The Devil Is in the Defaults

Ian Kerr*

Abstract

This review essay explores the notion of "shifting defaults" as discussed by Mireille Hildebrandt in her book *Smart Technologies and the End(s) of Law*. Although readers might mistakenly see defaults as a fleeting topic within Hildebrandt's text, this review essay demonstrates their central significance, identifying and elaborating on fundamental characteristics of four categories of shifting defaults: (i) natural defaults; (ii) technological defaults; (iii) legal defaults; and (iv) normative defaults. The essay concludes by reframing Hildebrandt's central question, considering whether the Rule of Law is itself merely our current legal default, and whether it could be legitimately displaced by smart technologies.

I. Introduction

Although it will surely cause discomfort to some, very few members of an increasingly tech-savvy legal profession would be surprised by claims that advances in robotics and artificial intelligence will revolutionize the delivery of legal services and transform the practice of law.[1] But *here* is a truly disquieting thought: what if "modern law is dependent on and shares the affordances of the printing press . . . and, ultimately . . . under the next dominant information and communications infrastructure, law as we know it might be gone"?[2]

In her perspicacious new book, *Smart Technologies and the End(s) of Law,* Mireille Hildebrandt, philosopher, lawyer, and internationally renowned expert in intellectual macramé, examines this and other core questions at the nexus of philosophy of technology and philosophy of law. In a stunning display of rigor and discipline, Hildebrandt weaves together a dazzling array of key sources from law, philosophy, computer science, psychology, sociology, anthropology, science and technology studies, and other fields, exercising some of the very best lateral thinking I have seen in the past decade.

---

* Canada Research Chair in Ethics, Law and Technology, University of Ottawa, Faculty of Law. Contact: iankerr@uottawa.ca. I would like to thank Dustin Moores for his tireless enthusiasm, his ability to find anything under the sun and for the high quality research assistance that he so regularly and reliably provides. Thanks also to Ryan Calo, Woodrow Hartzog and Jason Millar for insightful feedback on an earlier draft. Finally, thank you to Mireille Hildebrandt for her superb and inspiring scholarship, her many intellectual contributions to our community, and for the honor of including me to participate in this book forum with such eminent scholars in the field.

[1] Richard Susskind & Daniel Susskind, The Future of the Professions: How Technology Will Transform the Work of Human Experts (2015); Julie Sobowale, How Artificial Intelligence is Transforming the Legal Profession, ABA J. (Apr. 1, 2016), http://www.abajournal.com/magazine/article/how_artificial_intelligence_is_transforming_the_legal_profession.

[2] Mireille Hildebrandt, Smart Technologies and the End(s) of Law 176 (2015).

ISSN 2291-9732

Commencing with a compelling day-in-the-life narrative, she illustrates how smart technologies will catalyze the coming shift from life online to an "onlife world"—"a transformative life world, situated beyond the increasingly artificial distinction between online and offline . . . thriv[ing] on artificial life forms, or at least on 'things' that seem to develop a life of their own" (8). As Hildebrandt goes on to explain, through autonomic computing and emerging techniques in machine learning, these "data-driven agents" will generate the capability to profile us, and to predict and preempt many of our day-to-day activities. Without our help (often, without our awareness), they will anticipate and serve our preferences and, in some instances, reconfigure them. Imagining, as she does, a world in which we have delegated many of our daily decisions to machines, devices that we come to rely upon to anticipate our needs and accomplish our goals, Hildebrandt warns that smart technologies have the potential to threaten fundamental rights including: privacy, identity, autonomy, non-discrimination, due process, and the presumption of innocence.

In 226 pages of erudite, urbane investigation, Hildebrandt offers an extremely sobering synthesis that details the character of the threats that smart technologies pose to fundamental rights and to the end(s) of law. One intriguing thing about her book, however, is that despite these threats, she believes that "[t]here is no way back, we can only move forward" (214). With no turning back Hildebrandt instead forewarns that the only thing able to save the Rule of Law as we know it is "legal protection by design." These legal protections are not meant simply to forbid preemptive computing when it interferes with fundamental rights.[3] Rather, Hildebrandt follows a well-entrenched regulate-by-design approach, recommending two mechanisms for legal reform as examples of how the legal protection by design method can be baked directly into the emerging information and communications infrastructure. These and other such mechanisms are meant to ensure that not only our fundamental rights, but also the very fabric of modern law, remain intact. To whet appetites, I will quickly mention her two primary examples, both of which are too complicated to fully develop in my brief description. After that, I will turn my focus to a recurring theme in the book: the shifting defaults in our technological and legal architectures.

First, Hildebrandt recommends the creation of a legal obligation to provide the socio-technical infrastructure necessary to enshrine "counter-profiling" as a fundamental right. Performing an analogous role to "freedom of expression" in our inherited legal infrastructure (which she argues was constructed as a result of the affordances of the printing press),[4] the right to counter-profile would entail that the objects of profiling be-

[3] This is an approach that I had suggested in an earlier volume co-edited by Hildebrandt. See Ian Kerr, Prediction, Preemption, Presumption: The Path of Law After the Computational Turn, in Privacy, Due Process and the Computational Turn (Mireille Hildebrandt & Katja de Vries eds., 2013); see also Ian Kerr & Jessica Earle, Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy, 66 Stan. L. Rev. Online 65 (2013).

[4] As Hildebrandt puts it: "In many ways, counter-profiling has the same function as the free press had in the era of books and newspapers. From the perspective of the Rule of Law, the right to freedom of information has horizontal effect and may include a positive obligation on the state to ensure that the right is effective" (223).

come agents of profiling, rendering them capable of conducting data mining operations on the behaviors of those that are in the business of profiling. It is crucial to understand, however, that this prescription is far more than merely sanctioning audits or permitting counter-profiling as an activity. It is a much bigger deal than that. Hildebrandt is recommending a legal requirement that we build a technological infrastructure that would allow everyone the continuous ability to watch the watchers. Such a change to our infrastructure would be a serious and contentious commitment to transparency.

Second, Hildebrandt advocates the adoption of "morphological computing" as a means of diminishing dependence on central control models of intelligence. "Morphological computing refers to the embedded nature of cognition, which enables granular adaptive responses by body parts based on the morphology of that particular part instead of being initiated by a control mechanism like the brain" (29). Although it is unclear whether this kind of computation would likewise become an actual legal requirement, to the extent that more morphological computation means less data-driven computation, dictating the use of such techniques accords with the prime directive of "big data space": namely, data minimization.[5]

One of the things I admire about Hildebrandt's book is the way in which it moves beyond Lessig's famous watchword that "code is law."[6] Following on Joel Reidenberg's classic work on the formulation of information policy rules through technology,[7] Lessig was among the first technology lawyers to recognize as dangerous the strategy of using preemptive technologies as a means of regulating conduct.[8] As Hildebrandt depicts the strategy, "If the idea is to influence behavior instead of addressing action, and if the means are interchangeable, why not opt for a means that is less visible, less contestable and thus more influential in getting people to behave in alignment with policy objectives?" (165). Hildebrandt opposes this strategy and provides several successful counter-examples throughout the book. However, Hildebrandt's disquisition is not simply about the perils of such techno-regulation or how best to address them. In addition, Hildebrandt calmly, meticulously, and persuasively offers a philosophically rich account that explains how smart technologies might alter the modality of law's existence. Her book isn't just about how to debug legal code in order to hold techno-regulation in check. Although she does offer proposals in that regard, her central purpose is to provide an ontological account of the nature of law through an examination of its philosophical entanglements with technology. It is a tall order and she rises to the occasion. *Luddite jurisprudes, take notice:* your understanding of the philosophy of law is impoverished and

---

[5] According to Hildebrandt, morphological computing permits many of our transactions with data-driven agents to escape the storage and searchability of human behaviors, enabling smooth and safe interaction with humans based on the physical design of robots, instead of being based on the data-driven computations in their central processing units.

[6] Lawrence Lessig, Code 2.0 (2d ed. 2006).

[7] Joel R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules Through Technology, 76 Tex. L. Rev. 553 (1997).

[8] Rather than using law to redress wrongs ex post.

incomplete without also understanding the affordances of the information and communications infrastructure that makes any given modality of law possible. As Hildebrandt makes clear, law and technology are intricately entangled.

II. Shifting Defaults

As even my cursory overview of the book reveals, there are many fascinating aspects of *Smart Technologies* worthy of dissection and discussion. This review essay will focus on what some readers might mistakenly see as a fleeting topic within the text—the important role of *defaults*—taking its cue from Hildebrandt's insightful observation in her prefatory remarks, which practically jumped off the page and looked me in the eye:

> We are on the verge of shifting from *using technologies* to *interacting with them*, negotiating their defaults, pre-empting their intent while they do the same to us (ix, emphasis in the original).

Although the observation is not novel, I see the shift that Hildebrandt is describing as profound—a kind of *gestalt shift*. One of its key elements is that we are coming to understand smart objects as agents. That is, their ontological status is already shifting from one end towards the middle of a continuum. Psychologist Peter Kahn and colleagues were among the first to see this, proposing a new ontological category for robots due to the difficulty subjects in experimental studies displayed in trying to categorize robots as animate or inanimate.[9] No longer simply things but by no means persons. Not rights-bearing entities but not merely toasters either. A second vital element in the shift that Hildebrandt is describing is that these agents have the ability to preempt our intentions—so much so, that we begin to interact with them in a kind of tango, anticipating their next move to ensure that it is consonant with our own. We start to act in a way that ensures our technologies will act in a way that comports with our preferences. And they do the same. These two shifting aspects of smart technologies—agency and reciprocity—build on a well-entrenched understanding of the capacity of artificial agents to participate in networks.[10]

It is the third element that Hildebrandt mentions in her preface that caught me off-guard. As she describes it, the transformation to smart technologies and what she calls the onlife precipitates *a shift in defaults*. Not just a shift in the default ontological status of objects from inanimate things to interactive agents (as if that weren't significant enough). But also, as she describes, a *shift* in the very nature of *shifting defaults*. Before we had sophisticated machines, it used to be that only nature or humans could be the exclusive architects of our default settings. Now, the defaults settings of the onlife will be negotiated with and by machines without our intervention or oversight. To me, this is a *tectonic shift*.

Scattered throughout the work, Hildebrandt devotes nearly fifteen pages to a series of interesting snippets on shifting defaults. Although she does not draw many connections between them and does not provide a typology as such, my contribution in

---

[9] Peter H. Kahn, Jr. et al., The New Ontological Category Hypothesis in Human-Robot Interaction, Proceedings of the 6th International Conference on Human-Robot Interaction, ACM, 2011.

[10] Bruno Latour, Reassembling the Social: An Introduction to Actor-Network-Theory (2005).

this review essay is to organize these snippets into basic categories and elaborate on some of their fundamental characteristics. This additional understanding of our shifting defaults will help us understand the magnitude of the potential impact of smart technologies on what must also be understood as the shifting nature of law itself.

Without actually saying so, I believe that Hildebrandt describes at least four different categories of shifting defaults: (i) natural defaults; (ii) technological defaults; (iii) legal defaults; and (iv) normative defaults. In some places, she also talks about some of these defaults alongside important juridical concepts such as autonomy and liability. I shall briefly elaborate on each of these.

A. Natural Defaults

Nature may be said to set its own defaults, some of which have been shifted by human ingenuity. Hildebrandt acknowledges this in an interesting discussion of Maryanne Wolf's work, *Proust and the Squid*.[11] Wolf argues that human beings were never born to read; reading is a human invention that reflects how the brain rearranges itself to learn something new. As Hildebrandt puts it, "[R]eading and writing are not innate skills, we do not master them by default, as we do with vision and hearing and walking" (49). What Wolf is essentially describing is that we shift our biological defaults—undertaking the hard work of learning to read and write—in order to gain access to our external memory (i.e., memory stored in script or, these days, digital devices), which, in turn, shifts other defaults. Whether this is understood to happen by human choice or by evolutionary forces, through technology, human beings are sometimes in a position to shift natural defaults in order to achieve various ends. As Hildebrandt further points out, reading and writing (indeed, abstract thought) are affordances of script and the printing press that are enabled, not caused, by the plasticity of our brains. This tells us that novel information and communications infrastructures will also enable further reconfigurations of our brains and an ability to further shift the defaults of our current minds.

To offer a more mundane but important example, one can also understand the state of privacy as a kind of natural default. "By default, opacity shields individual citizens from the scrutiny of governmental spying" (189).[12] However, the defaults of our once opaque existence ("obscurity" as some have called it[13]) are shifting as a result of the proliferation of various surveillance technologies. Similarly, other authors have talked about the role that natural defaults such as human forgetting have played in our ability to maintain privacy.[14] This natural default setting of the human brain has also shifted with the

---

[11] Maryanne Wolf, Proust and the Squid: The Story and Science of the Reading Brain (2008).

[12] Although Hildebrandt's actual observation likely was referring to a legal, not a natural default.

[13] Woodrow Hartzog & Evan Selinger, Obscurity, A Better Way to Think About Your Data than 'Privacy,' The Atlantic (Jan. 17, 2013), http://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-than-privacy/267283.

[14] Viktor Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age (2011); Meg Leta Jones, Ctrl + Z: The Right to Be Forgotten (2016).

affordances of searchable online databases, cheap information storage and the external memory that they have helped to create. Like Hildebrandt, many authors see potential protections against these shifting natural defaults in legal protection by design. In these instances, it is often suggested that we must mandate the provision of functional equivalents for "obscurity," "forgetting," and the like, requiring by law that they be built directly into our information and communications infrastructures.[15]

B. Technological Defaults

Natural defaults can be displaced by technological defaults. One might in fact say that the very essence of technology is to change natural defaults.[16] Hildebrandt offers several examples in which humans create default settings within the architecture of a given smart technology, permitting what she calls 'machine interventions.' For example, in her narrative of the onli*f*e, she imagines a car with several default settings aimed at ensuring safety for a driver who is too emotionally distraught to operate the vehicle: "Diana is free to take the car because a certain threshold of nervousness has not been reached; at a later point the car itself announces that it will cease to function within five minutes" (68). Unlike the natural defaults of the brain, which can be individually overridden by hard work, displacing technological default settings is a question of permissions, invoking the need for sophisticated 'digital rights management systems.'[17] Hildebrandt asks:

> Who or what sets these defaults and which are the goals; is Diana in charge and has she instructed these smart systems to constrain her, or do they operate in accordance with the settings of the relevant service providers? . . .
>
> Can Diana intervene, change her mind (or [the machine's] "mind"), for instance by resetting certain defaults? Will she have or make the time to address this issue, and direct her attention to this on a regular basis? (73)

Technological default settings, Hildebrandt reminds us, have the potential to create legal effects. They can be used to generate contracts automatically; settings can also generate real life harms if not properly attended to. How law will deal with the implications of such default settings remains uncertain. "What if the hardware or the default settings of the software . . . create consequences that Diana could not have foreseen?" (73).

To date, one of the central challenges with using technological defaults to regulate human conduct in the onli*f*e is that they are difficult to contest, "because they are often invisible and because most of the time there is no jurisdiction and no court" (12). "[A]s long as the default settings are a part of the hidden complexity people simply lack the means to context their manipulation" (165). It is important to understand that this isn't just about affecting one-off choices. As Hildebrandt so eloquently puts it,

---

[15] Woodrow Hartzog & Frederic Stutzman, Obscurity by Design, 88 Wash. L. Rev. 385 (2013).

[16] I owe this point to Woodrow Hartzog, although it is possible to create technologies aimed at preserving natural defaults (in the face of a shifting default caused by some other technology).

[17] Ian Kerr, Digital Locks and the Automation of Virtue, in From "Radical Extremism" to "Balanced Copyright": Canadian Copyright and the Digital Agenda 247 (Michael Geist ed., 2010).

> To act autonomously would mean that if I want, I can reflect on my own default settings or on those of my environment and reframe them to be in accordance with my second order desires . . . . However, the most serious violation is when others diminish my capability to reflect on my habits or inclinations, for instance by taking my first order preferences for granted and catering to them before I become aware of them (192).

Here, what is so egregious is the interference in shaping a person's intent such that they are unable to assess their own desires, let alone develop intentions about such desires.

C. Legal Defaults

Hildebrandt does not spend much time delineating "the legal default" as a separate category, though some of her comments tacitly recognize that it is. For example, she talks about "default prohibitions" both in the context of discrimination law (192) and data protection law (195). Here, she is referring to a default rule in the sense that civil codes often prescribe a general rule (where a law applies by default) and then stipulate additional rules (which shift away from the application of the general rule). These are not default rules in the meaning usually ascribed by the common law. As explained in greater detail below in Section IV, common law defaults are legal rules that can be overridden—not by other provisions within a statute or code but rather through the instrumentality of private actors manifesting an assent to the contrary.

Still, Hildebrandt's central question in the book is relevant to the common law notion of a legal default rule in its broadest sense (though she never explicitly mentions this). To put my own spin on it, Hildebrandt is asking whether conceptions of the Rule of Law are ineradicable or whether they are merely the defaults of a legal system: the results of the affordances of a particular information and communications infrastructure, subject to change as we modify our instruments and infrastructures. I will return to the question of whether the Rule of Law is itself a kind of default rule in the final section of this review.

D. Normative Defaults

As we have seen, technological defaults can regulate conduct by making certain behaviors more likely while narrowing the possibility of others. This permits what Hildebrandt refers to as the development of a "default of usage":

> Once a default of usage has settled, artefacts like typewriters, traffic lights, mobile phones, speed bumps, smart fridges and search engines impact the way we interact with each other, often enabling types of interaction previously not possible or ruling out alternate ways of doing things (11).

Once defaults have settled, opposition to their usage is increasingly difficult: expectations tend to consolidate in favor of their use. In other words, technological defaults can be used to create normative defaults, or "mutual expectations that regulate human interaction" (11). As described above in the section on technological defaults, default settings can be used to interfere with choice autonomy. In a different way the same is true of normative defaults. They can lead to what philosophers (in other contexts) have called a

hardening of the categories. Once a particular norm is put in place, it becomes more difficult to do otherwise without breaching social standards.

Having offered a typology and a structure for considering Hildebrandt's interesting but distributed remarks on shifting defaults in relation to the adoption of smart technologies, I will now elaborate on two of these categories. I will then conclude by deliberating on their relationship to Hildebrandt's reflections about the Rule of Law.

III. Technological Defaults

I have long held that one of the most important lessons of techno-regulation not explicitly articulated by Reidenberg, Lessig, or anyone writing on the subject during the past decade is the importance of understanding default settings in technological architectures. The importance of defaults has been recognized in neighboring fields such as computer science and psychology for many years. Since at least the 1960s, computer scientists found it useful to assign a pre-existing value to a user-configurable setting for various hardware and software applications. These "factory presets" could be altered by consumers but were a useful starting point for users—many of whom never knew that these presets could be changed, nor had any reason to change them.

In the field of psychology this technological possibility later evolved into a broader technique for affecting choice, known as a "default effect."[18] In this context, a "default" refers to the position that people end up in if they fail to make an active choice. It was observed that setting a default affects how likely people are to end up with that particular option. More specifically, the default effect refers to changes in the probability that an agent will choose a particular option when it is set as a default (as opposed to a scenario in which that option was not preset). The technique of pre-setting defaults to increase the probability of a particular choice has become more prevalent during the past decade through what some behavioral economists have called "choice architecture." The purpose of building such architectures is to "stack the deck" in favor of particular outcomes in order to 'nudge' people towards certain decisions without directly coercing their decision-making.[19] It took a while, but those working in the technology law space eventually caught on.[20]

I don't think that I quite fathomed the sheer magnitude of potential manipulation made possible by the default effect until 2009. In response to recommendations made by the Privacy Commissioner of Canada,[21] Facebook created a single, simplified control pan-

[18] Isaac Dinner et al., Partitioning Default Effects: Why People Choose Not to Choose, 17 J. Experimental Psychol.: Applied 432 (2011); Eric J. Johnson & Daniel Goldstein, Do Defaults Save Lives? 302 Science 1338 (2003).

[19] Richard Thaler and Cass Sunstein refer to this technique as "libertarian (or 'soft') paternalism." See Richard Thaler & Cass Sunstein, Nudge: Improving Decisions about Health, Wealth, and Happiness 4-6 (2008).

[20] See Ian Kerr, et al., Soft Surveillance, Hard Consent: The Law and Psychology of Engineering Consent, in Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society (Ian Kerr et al. eds., 2009); see also Ryan Calo, Digital Market Manipulation, 82 Geo. Wash. L. Rev. 995 (2014).

[21] Elizabeth Denham, Letter from OPC to CIPPIC Outlining Its Resolution with Facebook, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2009/let_090827/. This letter responds to a complaint filed by my law school's technology law clinic, CIPPIC.

el allowing its users, for the first time ever, to choose who gets to see their posted content. Numerous trusted media outlets, privacy advocates and politicians around the globe reported this event as "a privacy U-turn" (*The Sun* in Britain), an "about face" change (*Economist*), "a major step forward for privacy" (American Civil Liberties Association), and a "significant first step that Facebook deserves credit for" (Senator Charles Schumer).[22] I, however, was not convinced; as I put it in an op-ed published at the time, "[t]he devil is in the defaults."[23] Here is what I meant by that.

In December 2009, Mark Zuckerberg posted an open letter on Facebook's official blog announcing the changes to its privacy settings. Users were promised more granular control and could decide whether they wanted to share any given piece of information with "friends," "friends of friends," or "everyone." But what Facebook gave with one hand, it took away with the other. The so-called increase in privacy control came alongside default settings that made each user's name, profile picture, current city, gender, networks, and fan pages publicly available. Through the introduction of its "choice architecture"—knowing full well that eighty-eight percent of its users would not bother changing their default settings—Facebook grabbed more data from its four-hundred million active users in one fell swoop than perhaps any other company had ever done before in human history—all under the guise of choice.

We are only just now starting to understand the full effect of the power afforded to those who control technological defaults. At the same time, we are starting to delegate significant decision-making powers to smart technologies, allowing machine interventions to affect our own ability to decide things. This further relinquishment of control—especially as we continue to push forward in the field of machine learning, in which we train smart technologies to behave on their own without being explicitly programmed—risks becoming a force multiplier of shifting defaults. With machine learning and other techniques in artificial intelligence, many of these shifting defaults will be unpredictable by design.[24] Given the potential threats that come with automating defaults, it is clear that smart technologies do indeed pose significant risks to privacy, identity, autonomy, non-discrimination, due process, and even the presumption of innocence.

IV. Legal Defaults

The above discussion of technological defaults has rightly focused on their opacity and their potential for manipulation and misuse However, it is worth remembering the more neutral (even beneficial) historical origins of defaults as "factory presets," flexibly preconfigured in order to accommodate users in situations where programmers or manufacturers

---

[22] Ian Kerr, The Devil Is in the Defaults, Ottawa Citizen, May 29, 2010, http://www.iankerr.ca/blog/2016/6/21/the-devil-is-in-the-defaults.

[23] Id.

[24] Jason Millar and Ian Kerr, Delegation, Relinquishment and Responsibility: The Prospect of Robot Experts, in Robot Law (Ryan Calo et al. eds., 2016).

were uncertain of users' exact needs. This more noble understanding of the role of default settings provides a good segue to common law default rules.

In fact, the best-known academic work on the subject directly connects common law default rules to technological default settings:

> The default rule approach analogizes the way that contract law fills gaps in the expressed consent of contracting parties to the way that word-processing programs set our margins for us in the absence of our expressly setting them for ourselves. A word-processing program that required us to set every variable needed to write a page of text would be more trouble than it was worth. Instead, all word-processing programs provide default settings for such variables as margins, type fonts, and line spacing and leave it to the user to change any of these default settings to better suit his or her purposes.[25]

According to Barnett, what is common to both technological and legal defaults is that default rules are binding in the absence of manifested assent to the contrary.[26] In other words, default rules will be employed unless they are intentionally displaced. A corollary of this principle, of course, is that the defaults are knowable and that there are mechanisms to displace them. As discussed above, because opacity (or complexity) can render technological defaults unknown or difficult to displace, they have the potential to manipulate. And, in the face of "nudges" and the exploitation of other cognitive biases, knowledge of the default settings alone may not suffice to protect users from manipulation. The opposite is most often the case with contracting parties, who know the default rules and work with (or against) them to create the best possible arrangements that are in line with their interests.

It is important to understand the function of common law default rules. In the context of contract law, where they are perhaps best known,[27] default rules are needed because contracting parties are never quite able to contemplate every possible future contingency arising through the instrumentality of their contracts. The future is full of question marks, and default rules fill the knowledge-gaps that may arise in future dealings under a contract; they tell the parties how they must act in situations on which the contract is silent. As Lawrence Solum put it:

> Once you think about it, it becomes clear that no actual contract could be complete. There are infinitely many possible future states of the world—and a contract that covered all of them would have an infinite number of provisions, and hence the drafting of such a contract would never be complete—it would still be unfinished when the universe reached a state of complete entropy. So the notion of a complete contract is an idealization—not a practical option.[28]

---

[25] Randy E. Barnett, The Sound of Silence: Default Rules and Contractual Consent, 78 Va. L. Rev. 821 (1992).

[26] It is worth noting a point that Barnett either misses or ignores, which is that even basic default settings such as those in Word or PowerPoint can have normative effects, including the power to alter our thought processes: Ian Parker, Absolute PowerPoint: Can a Software Package Edit Our Thoughts?, New Yorker, May 28, 2001, http://www.newyorker.com/magazine/2001/05/28/absolute-powerpoint.

[27] Default rules are also present in many other areas of private law, such as trusts, wills, corporate law, and the like.

[28] Lawrence Solum, Legal Theory Lexicon: Default Rules and Completeness, Legal Theory Blog (Sept. 30, 2012), http://lsolum.typepad.com/legaltheory/2012/09/legal-theory-lexicon-default-rules-and-completeness.html.

For this reason, judges and legislators create default rules to preempt legal uncertainty that arises with incomplete contracts, accommodating situations where contracting parties may not have thought to specify rules of their own. If they do specify their own rules,[29] the defaults do not apply. A classic example of this is the "postal acceptance" rule, commonly referred to as the "mailbox" rule. Once technology allowed people to conduct business by way of the post, courts found it necessary to stipulate rules for determining when an offer is accepted given possible delays or failures in delivery.[30] As master of the offer, an offeror may decide instead to stipulate a different moment that determines when acceptance is said to occur, or stipulate instead that mail cannot be used as a means of communicating the acceptance of an offer.[31] But a failure to stipulate an alternative will invoke the default rule.[32] Such a rule is designed to promote business efficacy and ensure legal certainty.

Courts and commentators have refined the proper approaches to setting legal defaults. Suffice it to say for present purposes that, in some cases, defaults are "tailored" to achieve what the parties would have wanted; in other cases, they are "untailored" to provide an off-the-rack standard that accommodates the majority of contracting parties.[33] Often, default rules are used to promote broader social goals such as efficiency or to maximize utility.[34] But in all cases, contractual defaults are regulated by courts and legislators and generally aim to advance the public good rather than merely private interests. This feature of legal defaults distinguishes them from technological defaults. Despite sharing significant structural similarities, including the desire to preempt future uncertainty, the actual purposes and effects of technological defaults are completely unregulated and left entirely in the hands of private actors. This is a serious problem and not enough scholars are addressing it.

V. Mandatory Defaults

Although Hildebrandt discusses the threats posed by default settings in smart technologies, she does not include defaults in her proposal for legal protection by design. I think a lesson to be learned from the above comparison of technological and contractual defaults is that (at least some) technological defaults ought to be regulated in a manner similar to contractual defaults. In this brief section, I want to further suggest that law needs to mandate certain defaults.

The notion of a mandatory default may sound oxymoronic; defaults, after all, are about choice.[35] But law could require that certain defaults be set to afford some minimal

---

[29] What Barnett referred to above as "manifesting assent to the contrary."

[30] Consequently, the creation of a default rule: acceptance is deemed communicated once the letter is postmarked.

[31] Household Fire & Carriage Accident Insurance Co. v. Grant, (1879) 4 Ex. D. 216 (C.A.).

[32] Additional default rules are now in place for email and other emerging communications technologies: e.g., Electronic Commerce Act, 2000, S.O. 2000, c. 17, ss. 19-22.

[33] Ian Ayres & Robert Gertner, Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules, 99 Yale L.J. 87 (1989).

[34] Solum, supra note 28.

[35] In fact, the first thing one learns about contractual default rules is that they are to be distinguished from mandatory rules. See Barnett, supra note 25; Solum, supra note 28; Ayres & Gertner, supra note 33.

(or maximal) level of protection. For example, in previous writing about suggested reforms to Canadian privacy law, I argued that it is time to enact a set of legal provisions that prescribes "privacy by default."[36] Although I have not yet had the opportunity to develop a more concrete proposal for its enactment, Article 26 of the *General Data Protection Regulation* creates a general requirement in its favor.[37] Such a principle would provide that the strictest privacy settings automatically apply once a customer acquires a new product or service. In other words, no manual change to the privacy settings should be required on the part of the user. This would avoid manipulations of the sort described above, where Mark Zuckerberg was able to undermine the privacy of hundreds of millions of Facebook users under the guise of "choice." If the onli*f*e entails that default settings will be in a constant state of renegotiation with artificial agents, as Hildebrandt maintains it does, it seems to me that law ought to intervene to set the most important defaults.

VI. Law's Mode of Existence

Having focused mainly on the nature and role of defaults, I conclude this review essay by returning to the central question that Hildebrandt asks in her book: "should we expect that artificial intelligence—as a technology—transforms the mode of existence of the law?" (159). These two things can, of course, be conceptually linked by restating the question as follows: is the Rule of Law merely our current legal default, a legal system that could be displaced by adopting smart technologies in big data space? Can we vanquish modern law's mode of existence and still think of the remaining elements in their new digital ensemble as a legal system in some legitimate sense? These are not easy questions.

Hildebrandt's position is that law's current mode of existence, reflected in the Rule of Law, is a historical artifact rooted in its textual nature. Such a system generated a need for linear deliberation, sequential reasoning, reflection, consideration, hesitation, and contestation among other things. But Hildebrandt is worried that smart technologies could displace all of these through an instrumentalization of the law:

> In so far as the onli*f*e world is designed and engineered in a way that is conducive to preemptive computing as an instrument for achieving policy objectives that can replace legal precepts whenever these are less effective or efficient, the mode of existence of the law will be reduced to the instrumentalist modus (185).

If this sounds far-flung, it is worth noting that three law professors from a prominent Canadian law school recently adopted this very position in a paper accepted at a symposium titled, "Machine Learning and The Law" (taking place at the most important annual conference on artificial intelligence, Neural Information Processing 2016).[38] They posited this

---

[36] Kerr, supra note 22.

[37] E.C., Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), [2016] O.J., L 119/1.

[38] Benjamin Alarie et al., Regulation by Machine (presentation at Machine Learning and the Law, NIPS 2016), http://www.mlandthelaw.org/papers/alarie.pdf.

not merely as a prediction of how things are likely to turn out, but as a normative prescription for how things should be. Hildebrandt warns that if this happens, law loses its specific mode of existence, "turn[ing] written law into a paper dragon" (226). Alarie and his co-authors are not deterred by this possibility. They think this would improve the efficiency of the legal system. Hildebrandt thinks this would end it.

With limited space, I am not completely sure what to say about all this. I certainly share Hildebrandt's concerns about the risk that techno-regulation can displace legitimate decision-making. But at what point would a shift to the onli*f*e completely undermine legality?[39] The onli*f*e of Hildebrandt's initial narrative certainly seems to run afoul of the second, fourth, seventh and eighth desiderata of Lon Fuller's formal requirements of legality commonly associated with the liberal conception of the Rule of Law.[40] But would we ever delegate *that much* normative and preemptive decision-making to machines, such that the Rule of Law would transmogrify into an administrative regime of techno-regulation? If such were the case, then the devil is in the defaults—and for that reason, I read Hildebrandt's remarks on the end of law as an important cautionary tale.[41]

At the same time, perhaps the disquieting thought about smart technologies that launched this review is less of a reason *in favor* of understanding that modern law's default mode of existence is in jeopardy; rather, it may be taken as an illustration of exactly why the Rule of Law provides a reason *against* permitting or precluding particular defaults (natural, technological, legal, and normative). I'm willing to bet a golden fiddle[42] that Hildebrandt would not disagree.

---

[39] See Ian Kerr & Carissima Mathen, Chief Justice Roberts Is a Robot (presentation at WeRobot 2014), http://robots.law.miami.edu/2014/wp-content/uploads/2013/06/Chief-Justice-John-Roberts-is-a-Robot-March-13-.pdf.

[40] Lon L. Fuller, The Morality of Law 38-39 (rev. ed. 1969):

> [T]he attempt to create and maintain a system of legal rules may miscarry in at least eight ways; there are in this enterprise, if you will, eight distinct routes to disaster. The first and most obvious lies in a failure to achieve rules at all, so that every issue must be decided on an ad hoc basis. The other routes are: (2) a failure to publicize, or at least to make available to the affected party, the rules he is expected to observe; (3) the abuse of retroactive legislation, which not only cannot itself guide action, but undercuts the integrity of rules prospective in effect, since it puts them under the threat of retrospective change; (4) a failure to make rules understandable; (5) the enactment of contradictory rules or (6) rules that require conduct beyond the powers of the affected party; (7) introducing such frequent changes in the rules that the subject cannot orient his actions by them; and, finally, (8) a failure of congruence between the rules as announced and their actual administration.

[41] However, as Ryan Calo astutely reminds me, this ignores Lessig's important lesson in *Code* that the empire strikes back! In other words, lawmakers can and do require architectural changes in order to further certain legal objectives (precisely Hildebrandt's legal protection by design). Lessig's best example is the Communications Assistance for Law Enforcement Act (Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 U.S.C. §§ 1001-1010), which requires networks to facilitate surveillance by building in the capacity to isolate particular communications and creating what amounts to a separate port for the FBI. The U.S. is currently considering a similar approach aimed at encryption.

[42] Charlie Daniels Band, The Devil Went Down to Georgia (Epic Records 1979). H/t Ryan Calo :).