family members. If each family member has their own user profile, then a mother may have access to programs and files that her daughter does not have access to and vice versa. Similarly, on the Internet, when logging in to Facebook, the information and options that are presented on one person's screen (e.g., the content of private groups, chats, or the newsfeed) are probably different than yours. While some might see content about design and architecture, others might never be aware that those exist on Facebook and only see content about politics and law.[100] Hence, code is a mode of regulation that can be used to impose personalized constraints.[101] Since computer codes can be created and modified by simply rewriting lines of code, it is a relatively easy and dynamic form of constraint.

Using code to facilitate particular services to particular users—be it a desktop's operating system, social media websites, or any other platform—is personalization via code. It allows only certain users to perform specific actions or see specific content, while conversely limiting others from accessing such content.[102] As mentioned, these can be used for more or less praiseworthy endeavors.[103] Examples of the former were mentioned in the previous paragraph; examples of the latter include limitations imposed on TikTok and iPhone users in countries surrounding China, barring them from seeing specific languages or emojis that are available to other users.[104]

Lessig also held that physical architecture could impose physical burdens to constrain users, one obvious example being a wall blocking the way.[105] Such physical burdens can also impose personalized con-

99. *See* Grimmelmann, *supra* note 96, at 1729.

100. *See* Grafanaki, *supra* note 68.

101. *See supra* Part II.B.

102. *Supra* notes 98–100.

103. *See supra* Part I.B.

104. *See* Jay Peters & Nick Statt, *Apple is hiding Taiwan's flag emoji if you're in Hong Kong or Macau*, THE VERGE (Oct. 7, 2019, 6:32 PM), https://www.theverge.com/2019/10/7/20903613/apple-hiding-taiwan-flag-emoji-hong-kong-macau-china (For users that buy Apple devices in China, the Taiwanese flag is replaced by a missing character sign, while users in Hong-Kong can see the Taiwanese flag if used by others, but their Emoji keyboard does not include this flag. Thus, all these users are limited from using their devices in a specific according to the code used in their specific case.); Casey Newton, *It turns out there really is an American social network censoring political speech*, THE VERGE (Sept. 26, 2019, 6:00 AM), https://www.theverge.com/2019/9/26/20883993/tiktok-censorship-china-bytedance-politics (publishing that TikTok instructs its moderators to censor videos "that mention Tiananmen Square, Tibetan independence, or the banned religious group Falun Gong, according to leaked documents detailing the site's moderation guidelines").

105. LESSIG, *supra* note 96, at 124.

straints. Think of parents that limit their children from accessing the cookie jar by placing obstacles aimed at children. Parents may place it in a high cabinet or use a lock that only adults know how to open. This is the physical personalization of the cookie jar—the operators (parents) use the physical space to limit specific users (children) from accessing certain functions (getting the cookie jar and eating the cookies). Like personalization by code, personalization by physical architecture limits users' actions within the relevant space—physical or cyber. Compared to the personalization of code, personalization of physical space may be more salient and thus normatively more troubling given the physical nature of the limitation.[106]

These two modes of regulation are crucial for smart-devices. I explained that the digitization of smart-fridges' functions empowers remote operability of those functions.[107] Remote-operability allows operators to use a code to activate the digitized functions in a specific way that modifies the physical architecture of the device. In the case of smart-devices, the personalization of code facilitates the personalization of space.

For example, personalization of smart-fridges can involve operators using code to: allow only specific users to open the beer compartment, prohibit specific users from opening the doors after a specific time, or reorganize the content of the fridge to make some products more accessible or visible for specific users. Similarly, smart-cars can be personalized, namely by using code to apply speed limits on specific users and not on others. In a similar vein, smart-modems (and indeed smartphones) can apply code to limit specific users from accessing specific applications or websites during specific times, smart-doors can lock certain users inside or outside specific rooms, and the list goes on.[108]

Indeed, the operation of smart-devices essentially uses code architecture to modify physical architecture. This combination allows operators to enjoy the dynamic advantages of personalization by code with the salient advantages of personalization by physical space. Those advantages grant operators of smart-devices unprecedented power to prompt users to do or refrain from doing certain actions.[109] This is the primary and most essential aspect of smart-devices' personalization, which can be utilized by various operators and by other forms of constraints.[110]

---

106. *See supra* note 55–56, 73–74 and accompanying text.
107. *Supra* the text accompanying note 41–45.
108. *See supra* the text accompanying notes 58-62.
109. *See id.*; *see supra* the text accompanying notes 70–72.
110. *See infra* Part II.C.2–3, III.A.

2. Smart-Devices and Personalization of Law

Laws can be personalized.[111] Personalized law can be seen as "a personalized command that is based on information about this actor's specific characteristics."[112] When laws are personalized, the limitations that they impose vary according to the specific attributes and circumstances of the individual, thereby limiting one person but not another in cases that would otherwise be treated indiscriminately. Instances of personalized law include adapting reasonability standards in negligence to the characteristics of the specific actor,[113] using personalized default rules based on specific characteristics in contracts,[114] personalizing taxes based on income or other measures,[115] personalizing disclosures for the knowledge and expertise of the specific actors,[116] etc.[117] Arguably, norms may also be personalized to some extent, as exemplified by gender-based personalization of dress codes.

The claim that law can, and often should, be personalized is not innovative in any way. Indeed, the idea that the law should be tailored to better fit the relevant context to which it applies is obvious and has been around as long as the idea of law itself. Indeed, every law has some contextual parameters. The question is how specific—or how finely tailored—those parameters will be."[118] More exciting is the possibility of combining the personalization of law and personalization of smart-devices, as it can affect both the kind of laws enacted and their application.[119]

Consider how smart-devices can *personalize the application of law*. This Article previously argued that personalization includes operating the functions of smart-devices to drive users to do or refrain from do-

111. Cass R. Sunstein, *Deciding by Default*, 162 U. PA. L. REV. 1, 11 (2013) (discussing the adoption of personalized default rules for specific legal contexts).

112. Ben-Shahar & Porat, *supra* note 92, at 629; Anthony J. Casey & Anthony Niblett, *A Framework for the New Personalization of Law*, 86 U. CHI. L. REV. 333, 335 (2019).

113. *See* Ben-Shahar & Porat, *supra* note 92; Casey & Niblett, *supra* note 112, at 341–44.

114. Omri Ben-Shahar & Ariel Porat, *Personalizing Mandatory Rules in Contract Law*, 86 U. CHI. L. REV. 255, 256 (2019).

115. John K. McNulty, *Flat Tax, Consumption Tax, Consumption-Type Income Tax Proposals in the United States: A Tax Policy Discussion of Fundamental Tax Reform*, 88 CAL. L. REV. 2095, 2103 (2000).

116. Christoph Busch, *Implementing Personalized Law: Personalized Disclosures in Consumer Law and Data Privacy Law*, 86 U. CHI. L. REV. 309, 312 (2019).

117. Ariel Porat & Lior Jacob Strahilevitz, *Personalizing Default Rules and Disclosure with Big Data*, 112 MICH. L. REV. 1417, 1421 (2014); Lee Anne Fennell, *Personalizing Precommitment*, 86 U. CHI. L. REV. 433, 434 (2019); Adi Libson & Gideon Parchomovsky, *Toward the Personalization of Copyright Law*, 86 U. CHI. L. REV. 527, 528 (2019).

118. Casey & Niblett, *supra* note 112, at 333.

119. *Id*. at 339–43.

ing something.[120] One instance of personalization can therefore be driving users to obey the law. Examples include smart-fridges applying laws that require consumers to be warned about harmful ingredients in a product, smart-cars limiting the speed limit based on the speed limit on the specific road, or a smart-door locking and stopping burglars from running away.[121] As we shall see later, personalization methods vary in their stringency, and the more stringent the method the more likely it is to drive the user to do or refrain from doing some action.[122] At its extreme, personalization of smart-devices can apply laws to the degree of absolute coercion: blocking any possibility for breaking the law—enforcement of speed limits by smart-cars being a primary example.[123]

A particularly interesting implication of using personalization of smart-devices to drive individuals to obey the law, is that smart-devices can *potentially extend law's practical reach* to spaces, actions, or details that were not previously feasible. In this sense, it resembles other technologies that empower more pervasive, consistent, and potentially absolute application of law within their realm of application.[124] The ability to employ personalization of smart-devices for more comprehensive application of law raises various normative questions: should the state be permitted to use this technology to enforce its law wherever and whenever it can? Should it be encouraged to? Answering these normative questions raises familiar issues about selective enforcement of laws that cannot be fully addressed here.[125] The main point here is that the technological ability to personalize the use of smart-devices influences the practical ability to enforce law.

120. *See supra* Part II.A.

121. Admittedly, these examples might require additional information as explained above, see *supra*, notes 56–57.

122. *See infra* Part III.A.2.

123. *See, e.g.*, Michael L. Rich, *Should We Make Crime Impossible?*, 36 HARV. J.L. & PUB. POL'Y 795, 802–04 (2013) (discussing the use of IoT technology to make certain actions impossible, and distinguishing between allowing individuals to act in undesired ways and punishing them afterwards, and creating a system that limits individuals' ability to do the undesirable act); MyungSan Jun, *Blockchain government - a next form of infrastructure for the twenty-first century*, 4 J. OPEN INNOVATION: TECH., MKT., & COMPLEXITY 1, 5, 9 (2018) (discussing the notion of blockchain-based "absolute laws" that compel "absolute coercion," meaning laws that the user cannot break).

124. Jun, *supra* note 123. For information on the way social media technologies facilitates better application of speech regulation, see, e.g., HCJ 7846/19 Adalla v. Cyber Unit State Att'ys Off. (2021) (Isr.).

125. *See, e.g.*, John Kleinig, *Selective Enforcement and the Rule of Law*, 29 J. SOC. PHILO. 117 (1998); Nicola Persico, *Rational Choice Foundations of Equal Protection in Selective Enforcement: Theory and Evidence*, U. PA. INST. FOR L. & ECON. (Aug. 2, 2006), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=921612.

Thereby, personalization of smart-devices invites us to revisit and question our normative stance on law enforcement and its limits.

Furthermore, by expanding the potential practical reach of law's application, personalization of smart-devices can *ex ante influence the content of law*. As smart-devices empower the application of law on more nuanced situations and in previously unregulated (or unregulatable) actions and spaces, they pave the way for the state to legalize and regulate situations, actions and spaces. For instance, the ability to identify the characteristics of the user approaching the smart-fridge can support more nuanced alcohol consumption regulation, such as determining the limit on consumption of alcoholic goods based on the amount of alcohol they consumed recently (e.g., by calculating the alcohol volume in the different products). It can also support more direct regulation of alcohol-consumption in one's private homes. In a similar vein, smart-cars can support a more nuanced speed limit regulations, allowing more experienced drivers to drive faster and imposing more restricting limitations on inexperienced drivers. It can also facilitate more frequent changes to the speed limit, for instance when the weather conditions change, overcoming the stringency of existing rules.

Put simply, the ability to personalize the *application* of law using smart-devices might serve as a catalyst for *creating* more nuanced personalized law or to regulate activities and spaces that were not previously regulated. In turn, this can change the way we think about legal regulations in several aspects.[126]

First, personalized laws based on smart-devices rely on a more detailed characterization of the regulated actor and the specific circumstances. As such, they can be more nuanced and better suited for the desired outcomes of the law, as the laws discussed in the previous paragraph exemplify, and thereby allow at least some users more leniency and less coercion.[127]

Second, shifting the burden of enforcement onto smart-devices that can apply the law in a more robust and personalized way can influence the distinction between rules and standards. For instance, the changing speed limit example noted above can replace standards like "driving according to the road conditions." As such, personalized laws based on smart-devices might undermine the use of legal standards that rely on ex-post human interpretation in favor of an abundance of

126. *See, e.g.*, Casey & Niblett, supra note 112; Anthony J. Casey & Anthony Niblett, *The Death of Rules and Standards*, 92 IND. L.J. 1401 (2017).

127. *See supra* the text accompanying note 123–25.

clearer and more precise rules that regulate different scenarios and are easier to enforce using smart-devices' code.[128]

Third, relatedly, the distinction between conduct rules and decision rules may not be necessary anymore:[129] if the smart-devices would effectively prevent users from breaking the law, then users would not be able to act according to the conduct rule, turning this into a distinction without a difference. For instance, if smart-cars limit drivers from exceeding the speed limit on any specific road, then users are incapable of exceeding it, as they usually would do on an open road.[130]

Fourth, if enforcement by smart-devices refrains users from acting according to conduct rules over decision rules, then regulators do not have to bear in mind the conduct rules and would be able to set less restrictive rules to begin with, such as raising the speed limit.[131]

Fifth and finally, should the state decide to use personalization of smart-devices to create or apply law onto previously under-regulated activities, it might put significant pressure on the distinction between private and public realms. This can be illustrated by the potential regulation of alcohol consumption within one's home using one's smart-fridge.

3. Smart-Devices and Personalization of Markets

For the purposes of this paper, market limitations are constraints that originate in market analyses and for market-based reasons.[132] Private actors have incentives to apply various constraints, including personalization policies, in order to extract monetary surplus.[133] Market constraints can limit certain users from gaining certain products in many ways. Consider two instances. First, setting different prices for

---

128. *See, e.g.*, Mireille Hildebrandt, *Prefatory Remarks*, *in* HUMAN LAW AND COMPUTER LAW: COMPARATIVE PERSPECTIVES 7 (M. Hildebrandt & J. Gaakeer eds., 2013) ("[T]he ambiguity that provides law with its ?exibility, while challenging the need for legal certainty, derives from the fact that law is language, requiring students of law to immerse themselves in the richness as well as the boring precision of legal text."). For a discussion about rules and standards, see generally Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557 (1992); Russell B. Korobkin, *Behavioral Analysis and Legal Forum: Rules v. Standards Revisited*, 79 OR. L. REV 23 (2000); Casey & Niblett, *supra* note 112.

129. On decision rules and conduct rules, see Meir Dan-Cohen, *Decision Rules and Conduct Rules: On Acoustic Separation in Criminal Law*, 97 HARV. L. REV. 625 (1984).

130. *See* European Commission Press Release, Road safety: Commission welcomes agreement on new EU rules to help save lives (Mar. 26, 2019); Rich, *supra* note 123, at 802.

131. I am grateful to Omer Y. Pelled for pointing this out.

132. *See* LESSIG, *supra* note 96, at 123–25.

133. *See, e.g.*, Andrew Kasabian, *Litigating in the 21st Century: Amending Challenges for Cause in Light of Big Data*, 43 PEPP. L. REV. 173, 190 (2015).

different users based on their characteristics.[134] Online retailers may sell similar goods to different people for different prices—asking a higher price from people that really need the product or from wealthier potential clients.[135] Second, markets may apply personalized constraints by suggesting different products to different users; for instance, suggesting blue shirts for parents that have sons and pink shirts for parents that have daughters.[136] In both cases, market personalization limits particular users (or at least significantly burdens them) from buying particular products, either by the price tag attached to the product or by its availability.[137]

Market personalization can also use smart-devices to impose restrictions on users.[138] Rebecca Crootof explained how private companies could use the remote operability of the devices to monitor and limit users. She includes examples such as retailers remotely limiting the use of smart-cars when the users break the terms of the contract: falling behind on payments or driving beyond state bounds, landlords locking the doors to tenants that violate leases, e-reader books disappearing from the device once the loan period is over, etc.[139] Other instances may include forcing users to update software on the device; otherwise, the device's capacity will be diminished.[140] Market personalization of smart-devices can also be used to promote specific products. Imagine an Amazon-operated smart-fridge, paid to favor Heinz ketchup over the competitors. The smart-fridge can be set to

134. *See generally* Ramsi A. Woodcock, *Personalized Pricing as Monopolization*, 51 CONN. L. REV. 311, 321–26 (2019).

135. *See, e.g.*, Brian Wallheimer, *Are you ready for personalized pricing?*, CHI. BOOTH REV. (Feb. 26, 2018), http://review.chicagobooth.edu/marketing/2018/article/are-you-ready-personalized-pricing; Rafi Mohammed, *How Retailers Use Personalized Prices to Test What You're Willing to Pay*, HARV BUS. REV. (Oct. 20, 2017), https://hbr.org/2017/10/how-retailers-use-personalized-prices-to-test-what-youre-willing-to-pay.

136. Kenneth A. Jacobsen, *Rolling Back the "Pink Tax": Dim Prospects for Eliminating Gender-Based Price Discrimination in the Sale of Consumer Goods and Services*, 54 CAL. W. L. REV. 241, 249 (2018).

137. Admittedly, in a free market system this limitation is seldom as strict as architecture or law because the users may shop the same products in by other merchants. This does not mean that users are not limited, but that they can more easily overcome the limitation.

138. Market personalization also include collecting information about the different users. *See, e.g.*, ZUBOFF, *supra* note 64, at 293–328; Crootof, *supra* note 41, at 596–99. However, those do not directly pose physical restrictions on users, and therefore are beyond the scope of this argument.

139. Crootof, *supra* note 41, at 598–606.

140. To see the problems with such distinction, note the case of Sonos speakers, in which the company announced it will stop operating some devices, rendering them useless to the users even as "traditional" speakers. Lauren Goode, *Sonos Will Soon End Software Support for Its Older Speakers*, WIRED (Jan. 21, 2020, 9:00 AM), https://www.wired.com/story/older-sonos-speakers-will-stop-receiving-updates/.

only order this specific brand of ketchup (as a default or limitation), to rearrange itself to make that product more visible, to make annoying sounds when a competing brand is put in the smart-fridge, or, even more pervasively, refuse to cool any compartment containing competing products.[141]

* * *

There are three main takeaways from this Part. First, analytically, personalization involves an imposition of specific limitations on specific users by operators, aimed at prompting users to do something. Second, practically, personalization of smart-devices brings to the forefront new and more invasive possibilities for operators to limit users and drive them to act. Third, this ability to personalize the use of smart-devices *ex ante* invites different actors to impose more nuanced limitations on users, which in turn can change the nature of legal and market regulation.

The endless possibilities of personalization using smart-devices, some more beneficial and some more harmful, makes attempts to devise regulatory approaches to specific personalization policies extremely difficult.[142] The next chapter will explore and tease out normative intuitions and theoretical concerns regarding regulating the personalization of smart-devices—focusing on the operators of the devices and the justifications to allow them to impose personalization policies on users.

III. Personalization by Ordinary Operators

This Article previously argued that by facilitating remote operability, smart-devices invite more actors into the relationship between the user and the device, namely operators.[143] It also discussed a unique power that those operators have when using the device—the ability to personalize the operation of the device to drive particular users to particular outcomes.[144] This Part advances a legal analysis of personalization by smart-devices. It starts by identifying the legal actors pulling the strings of smart-devices and categorizing three main

141. While these could seem as hypothetical possibilities, it is important to realize that the technology as well as the distribution of legal powers can support such personalization for smart-fridges that are in the market today.

142. *See, e.g.*, Omri Ben-Shahar, *Data Pollution*, 11 J. Legal Analysis 104, 105 (2019); Charlotte A. Tschider, *Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age*, 96 Denver U. L. Rev. 87, 133–43 (2018).

143. *See supra* Part I.

144. *See supra* Part II.

methods of constraints that they may apply.[145] Then, it turns to analyze the desirability of such personalization policies, first adopting the users' perspective and assessing how personalization policies harm their freedoms,[146] and then discussing the distribution of legal and physical powers that govern those personalization policies.[147]

Before we delve in, a quick qualification of scope. As explained, smart-devices can theoretically connect to any server (computer) on the Internet in order to receive commands and share the information it collects.[148] Since this Article focuses on servers that are legitimately authorized to access or operate smart-devices, i.e., "friendly" servers, interesting discussions about cybersecurity and the prevention of unauthorized or malicious operation of the smart-devices will not be addressed.[149]

A. Meet the Ordinary Operators

1. Three Ordinary Operators

To advance a legal analysis of the personalization of smart-devices, it is crucial to point out the legal actors that operate the digital functions of the smart-device.[150] These actors are (server) *operators*, defined here as *the legal entity that controls a server that sends commands to the smart-devices or retrieves information from it*.[151] Remember that operators may operate the device in real-time or in advance.[152]

Admittedly, since decision-making about smart-device operations is often initiated by algorithms, which were often themselves partly or entirely created by other algorithms, the identification of *the* legal entity that best fits the definition of operator can be difficult.[153] This

145. *See infra* Part III.A.

146. *See infra* Part III.B.

147. *See infra* Part III.C.

148. *See supra* notes 24, 26.

149. For discussions about cybersecurity concerns that arise from smart-devices, see, e.g., Sara Sun Beale & Peter Berris, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, 16 DUKE L. & TECH. REV. 161, 162–63 (2018); Mauricio Paez & Kerianne Tobitsch, *The Industrial Internet of Things: Risks, Liabilities, and Emerging Legal Issues*, 62 N.Y.L. SCH. L. REV. 217, 220–21 (2018); Liz Allison, *You Can't Hack This: The Regulatory Future of Cybersecurity in Automobiles*, 21 J. TECH. L. & POL'Y 15, 16 (2016); Scott J. Shackelford et al., *Securing the Internet of Healthcare*, 19 MINN. J.L. SCI. & TECH. 405, 415–16 (2018). For recent regulatory approaches to cyber-security threats posed by smart-devices see CAL. CIV. CODE § 1798.91.04 (West 2018); 2019 O.J. (L 151) 881.

150. FISCHER, *supra* note 17, at 3.

151. *Cf.* GRIMMELMANN, *supra* note 26, at 32.

152. *See supra* text following note 38.

153. For discussion about the control and effective oversight of AI decision-making, see, e.g., Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. DAVIS L. REV. 399 (2017); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated*

challenge need not be sorted out here. For our analysis, suffice to assume that there exists an identifiable legal entity that is the operator, be it the humans that send commands and retrieve information directly or other legal entities that created (or are otherwise legally responsible for) an algorithm that "independently" performs these tasks.

I distinguish between three kinds of ordinary operators. The first kind of operators that can impose limitations on users are the users themselves. Here, a user is anyone that physically uses the smart-device, and is exposed to and affected by the operations of its functions. Users can operate the smart-devices in two ways: directly, using hardware embedded in the smart-device itself such as a touch-screen, voice-activation system, or a steering wheel; or remotely, through a designated software installed in users' smartphones or personal computers. Crucially, users can operate the smart-device in ways that affect themselves or other users. I refer to these alternatives respectively as self-imposed operation and inter-user operation.[154]

The second kind of limiting operators are private companies, operating the smart-devices remotely for business reasons. These could include both the company that manufactured or initially sold the smart-fridge to the users, its authorized technicians,[155] or private companies that gained access to the devices via contractual agreements.[156] Limitations posed by those private companies are usually market limitations.[157]

The third kind of operator is the state. It is technologically possible for state officials to operate smart-devices' servers directly by acquiring access to the server, collecting relevant information, hiring coders to operate it, and sending commands directly to the devices.[158] However, it seems more likely that the state would use its powers to regulate the use of the smart-fridge, particularly, by requiring other actors

---

Predictions, 89 WASH. L. REV. 1 (2014); Anupam Chander, *The Racist Algorithm?*, 115 MICH. L. REV. 1023 (2017).

154. *See supra* Part I.B.

155. *Cf.* the definition of "manufacturer" in CAL. CIV. CODE § 1798.91.05 (West 2018).

156. *See, e.g.*, an Alexa embedded smart-fridge. LG, https://www.lg.com/us/refrigerators/lg-LNXS30996D-door-in-door#none (last visited July 11, 2021).

157. *See supra* Part II.C.3; LESSIG, *supra* note 96, at 123–25 (explaining that constraints on users that originate in market-based reasons are market constraints).

158. On the possibility of mass use of IoT by the state to collect information and achieve policy goals, see, e.g., Akemi Takeoka Chat?eld & Christopher G. Reddick, *A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government*, 36 GOV'T INFO. Q. 346 (2018); Jean Pierre Maissin et al., *How will IoT improve public sector services?*, *in* INSIDE (2015); John G. Browning & Lisa Angelo, *Alexa, Testify: New sources of evidence from the internet of things*, 82 TEX. BAR J. 506 (2019).

to operate the smart-fridge in the ways the state sees fit.[159] As explained, the state can require operators to limit specific users from making specific actions, personalize rules that would limit different users in various situations, or determine a recommendation for specific users and require other operators to implement it.[160]

2. Three Methods of Constraint

Each of the ordinary operators can use various methods of constraint to impose personalized limitations on users of smart-devices, some more stringent than others.[161] To simplify, I distinguish between three methods: notice (easy nudge), nudge, and prevention.[162]

The most lenient of the three is notice, that is, providing the user information about the action that they are about to pursue.[163] In our context, this may include providing information about the nutritional value of the product they are about to consume, about recommended usage, about past use, etc.[164] The most stringent limitation is prevention, which refers to the maximal limitation the smart-device can impose on a user's ability to perform some action.[165] For instance, prevention by smart-fridges includes locking doors or specific compartments, not cooling a specific area, breaking products to prevent use, or issuing bright lights and annoying sounds.[166]

The intermediate method of constraint is the nudge, the "liberal paternalism." This approach aims to apply behavioral levers to regulate the choice architecture of the users, incentivizing them to perform some acts and refrain from others, while preserving their ability to

159. *See supra* Part II.C.2. For a related discussion about empowering private entities to personalize and enforce the law, see Andrew Verstein, *Privatizing Personalized Law*, 86 U. CHI. L. REV. 551 (2019).

160. *See supra* Part I.A.2.

161. *Cf.* Daniel Susser et al., *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1, 12–29 (2019) (discussing persuasion, coercion, and manipulation online).

162. *See, e.g.*, Ryan Calo, *Code, Nudge, or Notice?*, 99 IOWA L. REV. 773 (2014) (arguing that there are three main forms of regulation that ought to be regarded—code, notice, or nudge); *cf.* ZUBOFF, *supra* note 64, at ch. 10 (distinguishing between: tuning, viz. nudging for commercial interests; herding, viz. controlling user's immediate context; and conditioning, viz educating users to respond to a specific stimulus with a specific response).

163. Calo, *supra* note 162, at 787–89.

164. I realize that nudges come in many shapes and forms, and that often notices could be seen as nudges. By notices here, I have in mind providing users the kind of information that increases their navigability, not those that necessarily push them towards a specific outcome. On navigability, see generally CASS R. SUNSTEIN, ON FREEDOM (2019).

165. I focus on common smart-devices that can be physically overcome by users by unplugging it, disconnecting it from the network or hacking it submission. Thus, absolute prevention will not be discussed.

166. Less immediate prevention methods include shaming the user by informing another user (or the state) about lack of compliance.

choose to opt-out.[167] Richard Thaler and Cass Sunstein define a nudge as "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives . . . intervention must be easy and cheap to avoid. Nudges are not mandates. Putting fruit at eye level counts as a nudge. Banning junk food does not."[168] Nudges vary in stringency; sometimes they will seem indistinguishable from mere notices (e.g., calorie signs), and other times, they may be so stringent that people almost always comply with them—making them seem more like mandates.[169] In the case of smart-fridges, nudges may include making specific products less accessible by requiring additional passwords to reach them or by automatically reorganizing products in a particular way that makes them less reachable. Nudges may also make products less appealing, for instance by warming beer that should be served cold or freezing ice cream beyond (immediately) useable temperature.

B. Towards Legal Intervention I – Assessing the Harms to Users' Freedom

It is difficult to accurately measure harms to users, both generally and in instances of personalization by smart-devices.[170] However, a rough estimation of objectionability can be achieved by combining the kind of operators imposing the personalization policy and the methods of constraints used in each setting. The following table presents the intersection of the kinds of operators and methods of personalization articulated above. It suggests a simplified view of personalization schemes that smart-devices enable, and thus invites an intuitive normative evaluation of those based on a tangible example.

The working example for this table is simple: a user approaches the smart-fridge in order to get yogurt. The smart-fridge has a dairy compartment where yogurts are stored, and this compartment can be locked or unlocked digitally by the operator. The device identifies the

167. Calo, *supra* note 162, at 783–87.

168. RICHARD THALER & CASS SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 6 (2008). Sunstein recently expanded this view, explaining that the role of nudges is to overcome the problem of *navigability*, which prevents people from pursuing their real goals and thus hinders individuals' freedom, see generally SUNSTEIN, *supra* note 164.

169. *See* Lavi, *supra* note 64, at 8–11, 21–35, 79–85 (explaining the nudge approach and discussing different ways for online intermediaries to nudge the users, and discussing various stringencies of nudges); Ryan Bubb & Richard H. Pildes, *How Behavioral Economics Trims Its Sails and Why*, 127 HARV. L. REV. 1593, 1594, 1638 (2014) (criticizing the nudge approach and arguing that because default rules suggested by it are so "sticky," they amount to mere regulation).

170. *See* Ben-Shahar, *supra* note 142; Tschider, *supra* note 142; *cf.* Crootof, *supra* note 41.

specific user and acknowledges that they belong to Category X (for instance, youth, overweight, diabetic, lactose intolerant, or specific user outlined by an operator). Then, the smart-fridge applies a personalization scheme that the operator initiated. The table showcases the different operators (in the columns) using different methods (in the rows). The first sentences in the boxes specify the pre-determined limitation imposed by the respective operator, followed by the actions taken by the smart-fridge or by other actors.

	User self-initiated limitation	**Other-user initiated limitation**	**Private Company initiated limitation**	**State initiated limitation**
Notice	John: "I wish to be informed if I eat more than five daily dairy products." Smart-fridge: "You had five dairies today, taking this will exceed your daily dairy limit."	John: "Inform Elli that it's bad for her to eat more than two daily dairy products." Smart-fridge: "Elli, John says that you should not eat more than two dairies per day, and this is your third."	Private company: "Suggest category X users to eat dairy products by brand B." Smart-fridge: "People like you eat at least two daily dairy products; did you know that brand B has all your vitamins?"	State: "It is recommended for category X users not exceed two daily dairy products; operators must inform users." Operator: "inform category X users about the recommendation." Smart-fridge: "FDA recommends that you will not eat more than two daily dairies.
Nudge	John: "I wish to limit my daily dairy consumption to two." Smart-Fridge: "You exceeded your daily dairy cap." - "To take dairy, say the password." or - Rearranging products to hide dairy until tomorrow.	John: "Nudge Elli not to eat more than two daily dairy products." Smart-Fridge: "Elli, you exceeded your daily dairy cap." - "To take dairy, say the password." or - Rearranging products to hide dairy until tomorrow.	Private company: "Nudge category X users to eat more than two daily dairy products by brand B." Smart-Fridge: "You have not completed your suggested daily dairy goal." - "Eat one type B dairy to get additional points." or - Rearranging products to show brand B dairy products.	State: "It is recommended for category X users not to exceed two daily dairy products; operators should nudge users." Operator: "Nudge user to eat less than two dairy products per day." Smart-Fridge: "You exceeded your daily recommended dairy consumption: - "To take dairy, say the password." or - Rearranging products to hide dairy until tomorrow.
Prevention	John: "prevent me from eating more than two daily dairy products. Smart-fridge: "You exceeded daily dairy cap; dairy drawer is locked until tomorrow."	John: "prevent Elli from eating more than two daily dairy products." Smart-fridge: "You exceeded daily dairy cap; dairy drawer is locked until tomorrow."	Private company: "prevent category X users from eating more than two daily dairies, unless they are by brand B." Smart-fridge: "You exceeded daily non-brand B dairy cap; dairy drawer is locked until tomorrow, brand B is available in the top shelf."	State: "It is forbidden for people of category X to eat more than five daily dairy products." Private company: "Prevent category X users from eating more than five dairies per day." Smart-fridge: "You exceeded daily dairy cap; dairy drawer is locked until tomorrow."

The table above illustrates how personalization of smart-devices play out from the user's perspective, namely by combining the operators imposing them and the constraint method used. It showcases how personalization policies limit users and drive them to action, and underscores the influence smart-devices' personalization policies can have, even when aimed at seemingly simple and innocent issues such as access to dairy products. In doing so, it invites the readers to use their intuition regarding the desirability of such personalization policies. The reader's reaction to the idea that their smart-fridge will rearrange their products, ask for a password, or stop them from taking dairy products, by orders of the state, private company, or other users can tell the reader something about the need to regulate those operators and actions.

To a legal audience, the table also sheds light on the broad range of legal issues involved in personalization by smart-devices. It blends relationships between state, private companies, and users, as well as various methods for imposing constraints. In turn, it shows that personalization of smart-devices raises a myriad of legal questions, including the regulation of commercial and compelled speech,[171] antitrust and consumer protection concerns,[172] quasi-regulatory questions about constructing individuals' choices,[173] as well as contract, torts, and fiduciary duties.[174] Such regulatory variety makes any attempt to regulate personalization policies by smart-devices extremely challenging and case-specific.

However, before rushing to analyze the personalization of smart-devices in light of any specific legal doctrine, it might be wise to take a step back and normatively evaluate the situation. One way to norma-

171. *See, e.g.*, Jeffrey S. Wettengel, *Reconciling the Consumer "Right to Know" with the Corporate Right to First Amendment Protection*, 12 J. BUS. & TECH. L. 325 (2017); Colleen Smith, *A Spoonful of (Added) Sugar Helps the Constitution Go Down: Curing the Compelled Commercial Speech Doctrine with FDA's Added Sugars Rule*, 71 FOOD & DRUG L.J. 442 (2016); Andrew M. Osarchuk, *An Argument for Public Health and Doctrinal Clarity: Why the Supreme Court Should Overturn* R.J. Reynolds v. FDA, 69 N.Y.U. ANN. SURV. AM. L. 265 (2013).

172. *See generally* Bill Batchelor & Grant Murray, *Internet of Things: Antitrust concerns in the pipeline?*, KLUWER COMPETITION L. BLOG (May 12, 2016), http://competitionlawblog.kluwercompetitionlaw.com/2016/05/12/internet-of-things-antitrust-concerns-in-the-pipeline/ ; D. Daniel Sokol & Roisin Comerford, *Antitrust and Regulating Big Data*, 23 GEO. MASON L. REV. 1129 (2016); Marc J. Veilleux, Jr., *"Alexa, Can You Buy Whole Foods?" An Analysis of the Intersection of Antitrust Enforcement and Big Data in the Amazon-Whole Foods Merger*, 37 CARDOZO ARTS & ENT. L.J. 481, 493, 495, 507, 510 (2019); 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).

173. *See generally* SUNSTEIN, *supra* note 164; THALER & SUNSTEIN, *supra* note 168; Lavi, *supra* note 64.

174. Crootof, *supra* note 41, at 646–60.

tively evaluate the (un)desirability of personalization policies, and respectively the need for regulation that protects from it, is by focusing on potential harms to users' freedoms—hindering negative freedoms or burdening users' freedom of choice to a higher degree.[175] When operators limit individual users from pursuing actions that they are otherwise free to pursue, they limit users' negative freedom (i.e., the freedom to act undisturbed).[176] When operators qualify the range of actions that individual users can pursue, they burden users' freedom of choice.[177]

The combination of the kind of actors and constraint method used, articulated in the table above, can help us assess the harm to users' freedoms. Discussing this intersection would not provide an accurate evaluation of harm to the users' freedom, but it can provide an ordinal scale that will help assess the (un)desirability of each policy in comparison to the others. To do that, we need first to scale the objectionability of each method and operator.

Previously, I scaled the different methods of constraint according to the stringency of the limitation they impose on users.[178] The objectionability of constraining operators can be scaled using the perspective of users' freedom. Arguably, the greater the ability of the user to influence (i.e., meaningfully consent to or reject) the actions of the operators that initiated the imposed constraint, the less normatively objectionable the operators' actions are.[179] Following this view, operators with whom users are more directly connected are less objectionable. Accordingly, self-imposed constraints are least normatively objectionable, since they can be traced back to the person's own free will.[180] Other operators are respectively ordinally situated based on

175. The distinction between freedom to decide and the freedom to act upon a decision dates back to Thomas Hobbes, see THOMAS HOBBES, LEVIATHAN OR THE MATTER, FORME & POWER OF A COMMONWEALTH ECCLESIASTICALL AND CIVIL, ch. 21 (Penguin Books, 1985) (originally published 1660); PHILIP PETTIT, MADE WITH WORDS: HOBBES ON LANGUAGE, MIND, AND POLITICS 134–36 (2008).

176. Isaiah Berlin, *Two Concepts of Liberty*, *in* THE PROPER STUDY OF MANKIND 191, 193–98 (Henry Hardy & Roger Hausheer eds., 1997) (developing the distinction between positive and negative freedom); Ian Carter, *Positive and Negative Liberty*, *in* STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Zalta N. Edward ed., 2018).

177. Ian Carter, *Choice, freedom, and freedom of choice*, 22 SOC. CHOICE & WELFARE 61, 69 (2004) ("A person has freedom of choice if she lacks constraints on the reasoned selection and performance of one or more of the items on an action-menu.").

178. *Supra* Part III.A.2.

179. *Cf.* SUNSTEIN, *supra* note 164, at 102, 114–15 (arguing that choosing between modes of choice architecture that best promote freedom, boils down to assumptions about users' ability to make good choices and the architects' reliability).

180. *See, e.g.*, Berlin, *supra* note 176, at 194 (noting that freedom is hindered only if one is limited *by others*).

the proximity of the user to the constraining operator as follows: other users,[181] followed by private companies,[182] and finally, the state (considered most objectionable).[183],[184]

Following those assumptions, upper left boxes are the more freedom preserving and, therefore less normatively objectionable; and lower right boxes are most freedom restrictive, and therefore more normatively objectionable.

Admittedly, qualifications could be raised against this simplified articulation; its underlying assumptions can be challenged and its broad perspective can be more finely detailed. The value of this birds-eye view is in elucidating the intricate scheme of personalization constraints that smart-devices users are exposed to, and thereby enrich our intuitions and understanding about the (un)desirability of personalization policies by various operators.

C. Towards Legal Intervention II – The Distribution of Legal Powers to Operate Smart-Devices

This part will take another step towards constructing a legal response to personalization of smart-devices by mapping out the distribution of physical and legal powers to operate the smart-devices. To

181. Perhaps the most interesting and confusing case is the justification of legal power for inter-user personalizations. Some instances seem clear and persuasive, such as granting parents the legal powers to limit their children's use of the smart-fridge. Other instances seem very objectionable, such as allowing a person to bully their spouse by limiting their access to the smart-fridge. On the intra-users application personalization, see *supra* Part I.B. The trouble is that distinguishing between these cases requires a mechanism that identifies the different relationships between the users of every device, and distributes legal powers accordingly. I shall elaborate on these questions and mechanisms later. *See infra* Part IV.B.

182. A recent example of users' ability to influence private-companies more efficiently than governments is the public pressure that made PornHub change their content-moderation policies: Nicholas Kristof, *The Children of Pornhub*, N.Y. TIMES (Dec. 4, 2020), https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html.

183. Various considerations support the objection to the state's use of personalization using smart-devices. While state actions to limit individuals' freedom is often justified in different manners, state-initiated personalized policies that rely on smart-devices would likely face difficult questions about legitimacy of algorithmic decision-making, and the values that are optimized by the algorithm used. While the state regularly holds legal powers to apply personalized regulations using laws, applying those regulations using smart-devices seems unduly invasive, and is even more troubling with stringent constraint methods. On these, see generally Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671 (2016); Emily Berman, *A Government of Laws and Not of Machines*, 98 B.U. L. Rev. 1277 (2018); Ari Ezra Waldman, *Power, Process, and Automated Decision-Making*, 88 FORDHAM L. REV. 613 (2019); Aziz Z. Huq, *A Right to a Human Decision*, 106 VA. L. REV. 611 (2020)

184. These are mere assumptions that could not be established here. I concede that other orders might be possible: limitations by private companies can seem worse than limitations by the state, since the state's actions are assumed to be legitimate as representing the people and working for them; and limitation by other users can be particularly difficult to challenge.

achieve this, it is helpful to revisit the work of Wesley Newcomb Hohfeld, who explored the nature of legal relations and entitlements. Hohfeld distinguished between legal power and the physical power to exercise it.[185] According to this view, having physical power to operate the functions of the smart-device does not necessarily coincide with having the legal powers to operate it.[186] There are two meanings of legal power that are relevant to our discussion: legal power as the ability to use something, and legal power as the ability to make changes in legal relations. The two kinds of legal powers can be respectively explained as first-order power, meaning the ability to operate the smart-device; and second-order power, meaning the ability to decide who *gets* first-order legal power to operate the smart-device.[187] Thus, having a legal power to operate the smart-device can amount to either legally using the different functions of the smart-fridge, or deciding who can legally use it, or both. Crucially, distributing legal powers to some actors ought to be normatively justified.[188]

Hohfeld explained that legal power correlates with legal liability, meaning that Adam's power subjects Ben to liability for some change of legal relations. For instance, when Adam sends a letter to Ben with an offer to sell some land for a specific price, Ben has correlating power to accept the offer and thus finalize the sale, making Adam liable to pass on the land. Liability, in this sense, is to be understood as legal responsibility, which could have monetary consequences.[189] Liability is the jural opposite of immunity, i.e., exemption or freedom from legal responsibility. If Ben has immunity regarding something, Adam has no power to wield over Ben with regard to that thing; thus,

185. Wesley Newcomb Hohfeld, *Some Fundamental Legal Conceptions as Applied in Judicial Reasoning*, 23 YALE L.J. 16, 24 (1913) [hereinafter Hohfeld (1913)]; Wesley Newcomb Hohfeld, *Fundamental Legal Conceptions as Applied in Judicial Reasoning*, 26 YALE L.J. 710 (1917). *See also* COHEN, *supra* note 74.

186. Leif Wenar, *Rights*, *in* STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Zalta N. Edward ed., 2015). *Cf.* Joseph Raz, *Normative Powers (revised)*, at 6 (Columbia L. Sch. Pub. L. Working Paper, Paper No. 14-629, 2019), https://scholarship.law.columbia.edu/faculty_scholarship/2460 (using a similar distinction to discuss the nature of normative powers, emphasizing that while someone may have the power to perform some act, they may be (normatively) directed not to do it).

187. Madeline Morris, *The Structure of Entitlements*, 78 CORNELL L. REV. 822, 827–34 (1993); *see also* Hohfeld (1913), *supra* note 185, at 45–46. *Cf.* Raz, *supra* note 186 (noting that one should distinguish between normative powers that originate from exercising a legal power by another person (i.e., a chained power), and powers that originate otherwise (basic power)).

188. One way to justify someone having a normative power (or having a *valid* normative power) lies on the bearer of the power having an undefeated value that justifies having such power, see Raz, *supra* note 186, at 4, 7, 9.

189. *See* Hohfeld (1913), *supra* note 185, at 50–54; David Campbell & Philip Thomas, *Introduction*, *in* FUNDAMENTAL LEGAL CONCEPTIONS AS APPLIED IN JUDICIAL REASONING BY WESLEY NEWCOMB HOHFELD (2001).

if Ben has immunity they are not liable.[190] This distribution of physical and legal powers and liabilities regarding the smart-device is the jurisprudential foundation for regulating the operation of smart-devices.

1. First-Order Legal Power

Let us begin with first-order legal powers to operate smart-devices. Sometimes operators hold legal powers to operate functions of the smart-device which are not available to the user. Aaron Perzanowski and Jason Schultz noted that manufacturers use smart-devices to limit users' usage of devices, and surveyed the accompanying changes of legal powers to operate the smart-devices.[191] More recent scholarly discussions about such distribution of legal powers to operate the smart-devices include contributions about the smart-devices' liability regimes[192] and about users' power to modify or repair the smart-device.[193] Previous parts of this Article that explained operators' ability to impose personalization schemes using smart-devices, compliment this scholarship.

In Hohfeldian terms, in all those cases users are legally disabled against operators' powers to operate the device in such instances, meaning that those operators are legally immune from claims that the user may have regarding the operation of the device. Such distribution of legal powers allows operators to impose limitations on users without any legal ramifications.[194] This leaves the users legally disabled or legally unable to perform certain actions regarding the device or to defy undesired actions by the operators.[195]

An interesting question arises about the nature of this first-order legal power to operate smart-devices. Some might see it as a property right derived from ownership over the device,[196] others might suggest that it is merely a limited property right, distinct from the property right of possession of the smart-device,[197] yet even others might sug-

190. Hohfeld (1913), *supra* note 185, at 54–58.

191. AARON PERZANOWSKI & JASON SCHULTZ, THE END OF OWNERSHIP: PERSONAL PROPERTY IN THE DIGITAL ECONOMY 139–40, 146, 152 (2016).

192. For a related discussion see Jane E. Kirtley & Scott Memmel, *Rewriting the "Book of the Machine": Regulatory and Liability Issues for the Internet of Things*, 19 MINN. J.L. SCI. & TECH. 455, 500–12 (2018); Crootof, *supra* note 41; Bethany Corbin, *Liability for the Internet of Things*, 21 TORT SOURCE 11 (2019).

193. *See* Kilovaty, *supra* note 42, at 458, 462–63; Leah Chan Grinvald & Ofer Tur-Sinai, *Smart Cars, Telematics and Repair*, 54 U. MICH. J.L. REFORM 283 (2021).

194. *See supra* notes 189–90 and accompanying text.

195. *See* Hohfeld (1913), *supra* note 185; the text next to *supra* note 38 and forth.

196. *See, e.g.*, Grinvald & Tur-Sinai, *supra* note 193, § I.A (making a similar argument for the right to repair).

197. *See, e.g.*, JOSHUA WEISSMAN, LAW OF PROPERTY: POSSESSION AND USE 9–53 (2005).

gest that it is a contractual right, based on an incomplete contract that can be modified and specified by the seller.[198] The nature of the legal power will affect the distribution of others' legal powers over the smart-device, and thus its regulation. Based on the technological preface articulated above, it is my intuition that the legal power to operate some function of the smart-device, including the power to personalize the device, is some sort of property right which is distinct from ownership or possession and can be held simultaneously by multiple actors. Explicating this view exceeds the scope of this paper.

Moving on, if operating smart-devices and applying personalization schemes is a legal power, distributing it to some actor must be justified.[199] Arguably, the legal power to apply personalization policies using smart-devices should be distributed between operators and users in such a manner that does not grant operators full immunity from users and that users are not fully disabled. One reason supporting this view is that personalization of smart-devices is one-directional: it impacts users and not the operators.[200] As explained in the previous part, users' diminished ability to influence the operators' actions (that impact the user) is assumed to be more difficult to justify than operators' actions that the users can leverage.[201]

Another reason not to grant operators full legal immunity in operating smart-devices stems from users' expectations. Users have certain expectations concerning their legal relationships with their traditional devices, which influence the legal regulation of such devices and are affected by it.[202] Since smart-devices usually launch on the basis of the traditional devices, the "smart" capabilities or features are added to the traditional ones.[203] In this sense, the smart-device and the traditional devices are, at least initially, the same "thing"—and thus the users' pre-digitized expectations about the traditional device echo the smart-device.[204] Arguably, since personalization policies—especially the constraints and limitations that are bundled with them—were not technologically possible in the traditional devices, users' expectations for those devices do not include the limitations brought about by the personalization policies.[205] Moreover, even if the users had accurate

198. *Id.*

199. *See supra* note 188.

200. *See supra* Part III.B.

201. *See supra* text accompanying notes 178–84.

202. *See, e.g.*, Crootof, *supra* note 41, at 623–24.

203. *See supra* Part I.A.

204. *See* Hoofnagle et al., *supra* note 46, at 815–16. On the argument that traditional and smart are the same "thing," see *supra* note 2.

205. *See* Zuboff, *supra* note 64; *supra* notes 191–93.

expectations towards smart-device operations when they bought them, those might become irrelevant because smart-devices are prone to change via software updates much more rapidly than comparable traditional devices.[206] While these changes might be expected in smartphones or Internet services like social media or search engines, they are rarely expected in fridges or cars.[207] This discrepancy is accentuated in those smart-devices that are not as frequently bought: the longer the user has the smart-device, the more modifications will likely occur, and thus expands the gap between users' original expectations and the actual operation of the device.[208] Respectively, the justification to grant operators the legal power to apply whatever personalization policies they choose using smart-devices diminishes.

2. Second-Order Legal Power

Smart-devices brought considerable change to the distribution of second-order legal powers. Since operating traditional devices required the operators to be in the same space and time as the device, the physical powers to operate traditional devices were limited to those that had physical access to it.[209] This meant that sellers would not have a significant incentive to achieve legal powers to operate traditional devices, and that the distinction between operators and users was of little practical significance. Therefore, until smart-devices came along, the question about deciding who gets to operate the device—and who decides that decision—was theoretical question at best.

Smart-devices changed that. Remote operability of smart-devices allowed operators to transcend the time and space challenges, *de facto* making it easier for operators to exercise physical powers over the device.[210] Interestingly, such redistribution of physical powers to operate the smart-device—from the users' unique ability to remote operability of multiple operators—revitalizes actors' interests to hold second-order legal powers and to shape how legal powers to operate

206. More about the changing expectations of similar things becoming smart, see generally Graham Johnson, *Privacy and the Internet of Things: Why Changing Expectations Demand Heightened Standards*, 11 WASH. U. JURIS. REV. 345 (2019) (discussing the expectations of privacy for similar things when they turn smart). About the different expectations regarding the new device of the smart-phone (but not the information stored in it), see Riley v. California, 573 U.S. 373, 395–96 (2014) (holding that "[p]rior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception").

207. *See* Johnson, *supra* note 206.

208. *See id.*

209. *See supra* Part I.A.

210. *Id.*

smart-devices will be distributed.[211] In practice, market incentives and the current property regime favor private companies—namely sellers and manufacturers—allowing them to distribute smart-devices' operating powers as they see fit.[212] This led to the current situation, in which operators hold objectionable legal powers over the devices and often leave users powerless and legally-disabled.[213]

But this second-order legal power grab is not a *fait accompli*. Our second-order distribution doctrines are themselves contingent, and there are viable alternatives. One alternative model is adopting the traditional-fridge framework, in which by buying the smart-device, the user gets all first and second-order legal powers, leaving the distribution of legal powers in the users' hands.[214] Other alternatives include regulating a default bundle of minimum legal powers that users of smart-devices get when buying the device;[215] identifying specific users' rights regarding the operation of smart-devices and the limitations that ought to be imposed on other operators to secure these rights;[216] rethinking our views about property rights altogether;[217] or perhaps imposing more significant public law duties on the sellers should they wish to retain such powers.[218] The most thought-provoking arguments call for reimagining the property regime altogether to better serve the growing economic and informational power of some actors over users.[219]

---

211. *See supra* notes 191–93.

212. *Id*. The most prominent example of this second-order power-grab are the operation moderators, see *infra* Part IV.B.

213. *See supra* notes 194–95.

214. *See supra* text accompanying notes 209–10.

215. Ferguson, *supra* note 14, at 859–61; Robin Kester, *Demystifying the Internet of Things: Industry Impact, Standardization Problems, and Legal Considerations*, 8 ELON L. REV. 205, 212 (2016). Both suggest that owners of smart-devices should have some powers over functions of those devices. While they only mentioned in passing general interest in information and data and interests in ownership of health data specifically, we might think about other interests for operating smart-devices such as exclusive power to lock or unlock the compartments of smart-fridges.

216. James Bonar-Bridges, *Regulating Virtual Property with Eulas*, 2016 WIS. L. REV. FORWARD 79 (2016); Kenneth W. Eng, *Content Creators, Virtual Goods: Who Owns Virtual Property?*, 34 CARDOZO ARTS & ENT. L. 249 (2016) (Both discuss the claims of gamers from the sellers of online games.).

217. S*ee, e.g.*, M. Scott Boone, *Ubiquitous Computing, Virtual Worlds, and the Displacement of Property Rights*, 4 J.L. & POL'Y FOR INFO. SOC'Y 91, 124–31 (2008); Lothar Determann, *No One Owns Data*, 70 HASTINGS L.J. 1, 5 (2018) (interestingly arguing that the data that IoT devices produce is not governed by rights at all, and therefore no one owns it, challenging the notion of personal data generally).

218. *See supra* note 158.

219. *See, e.g.*, ZUBOFF, *supra* note 64; Jedediah Britton-Purdy et al., *Building a Law-and-Political-Economy Framework: Beyond the Twentieth-Century Synthesis*, 129 YALE L.J. 1784 (2020); Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460 (2020).

The discussion about the adequacy of the existing distribution of second-order legal powers over the operations of smart-devices exceeds the scope of this Article. For my purposes, suffice to emphasize that this distribution is qualitatively different in the age of smart-devices. Remote operability made operators much more important, and the question of "Who decides who can operate the smart-device?" is a crucial consideration for any future attempt to regulate the field.

IV. PERSONALIZATION BY PRIME-OPERATORS

Some smart-device operators stand out. Like ordinary operators, they have legitimate access to operate the digital functions of the smart device, and they can use this access to personalize its operation, as previously discussed. However, while the operators discussed thus far were assumed to operate specific functions in a handful of smart-devices, the ones we turn to now are professional operators, who create systems that operate and personalize enormous amounts of functions and smart-devices. As the following discussion will illustrate, these operators have two distinct features that single them out from other operators: significantly improved ability to collect information and make inferences that are relevant for personalization, and significantly greater access to operate smart-devices alongside other operators. These two aspects provide those actors with considerable advantages over other operators, granting them the title of *prime-operators*.

A. Informational, Economic, and Computational Advantages

Earlier, I explained that personalization involves using the smart-devices' sensors to collect information about the user and that more information facilitates better and more nuanced personalization policies.[220] Operators use this information to personalize the operation of the smart-device[221]—to learn about trends of use, preferences, responses, or the condition of the device, and respectively choose the adequate operating response to various contingencies.[222] This process

220. *See supra* Part II.B.

221. *See, e.g.*, *IoT Is Building Higher Levels Of Customer Engagement*, FORBES INSIGHTS (June 14, 2018, 11:35 AM), https://www.forbes.com/sites/insights-inteliot/2018/06/14/iot-is-building-higher-levels-of-customer-engagement/#2117787d7d87. Some argue that the profiling information should be shared between companies, see, e.g., Kurt Collins, *A case for making it easier to personalize IoT devices*, TECHBEACON, https://techbeacon.com/app-dev-testing/case-making-it-easier-personalize-iot-devices (last visited July 11, 2021). On the privacy concerns that this raises, *see* 2016 O.J. (L 679) 119; Makker, *supra* note 19.

222. *See, e.g.*, FORBES INSIGHTS, *supra* note 221; Ferguson, *supra* note 14, at 818; Nikole Davenport, *Smart Washers May Clean Your Clothes, But Hacks Can Clean Out Your Privacy, and*

of collecting information and making inferences to personalize the operation of smart-devices peaks with Personal Assistant Services (hereinafter, PAS) such as Siri, Alexa, or Google Assistant.[223] The information PASs collect about the user from the particular smart-device is combined with information they collect from other sources, including information from other smart-devices or from other services they operate.[224] Based on this aggregation, PASs can better answer users' needs, and therefore lure in more users, which in turn provides even more information, continuing the cycle.[225]

By operating multiple sensors in millions of devices, prime-operators can observe countless comparable products and aggregate various information about specific products. The ability to continuously generate information about products located in smart-fridges—big data about such products—is a new feature facilitated by innovative technology that only actors that operate millions of smart-devices can take advantage of.[226] Using this data, the operators can make inferences

---

Underdeveloped Regulations Could Leave You Hanging on a Line, 32 J. MARSHALL J. INFO. TECH. & PRIV. L. 259, 268–70 (2016).

223. *See, e.g.*, Dan Feldman & Eldar Haber, *Measuring and Protecting Privacy in the Always-On Era*, 35 BERKELEY TECH. L.J. 197, 219 (2020) (discussing data collected by Amazon's Echo); David K. A. Mordecai, *Automated Personal Assistants with Multiple Principals: Whose Agent Is It?*, AM. BAR ASS'N (Jan. 17, 2020), https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2020/winter/automated-personal-assistants-multiple-principals-whose-agent-it/; Tom Mighell, *The Modern Personal Digital Assistant*, LAW PRAC. MAG., Jan./Feb. 2016, at 30. For a technological explanation on PAS's operation of several devices, see *Understand the Smart Home Skill API*, AMAZON ALEXA, https://developer.amazon.com/en-US/docs/alexa/smarthome/understand-the-smart-home-skill-api.html (last visited Jan. 14, 2020); Daniel Myers, *IoT & Google Assistant*, MEDIUM (Jan. 22, 2019), https://medium.com/google-developers/iot-google-assistant-f0908f354681.

224. *See, e.g.*, Peppet, *supra* note 30, at 122–24.

225. As Stucke & Grunes explain, "[T]he more people who actively or passively contribute data, the more the company can improve the quality of its product, the more attractive the product is to other users, the more data the company has to further improve its product, which becomes more attractive to prospective users." *See* MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY 170 (2016). Network theory relates to this as preferential treatment mechanism, or "the rich get richer" effect, see, e.g., Katherine J. Strandburg et al., *Law and the Science of Networks: An Overview and an Application to the "Patent Explosion"*, 21 BERKELEY TECH. L.J. 1293, 1308 (2006). *See also* Brill & Jones, *supra* note 14, at 1199; Matt Day, *Your smart light can tell Amazon and Google when you go to bed*, BLOOMBERG (Feb. 12, 2019), https://www.bloomberg.com/news/articles/2019-02-12/your-smart-light-can-tell-amazon-and-google-when-you-go-to-bed. On the antitrust concerns that this causes, see generally *supra* note 172.

226. A useful definition of big data is "the collection of large amounts of data or information and the ability to analyze it in a meaningful way." *See* Christopher C. French, *The Big Data Revolution and Its Impact on the Law*, 123 PENN ST. L. REV. 585 (2019). For a discussion about the difficulties of other actors to collect, access and use such big data, see generally Daniel L. Rubinfeld & Michal S. Gal, *Access Barriers to Big Data*, 59 ARIZ. L. REV. 339 (2017).

about the traits of similar products and apply those to make predictions about specific products in specific smart-fridges.[227]

By combining informational advantages with superior data analysis capabilities, prime-operators can personalize the smart-devices in ways that other operators could not.[228] Collecting such data, conducting such analysis, and providing such inferences are relatively cheap for prime-operators, especially once smart-devices are in extensive use, and they employ massive data analysis processes precisely for these reasons.[229] Gathering those inferences is not only cheaper for prime-operators, it is realistically almost always available only to them—given their unique access to millions of data points.[230] Moreover, once such inference is found, discovering traits and features of specific products in specific smart-fridges is even easier and cheaper.[231]

Consider two examples that illustrate how prime-operators can gather information that other operators could not (or would have trouble gathering) and use it to prevent physical harms to users.

First, consider a drug that must be refrigerated and cannot be used thirty days after its first use. Tom felt sick one day, bought the drug, used it, and stored it in the smart-fridge. After a few days of use, he felt better and forgot about the drug. The prime-operator could use sensors inside the device to track Tom's consumption of this drug—to find out exactly what kind of drug it is, what its expiration date is, when it was first used, infer how much time has passed since, how many doses Tom used and how many more he should use, and when

227. This is standard practice for the application of big data, see, e.g., FEDERAL TRADE COMMISSION, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? 1–12 (2016); STUCKE & GRUNES, *supra* note 225, at ch. 2; Peter Segrist, *How the Rise of Big Data and Predictive Analytics Are Changing the Attorney's Duty of Competence*, 16 N.C. J.L. & TECH. 527, 559–74 (2015); Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 253 (2013) (explaining the predictive analysis benefits of big-data).

228. The use of big data to personalize is similar in the case of smart-devices and in other platforms. Yochai Benkler put this point well: "Big data collection and processing, combined with ubiquitous sensing and connectivity, create extremely powerful insights on mass populations available to relatively few entities. These insights, together with new computational methods, make up what we think of as 'big data.' As Zeynep Tufekci has explained, when these methods combine with widespread experimentation (as in the Facebook experiments), behavioral science that analyzes individuals in a stimulus-response framework, and increasingly on-the-fly personalization of platforms, platform companies can nudge users to form beliefs and preferences, follow behaviors, and increase the probability of outcomes with ever-finer precision." Benkler, *supra* note 74, at 23.

229. *Id.*; *see supra* notes 225–27.

230. *See* s*upra* note 226.

231. *See supra* notes 225–27.

the last date of use should be.[232] In this case, the prime-operator could prevent the injury that might be caused to Tom if he were to consume the drug after the expiration date or against the recommended amount for use. Preventing this damage is relatively cheap and easy for the prime-operator once it has the technology to monitor the products in the smart-fridge.[233] Since individuals tend to be bad at tasks such as remembering expiration dates or counting doses over days, prime-operators can use their abilities to provide valuable social services.[234]

Second, a prime-operator might examine millions of milk jugs and find that when the milk turns sour, the bottle or package expands at some measure that is identifiable by the devices' sensors. The inference provided by the prime-operator about the milk would be more nuanced, and arguably more accurate, than the expiration date that is ordinarily mentioned on the packages, since the former analyzes the condition of the specific product while the latter is general. Achieving this information requires resources for collecting and analyzing copious amounts of data, which in turn requires access to millions of equivalent products and computing powers to make significant inferences about them.[235] In practice, this information is uniquely available to prime-operators.

In both examples, prime-operators translate their considerable informational and technological advantages into a (comparatively) cheap and effective ability to accurately detect possible future physical harms to users. Once detected, prime-operators could use the features of the smart-fridge to notify the user about the harm or otherwise prevent them from misusing the products in the smart-fridge.[236] While in theory, such data collection and inferences can be achieved by every operator, practical limitations of scale, money, and computing

232. Needless to say, gathering such information is already technologically possible for many smart-fridges, and many more will have such abilities in the near future. *See* Stables, *supra* note 2; Dami Lee, *Samsung and LG go head to head with AI-powered fridges that recognize food*, THE VERGE (Jan. 2, 2020, 2:11 PM), https://www.theverge.com/2020/1/2/21046822/samsung-lg-smart-fridge-family-hub-instaview-thinq-ai-ces-2020.

233. *See supra* notes 226–31.

234. Gal, *supra* note 43, at 76–91.

235. *See supra* notes 226–27.

236. Arguably, such informational advantage and social value might justify holding PASs liable for not preventing such damages. *See generally* R. H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960); Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV 1089 (1972); Steven Shavell, *Liability for Accidents*, *in* HANDBOOK OF LAW AND ECONOMICS 139 (A. Mitchell Polinsky & Steven Shavell, eds., 2007); Omri Rachum-Twaig, *Whose Robot Is It Anyway?: Liability For Artificial-Intelligence-Based Robots*, 2020 U. ILL. L. REV. 1141 (2020).

powers make those skills uniquely available to a handful of prime-operators. To conclude, those prime-operators have significant advantages in creating and refining the operation of smart-devices, which allows them to benefit (or harm) users in unique ways.[237]

B. Moderating Powers

The remote operability of smart-devices invites more actors into the relationship between the user and the smart-device.[238] These additional actors, the operators, can have access to different digital functions of the smart-device and activate those to impose personalization and constraints on users.[239] So far, our discussion assumed that only one operator operates the device at any given time. To probe this assumption, let us distinguish between access and operation to smart-devices.

Interconnectivity of smart-devices allows multiple operators to *access* the smart-device and send commands to its digitized functions. In ordinary cases, nothing limits mutual access to the digital functions by different users at the same time.[240] However, *access* to the smart-devices and *operation* of the smart-devices are different. While access relates to the ability to connect and send commands to the device, the operation of the device also involves making its physical functions perform certain actions or carry out certain personalization policies. Importantly, unlike access to the code that operates the smart-device, operating smart-devices' physical functions and using those to apply personalization policies is often rivalrous—one actor's operation of the smart-device often hinders another's.[241]

Consider a simple situation: two operators wish to set the smart-fridge's temperature. Both operators have access to the smart-device and can send commands to the digitized thermostat that controls the device's temperature. When Anne sets the temperature to 35°F and Ben sets it to 39°F, their desired operation of the device becomes rivalrous since the two choices contradict one another and are mutually exclusive. Naturally, since smart-devices facilitate much more complicated operating scenarios, as discussed above, a wide array of conflicts are expected between the different operators operating the device. For instance, conflicting personalization policies can involve

237. As noted, these raise antitrust concerns, see *supra* note 172.

238. *See supra* Part I.A.

239. *See supra* Part III.

240. *See supra* note 26.

241. On the rivalrousness of codes, see, e.g., Joshua A.T. Fairfield, *Virtual Property*, 85 B.U. L. REV. 1047, 1049 (2005).

one operator limiting a certain user from consuming more than one beer per day, while another might set the limitation at two beers.

Conflicting operation of smart-devices by different operators is a problem that requires solutions in the form of rules. Consider a simple rule determining that commands will be executed whenever they are received, regardless of other commands. Continuing our previous example, upon Anne's command, the smart-fridge's temperature will be set at 35°F, but later will be changed to 39°F upon Ben's command. In this case, the rule that was set resulted in Anne's operation being overridden by Ben's. Thus, in practice, operator Ben's power and expectation of being able to operate the device trumped Anne's powers and expectation. The desirability of such outcome depends on the details of the case—we might favor it if Anne is the virtual assistant that the manufacturer operates and Ben is the user, and we might object to it if Anne is the parent and Ben is the neighbor's child.

More to our point, any rule aimed to solve the conflicting operation of smart-devices is designed and applied by someone.[242] Prime-operators determine and apply the rules that govern the operation of smart-devices, they hold the power to decide which operation will prevail in different circumstances.[243] This is the *moderating power* of the prime-operators.

Since smart-devices technology empowers different operators to operate the smart-devices in ways that often conflict,[244] rules that govern the operation of different operators are inevitable. This, in turn, makes the prime-operators—actors that moderate the operation of smart-devices, determine the rules, and apply them—also necessary.[245] Prime-operators face difficult questions as they use their moderating powers to solve conflicts between operators. Importantly, like other moderators of innovative technologies, prime-operators are compelled to weigh in on those questions and cannot hide behind a veil of neutrality.[246]

In using their moderating powers, prime-operators ought to face questions like: Should parents be allowed to limit the speed of the car

242. *Cf. supra* note 98.

243. Arguably, they hold second-order legal powers to determine who operates the device, see *supra* Part III.C.

244. *See supra* Part I.A.

245. *See supra* Part IV.B.

246. On choice architecture see generally THALER & SUNSTEIN, *supra* note 168. On the a-neutrality of technology regulation, see generally Michael Birnhack, *Reverse Engineering Informational Privacy Law*, 15 YALE J. L. & TECH. 24 (2012); Marcelo Thompson, *The Neutralization of Harmony: The Problem Of Technological Neutrality, East and West*, 18 B.U. J. SCI. & TECH. L. 303 (2012).

for their children? Or their beer consumption? If so, until what age? And could these regulations be applied remotely, say, when their children move to another state?[247] On a different note, could private companies be allowed to buy access to smart-devices operations? If so, from whom? And would user-operators be able to override those companies' operations?[248] Also, would the state be allowed to operate features of smart-devices—either as broad policies applied by the prime-operator or specific operations directed to specific people?[249] Could user-operators override the state's operation?[250] More generally, when could users override the constraints imposed by certain operators?[251] Who can the user approach if they have been wronged by such an operation?[252] And what should be the legal standard of review for such a claim?

In many cases, the prime-operators that hold moderating powers will be the PAS. PASs often create the technological infrastructure that facilitates the operation of different smart-devices for other actors, from users to manufacturers.[253] Relatedly, their wide reach allows them to operate various kinds of smart-devices, strengthening their moderating powers.[254] Their informational and market advantages make users and sellers alike more inclined to use PASs' moderating services.[255] PASs also use those powers to force customers to use their moderating services, as part of a "take it or leave it" deal for the entire smart-device.[256] All those features drive most users and operators to rely on PASs for the operation of smart-devices. By creating the platforms that all other operators use to operate the devices, PASs assume the role of prime-operators.[257] They are the ones that have to

247. *See supra* notes 46–51.

248. *See supra* notes 140–43, 157–59, 216–21. For instance, the Samsung smart-fridge warranty limits the users power to contact third-parties to change or modify the device under penalty of limited warranty, see SAMSUNG, REFRIGERATOR: USER MANUAL 13.

249. *See supra* Part I.A.2.

250. *See supra* note 160–62.

251. *See, e.g.*, Grinvald & Tur-Sinai, *supra* note 193, § I, III (arguing for a regulatory change that would ensure users' right to repair smart-device); *see* Kilovaty, *supra* note 42 (arguing for hacker's right to hack smart-devices to audit the code for risks to consumers).

252. This could be operator's services such as Facebook's Board, see generally Kate Klonick, *The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression*, 129 YALE L.J. 2418, 2424–25 (2020). Or a state-operated mechanism such as the consumer protection, see McMahon, *supra* note 172.

253. *See supra* note 225.

254. *See supra* Part IV.A.

255. ZUBOFF, *supra* note 64, at ch. 10; Crootof, *supra* note 41; Benkler, *supra* note 74.

256. This is sometimes referred to as partnership transfers of data. *See, e.g.*, ERIN EGAN, DATA PORTABILITY AND PRIVACY 10 (2019).

257. *Cf.* PERZANOWSKI & SCHULTZ, *supra* note 191, at ch. 2, 8 (arguing that manufacturers have similar powers for similar reasons).

set the rules regarding the conflicting operation of smart-devices by different operators using their platforms.[258] Therefore, they are the ones that currently answer the questions posed in the previous paragraph.[259]

Given prime-operators' powers to moderate personalized constraints using smart-devices, a *laissez-faire* regulatory policy is not likely to safeguard users' interests.[260] Such approach merely leaves users at the mercy of more powerful private actors, who often bear no liability in regard to users' interest being trampled by operators.[261] Thus, prime-operators' moderating powers call for a change of focus: while with regards to ordinary operators, the question was "Should we allow them to operate?" with regards to prime-operators' moderating powers, the question is rather "How should we guide their moderation?"

We should start thinking about smart-devices' prime-operators much like content moderators on social media, as the actors that set the rules regarding what can be done on the platforms they control.[262] Like content moderators in social media, prime-operators should not be allowed to hide behind a false façade of neutrality. Considering the physical aspect of smart-devices' operation[263] and the expected prevalence of smart-devices,[264] developing scholarship that confronts the regulations of prime-operators is vital. The next and final Part of this Article will take the first steps in that direction.

C. Before Legal Intervention

The regulation of prime-operators is more complicated than the regulation of ordinary operators. While prime-operator's immense power, as identified here, might be intimidating and itself might justify some regulatory intervention,[265] these powers also allow prime-operators to uncover great social benefits that would probably be spared if those actors would be regulated to a freeze.[266] In addition, the regula-

258. *See supra* Part II.C.1; Grimmelmann, *supra* note 96, at 1729.

259. This is a contingent situation, as indirect legal regulation of such moderation is always available and often advisable. *See, e.g.*, Madeline Byrd & Katherine J. Strandburg, *CDA 230 for a Smart Internet*, 88 FORDHAM L. REV. 405 (2019); *infra* Part IV.C.

260. *See* Berlin, *supra* note 176.

261. *See supra* note 210–13; *see also* Crootof, *supra* note 41.

262. *See generally* James Grimmelmann, *The Virtues of Moderation*, 17 YALE J. L. & TECH. 42 (2015); Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598 (2018).

263. *See supra* notes 55–56, 73–74.

264. *See supra* note 7.

265. *See supra* note 215–19.

266. *See supra* notes 232–37.

tion of prime-operators involves complicated questions about regulating private actors that themselves regulate other operators.[267] These questions cannot be swept aside by adopting a *laissez-faire* approach, which merely shifts the burden to the prime-operators to make all the hard choices.[268]

Luckily, developing regulation against this background—the social interest in unveiling unknown benefits and the inherent need to moderate alongside the desire for proper moderation—is not unheard of. It resembles the conditions for the regulation of a similar technology at a similar developmental stage to that of smart-devices today: the Internet in the late 1990s. Following is a very brief presentation of this familiar story.

In the dawn of the Internet age, a question arose about the liability of Internet Service Providers (ISPs) and websites in terms of content that users publish on their platforms.[269] Two of the earliest cases that discussed this issue reached opposite conclusions: while one held that the ISPs were not liable for content published on its site, the other held that it is responsible for the content published on it, and hence, liable for legal claims regarding such content.[270]

Understanding the enormous potential of the Internet as a new sphere for deliberation and speech holding previously unimaginable possibilities, neither conclusion was satisfactory. On one hand, it warned companies that by developing content-sharing platforms for the Internet, they might be held liable for considerable damages for user-generated content published on their platforms. On the other hand, it incentivized those companies that do invest in the field to refrain from any content vetting, since too much control would deem them liable. In simple terms, websites that wanted to develop the Internet could either adopt the 4chan.org model of non-intervention or risk liability, clearly a disconcerting choice.

---

267. *See, e.g.*, Elizabeth R. Pike, *Defending Data: Toward Ethical Protections and Comprehensive Data Governance*, 69 EMORY L.J. 687 (2020).

268. *See supra* notes 260–61.

269. On the familiar story of Section 230, see generally Ryan French, *Picking up the Pieces: Finding Unity after the Communications Decency Act Section 230 Jurisprudential Clash*, 72 LA. L. REV. 443 (2012); Vanessa S. Browne-Barbour, *Losing Their License to Libel: Revisiting § 230 Immunity*, 30 BERKELEY TECH. L.J. 1505 (2015); Julio Sharp-Wasserman, *Section 230(c)(1) of the Communications Decency Act and the Common Law of Defamation: A Convergence Thesis*, 20 COLUM. SCI. & TECH. L. REV. 195, 201–11 (2018).

270. *See generally* Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991); Stratton Oakmont, Inc. v. Prodigy Servs. Co., 23 Media L. Rep. 1794 (N.Y. Sup. Ct., Dec. 11, 1995).

Congress addressed the problem by enacting § 230 to the Communication Decency Act.[271] Congress found that "[t]he rapidly developing array of Internet and other interactive computer services" holds extraordinary opportunities for diversifying discourse, for cultural developments, and for intellectual activities.[272] It held that the free market is the best way to nurture and harvest the potential fruits of the Internet.[273] To remove disincentives for private companies to both develop the Internet and filter objectionable content, Congress determined that ISPs will not be held liable for content published by users, nor for actions taken in good faith to limit access to "objectionable" content.[274] Put simply, by enacting § 230, Congress aimed to promote the development of the Internet as a space for robust communication. It envisioned a vibrant network developed and self-regulated by private actors, wherein content could be shared in ways that did not seem possible before.[275]

Congress was right. Private companies have, in fact, facilitated the benefits of online content sharing for billions of people in ways that were hardly imaginable, let alone accessible, only decades ago. They also initiated and developed different moderating standards for the operation of such technologies.[276] While those can and should be publicly scrutinized, it is very doubtful that better platforms or more desirable rules would have been employed more quickly, had the state not created the regulatory environment for this technology to develop. Thus, despite considerable shortfalls of today's Internet, it is hard to imagine how all the benefits of content sharing would have been developed without § 230.[277] Challenging this claim requires one to explain how companies like Facebook, YouTube, Google, or Yelp could have created their services in the first place, in light of significant damages liability at their very earliest stages.

By now, I hope the resemblance between the Internet in the 1990s and today's smart-devices is clearer. Both involve infant, innovative technologies, based on interconnectivity; both hold potential for a

271. 47 U.S.C. § 230. For a discussion about these cases and the incentives for § 230, see *supra* note 269.

272. § 230(a).

273. § 230(b).

274. § 230(b)–(c).

275. Zeran v. Am. Online, Inc., 129 F.3d 327, 330–31 (4th Cir. 1997); Force v. Facebook, Inc., 934 F.3d 53, 63 (2d Cir. 2019); Browne-Barbour, *supra* note 269, at 1519–38; French, *supra* note 269; Varty Defterderian, Fair Housing Council v. Roommates.com*: A New Path for Section 230 Immunity*, 24 BERKELEY TECH. L.J. 563, 581 (2009).

276. *See, e.g.*, Klonick, *supra* note 262.

277. On § 230 as regulating the "secondary liability regimes," see Byrd & Strandburg, *supra* note 260.

myriad of social benefits, some already foreseeable and some still on the horizon; and both are driven (at this stage) by private enterprises that rely on unique technological abilities and market powers to create services for users. Moreover, both are built around new forms of interaction between users and operators, and thereby, on the one hand, require expedient regulation to protect users, and on the other hand, should not be regulated to a halt. It is true that liability for speech harms on Internet platforms is not synonymous with liability for physical damages of smart-devices' users, mainly because of the various First Amendment considerations involved in the former and not the latter.[278] But the similarities between the cases, namely the possibility of foregoing unknown benefits of a promising technology and the need to develop and apply fair moderation standards for rapidly changing technologies, should not be ignored.

As long as one accepts the premises of § 230 for the regulation of the Internet—the desirability of the technology that could provide a myriad of avenues of human flourishing, the need to encourage such technology by removing private companies' disincentives to develop it, and the ability of the operators to self-regulate[279]—one should at least consider a similar regulatory approach for prime-operators of smart-devices. Arguably, the successful development of the Internet supports applying the same approach to smart-devices—granting prime-operators similar legal powers to operate scores of devices. To some extent, it also supports the legal power to moderate the use of other operators, albeit while requiring transparency regarding the guidelines to such moderation, which would encourage the social and scholarly scrutiny we see regarding today's social media moderation.[280]

A few caveats are in order. The case for operators' immunity, just like the case for ISPs immunity, is not limitless.[281] Even a free-market policy that supports self-regulation could, and arguably should, be limited when important countervailing values are on the line.[282] Moreover, this argument focuses on smart-devices technology at this

278. For the applicability of First Amendment considerations, see generally Note, *Section 230 as First Amendment Rule*, 131 HARV. L. REV. 2027 (2018); *Zeran*, 129 F.3d at 330–31; Defterderian, *supra* note 275; French, *supra* note 271.

279. *See supra* notes 275–77.

280. *See, e.g.*, Klonick, *supra* note 262.

281. Marshall's Locksmith Serv. Inc. v. Google, LLC, 925 F.3d 1263, 1272 (D.C. Cir. 2019).

282. *See generally* Allow States and Victims to Fight Online Sex Trafficking Act of 2017, H.R. 1865, 115th Cong. (2018); Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008); Doe v. Internet Brands, Inc., 824 F.3d 846 (9th Cir. 2016); Browne-Barbour, *supra* note 269, at 1538–47; Defterderian, *supra* note 275, at 568.

particular point in time. The incentives scheme discussed does not necessarily apply when the technology becomes well-established, once the economic benefits are more accessible, once the business risks are diminished, or once the shortfalls of self-regulation require the attention of policymakers.[283] In other words, regulatory policies can be relaxed in their infancy stage for promising technologies, but nuanced and stricter measures will be necessary as these technologies mature.[284]

Conclusion

The rise of smart-devices poses various legal and social challenges. This Article focused on often-ignored legal questions that smart-devices bring to the forefront. It provided an initiatory analysis of personalization within the context of smart-devices and discussed some of the key legal queries it raises.[285] The discussion also shed much-needed light on the operators of smart-devices. It underscored the importance of recognizing that smart-devices introduce new actors into the relationship between users and devices, and suggested fresh perspectives towards the regulation of these new and complicated relationships.[286] Finally, it also placed prime-operators on the pedestal they deserve, by arguing that they have unique, extraordinary powers to operate smart-devices to benefit society, while also holding powers to moderate between different operators. As such, this Article stressed that prime-operators of smart-devices pose challenges that resemble social media moderators, and thus, deserve equal attention from legal scholarship and regulators.[287]

Another contribution that this Article offers to the complicated and multifaceted legal scholarship about IoT and smart-devices relates to the method of analysis pursued here. It emphasized that in order to facilitate a meaningful debate about these topics, it is necessary to first understand the nuts and bolts of the relevant technology.[288] To wit, this Article used a mundane and simple example of smart-fridges to create the preface about the technology of smart-devices. This technological background was used to identify and explore concepts that are

283. Biden v. Knight First Amend. Inst. at Columbia Univ., 141 S. Ct. 1220, 1222 (2021).

284. *See* Nw. Airlines v. Minnesota, 322 U.S. 292, 300 (1944).

285. *See supra* Part II.

286. *See supra* Part III.

287. *See supra* Part IV.

288. *See, e.g.*, Lyria Bennett Moses, *Recurring Dilemmas: The Law's Race to Keep Up With Technological Change*, 2007 J.L. Tech. & Pol'y 239 (2007); Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 Yale J.L. & Tech. 59 (2013).

relevant for regulating this technology, and formed the factual basis on which legal and regulatory questions were discussed.

This Article also wished to broaden the scope of scholarship about smart-devices by focusing on underexplored legal paths. To this end, various legal concerns posed by smart-devices were mostly set aside in this Article, including personal data and privacy infringements,[289] cybersecurity,[290] or the Fourth Amendment.[291] Vital as these may be, legal scholarship about law and technology generally, and about smart-devices and IoT specifically, would benefit from exploring other questions more rigorously. While these are important topics, trying to solve the vast legal issues that smart-devices bring forth by continuously involving and modifying those concepts is ill-advised, the extensive use weakens those legal concepts while ignoring many important questions in the field. Significantly, this Article aimed to show how law issues discussed in the law and technology realm can be integrated within and contribute to well-establish legal theory discussions.

Finally, this Article sought to establish a foundation for a more elaborate legal conversation about the challenges of smart-devices. It included the first steps towards clarifying the role of personalization, operators, and prime-operators within the framework of smart-devices. Doing so, it invites future contributions to hone the understanding of these issues and develop more detailed regulations to govern it.

289. For articles discussing the privacy concerns that arise from IoT, see, e.g., McMahon, *supra* note 172; Stefan Ducich, *These Walls* Can *Talk! Securing Digital Privacy in the Smart Home Under the Fourth Amendment*, 16 DUKE L. & TECH. REV. 278 (2018); Branden Ly, *Never Home Alone: Data Privacy Regulations for the Internet of Things*, 2017 U. ILL. J.L. TECH. & POL'Y 539 (2017); Laura DeNardis & Mark Raymond, *The Internet of Things as a Global Policy Frontier*, 51 U.C. DAVIS L. REV. 475 (2017); Alexander H. Tran, *The Internet of Things and Potential Remedies in Privacy Tort Law*, 50 COLUM. J.L. & SOC. PROBS. 263, 265–73 (2017); Williams, *supra* note 29, at 14–16, 22; Peppet, *supra* note 30, at 129–33.

290. *See supra* note 149.

291. *See, e.g.*, Gabriel Bronshteyn, *Searching the Smart Home*, 72 STAN. L. REV. 455, 470–79 (2020); Haley Napier, Carpenter v. United States*: The Stored Communications Act is Not a Permissible Mechanism to Obtain Data from Smart Home Devices*, 45 U. DAYTON L. REV. 163 (2020).