


2011

# Open Robotics

M. Ryan Calo

*University of Washington School of Law*

Follow this and additional works at: <https://digitalcommons.law.uw.edu/faculty-articles>

 Part of the [Computer Law Commons](#), [Science and Technology Law Commons](#), and the [Torts Commons](#)

---

## Recommended Citation

M. Ryan Calo, *Open Robotics*, 70 MD. L. REV. 571 (2011), <https://digitalcommons.law.uw.edu/faculty-articles/32>

This Article is brought to you for free and open access by the Faculty Publications at UW Law Digital Commons. It has been accepted for inclusion in Articles by an authorized administrator of UW Law Digital Commons. For more information, please contact [cnyberg@uw.edu](mailto:cnyberg@uw.edu).

# Articles

## OPEN ROBOTICS

M. RYAN CALO\*

### I. INTRODUCTION

Robotics is poised to be the next transformative technology. Robots are widely used in manufacturing, warfare, and disaster response,<sup>1</sup> and the market for personal robotics is exploding.<sup>2</sup> Worldwide sales of home robots—such as iRobot’s popular robotic vacuum cleaner<sup>3</sup>—are in the millions.<sup>4</sup> In fact, Honda has predicted that by the year 2020, it will sell as many robots as it does cars.<sup>5</sup> Microsoft founder Bill Gates believes that the robotics industry is in the same place today as the personal computer (“PC”) business was in the 1970s,<sup>6</sup> a belief that is significant given that there are now well over one billion PCs—just three decades after their introduction into the market.<sup>7</sup>

---

Copyright © 2011 by M. Ryan Calo.

\* Director, Consumer Privacy Project, Center for Internet and Society, Stanford Law School. Co-Chair, Artificial Intelligence and Robotics Committee, American Bar Association. I would like to thank Daniel Siciliano, Mary-Anne Williams, Stephen Wu, Richard Craswell, Noriko Kageki, and Leila Takayama for helping me think through these ideas. Thanks also to the librarians at Stanford Law School for their research guidance.

1. *E.g.*, P.W. SINGER, WIRED FOR WAR: THE ROBOTICS REVOLUTION AND CONFLICT IN THE TWENTY-FIRST CENTURY 7–8 (2009) (noting that robots are being used in the contexts of manufacturing and warfare).

2. *See id.* at 8 (estimating that the number of personal robots in the world doubled between 2004 and 2007 and suggesting that the numbers will continue to expand at higher rates).

3. *See About iRobot*, iROBOT, <http://www.irobot.com/sp.cfm?pageid=74> (follow “About Our Robots” hyperlink) (last visited Mar. 21, 2011) (noting that more than five million home robots have been sold worldwide and that the “floor vacuuming robot is leading the charge”).

4. SINGER, *supra* note 1, at 7–8 (citing a 2007 United Nations report finding “that there were 4.1 million robots around the world working in people’s homes”).

5. Juha Ainoa et al., *The Digital Evolution—from Impossible to Spectacular*, in BIT BANG: RAYS TO THE FUTURE 8, 31 (Yrjö Neuvo & Sami Ylönen eds., 2009), available at <http://lib.tkk.fi/Reports/2009/isbn9789522480781.pdf>.

6. *See* Bill Gates, *A Robot in Every Home*, SCI. AM., Jan. 2007, at 58, 60, available at [http://www.cs.virginia.edu/~robins/A\\_Robot\\_in\\_Every\\_Home.pdf](http://www.cs.virginia.edu/~robins/A_Robot_in_Every_Home.pdf) (“The robotics industry faces many of the same challenges that the personal computer business faced 30 years ago.”).

7. Daniel Lyons, *Android Invasion*, NEWSWEEK, Oct. 11, 2010, at 42 (calculating the number of PCs in existence three decades after their introduction). There may be reason to believe that the number of robots in the world will increase more quickly than did PCs:

R

Personal robots under development are sophisticated and versatile. The Japanese company Kawada Industries recently released the HRP4, an all-purpose humanoid robot that is, according to one reporter, “quite definitely, a sign of the guest-greeting, vacuum-pushing, room-tidying, mail-delivering household robot revolution about to come.”<sup>8</sup> Intel has designed the Home Exploring Robotic Butler (“HERB”), a personal robot that can follow basic commands such as “‘please clean this mess.’”<sup>9</sup> The Silicon Valley startup Willow Garage recently released the Personal Robot 2 (“PR2”), which researchers have already programmed to fold laundry and to retrieve items from a refrigerator.<sup>10</sup>

Like today’s PCs, tomorrow’s personal robots will have operating systems and run software.<sup>11</sup> They will be able to connect with one another and to the Internet,<sup>12</sup> and the hope is that they will be capable of a wide variety of tasks limited only by end-user imagination.<sup>13</sup>

---

It took only one-third of the time for as many smart phones to be in use as household PCs.  
*Id.*

8. Kit Eaton, *AIST’s HRP4: Sci-Fi-Like Household Helper Robots Have Arrived*, FAST COMPANY (Sept. 15, 2010), <http://www.fastcompany.com/1689179/aists-hrp4-sci-fi-like-household-helper-robots-seem-to-have-arrived>. Kawada Industries collaborated with the National Institute of Advanced Industrial Science and Technology in developing the HRP4. *Mechatronics—Introduction*, KAWADA INDUSTRIES, INC., <http://global.kawada.jp/mechatronics/index.html> (last visited Mar. 21, 2011). The National Institute of Advanced Industrial Science and Technology was responsible for “total specification design.” *Mechatronics—Introduction*, *supra*.

9. Robert S. Boyd, *Robots Are Narrowing the Gap with Humans*, McCLATCHY (Apr. 20, 2009), <http://www.mcclatchydc.com/2009/04/20/66530/robots-are-narrowing-the-gap-with.html>. Boyd also describes a “Robobusiness” conference in which companies “demonstrated a robot firefighter, gardener, receptionist, tour guide and security guard.” *Id.*

10. See admin, *Beer Me, Robot*, WILLOW GARAGE (July 6, 2010, 3:42 PM), <http://www.willowgarage.com/blog/2010/07/06/beer-me-robot> (announcing success in programming a robot to deliver—and open—beer); Donald Melanson, *UC Berkeley Researchers Teach PR2 Robot to Fold Towels*, ENGADGET (Apr. 5, 2010, 10:21 PM), <http://www.engadget.com/2010/04/05/uc-berkeley-researchers-teach-pr2-robot-to-fold-towels> (explaining how the PR2 folds towels). Future plans involve everything from setting a table to pouring liquid into a cup. See Press Release, Willow Garage, Willow Garage Gives Away 11 Robots Worth Over \$4 Million to Accelerate Robotics Applications & Research (May 4, 2010), available at <http://www.willowgarage.com/sites/default/files/media/2010-04-04-Willow%20Garage%20PR2%20Release%20May%202010%20FINAL.pdf> (announcing the institutional and academic recipients of a PR2 robot giveaway and describing their projects, which were all designed to “make rigorous and creative use of the robots”).

11. See *infra* Part III.

12. See, e.g., Tamara Denning et al., *A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons*, in PROCEEDINGS OF THE 11TH INTERNATIONAL CONFERENCE ON UBIQUITOUS COMPUTING 105, 106–07 (2009), available at <http://dub.washington.edu/djangosite/media/papers/p105-denning.pdf> (discussing two commercial robots able to connect to the Internet).

13. Cf. *id.* at 113 (expecting “a greater number of increasingly sophisticated robots to be used in the home for diverse tasks”).

But unlike PCs, personal robots will have “actuators” that enable physical interaction with the external world.<sup>14</sup>

Many discussions of robotics and the law focus on legal responsibility for autonomous agents or on the possibility of robot rights.<sup>15</sup> That is not my focus here. In this Article, I will advance several hypotheses about the commercial prospects of robotics<sup>16</sup> in the United States. I will argue that to fulfill its enormous promise personal robotics<sup>17</sup> must be sufficiently “open” to third party innovation and that paving the way toward such openness may require modest legal intervention.

In Part II, I will briefly describe a recurrent theme in cyberlaw scholarship, namely the suggestion that openness of various kinds leads to greater innovation. In Part III, I will present two visions of personal robotics, one “closed” and the other “open.”<sup>18</sup> By “closed,” I mean that the robot has a set function, runs only proprietary software,<sup>19</sup> and cannot be physically altered by the consumer. The

---

14. *See id.* at 112 (“The actuators will dictate what physical assets the robot can affect and the ways that it can physically assist in an attack scenario.”).

15. For two early, but excellent, examples of such scholarship, see Sam N. Lehman-Wilzig, *Frankenstein Unbound: Towards a Legal Definition of Artificial Intelligence*, FUTURES, Dec. 1981, at 442, and Lawrence B. Solum, *Legal Personhood for Artificial Intelligences*, 70 N.C. L. REV. 1231 (1992). For a discussion that asks whether a robot could assert rights or be subject to criminal liability, see also CHRISTOPHER D. STONE, *EARTH AND OTHER ETHICS: THE CASE FOR MORAL PLURALISM* 12, 26–31 (1987). For a recent and short, but interesting, discussion about the perceived threats that artificial intelligence may pose to humans, see generally John O. McGinnis, *Accelerating AI*, 104 Nw. U. L. REV. 1253 (2010).

16. Robots differ from other technologies in that they combine three elements that acting together enable them to function as artificial organisms: sensors, processors, and effectors. SINGER, *supra* note 1, at 67. Effectors (or actuators) are components that enable the robot to act upon the external world. *Id.*

17. When using the term “personal robotics,” I refer to robots for personal, service, or business use, as distinct from military or manufacturing uses. I also focus on standalone robots, as opposed to distributed or embedded robotics.

18. In this sense, my project echoes that of Professor Jonathan Zittrain with respect to networked computing platforms. *See* JONATHAN ZITTRAIN, *THE FUTURE OF THE INTERNET—AND HOW TO STOP IT* 3–5 (2008) [hereinafter ZITTRAIN, *FUTURE OF THE INTERNET*] (suggesting that the future will bring “sterile *appliances* tethered to a network of control,” which inhibit the ability of “mainstream technology [to] be influenced, even revolutionized, out of left field”); Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 1976 (2006) [hereinafter Zittrain, *Generative Internet*] (explaining that the Internet was “built to be open to any sort of device . . . so long as it was properly interfaced” and acknowledging that “the openness of the Internet and the PC to third-party contribution is now so persistent and universal as to seem inevitable”).

19. *See infra* Part III.A. There is certainly an important role for proprietary software to the extent that an inability to protect intellectual property rights could also stifle innovation. *Cf.* Zittrain, *Generative Internet*, *supra* note 18, at 1978–79 (suggesting that, because “[p]roprietary systems can remain ‘open’ . . . by permitting unaffiliated third parties to write superseding programs and permitting PC owners to install these programs without

R

R

popular Roomba robotic vacuum cleaner and the first Artificial Intelligence roBOt (“AIBO”) mechanical pet are closed in this sense.<sup>20</sup> By “open,” I mean nondedicated use, nondiscriminatory software, and modular design.<sup>21</sup> The Swiss-designed e-puck robot is a paradigmatic example of an open robot.<sup>22</sup> It has no predetermined function (aside from the general goals of education and research), runs third party open source software, and can be physically altered and extended without compromising performance.<sup>23</sup>

Open robotics, I will argue, could lead to rapid innovation and growth within the personal robotics sector, just as open computers contributed to the success of personal computing.<sup>24</sup> Closed robotics, however, will move forward more slowly as companies design—and

---

requiring any gatekeeping by the [operating system] provider,” the focus of “debates about the future of our PC experience” should be on “generative versus nongenerative: understanding which platforms will remain open to third-party innovation and which will not”).

20. Consumer pressure ultimately led iRobot to develop the Create, a programmable “robot for tinkers.” See Don Woligroski, *Robotic R&D with the Son of Roomba*, TOM’S HARDWARE (May 14, 2007, 11:03 PM), <http://www.tomshardware.com/reviews/irobot-create-20070515,1602-2.html> (attributing the production of the Create to the popularity among robotics fans of the Roomba, another iRobot model). The Create is a more open version of the Roomba, which consumers can “hack.” See Khalid Hosein, *iRobot Create—Programmable Roomba-Like Robot*, GIZMOS FOR GEEKS (Jan. 12, 2007), <http://www.gizmosforgeeks.com/2007/01/12/irobot-create-programmable-roomba-like-robot/1252> (contrasting the Roomba and the Create in terms of their “hackability”). Similarly, Sony eventually opened the AIBO platform in response to consumer demand. See *infra* text accompanying notes 115–24.

21. See *infra* Part III.A. These are not the only qualities in the field of personal robotics that support innovation and adoption. There must also be a critical mass of standardization so that third parties can program software and build hardware for multiple platforms, thus enabling a critical mass of adoption. See *infra* notes 152–56 and accompanying text.

22. See Francesco Mondada et al., *The e-puck, a Robot Designed for Education in Engineering*, in 1 PROCEEDINGS OF THE 9TH CONFERENCE ON AUTONOMOUS ROBOT SYSTEMS AND COMPETITIONS 59, 60 (2009), available at <http://infoscience.epfl.ch/record/135236/files/epuck-robotica2009.pdf> (explaining the e-puck’s design as “[a]n open source hardware/software development model”).

23. *Id.* at 60–61, 63 (describing e-puck features). Other examples of open robots include (1) KUKA’s youBot (Germany), see *Key Features*, KUKA, <http://www.kuka-youbot.com/en> (last visited Mar. 21, 2011) (“desktop mobile manipulator”); (2) LEGO’s Mindstorms (Denmark), see *Products*, LEGO MINDSTORMS, <http://mindstorms.lego.com/en-us/products/default.aspx> (last visited Mar. 21, 2011) (“customisable programming”); (3) Robosoft’s Kompai (France), see *RobuBOX-Kompai Now Available in Open Source*, NEWS FROM ROBOSOFT (May 3, 2010), <http://robosoftnews.wordpress.com/2010/04/28/robubox-kompai-now-available-in-open-source/>; (4) Fujisoft’s PALRO (Japan), see *Robot Technologies: Features*, FUJISOFT, [http://157.120.140.213/e/solutions/robot\\_technologies/features.html](http://157.120.140.213/e/solutions/robot_technologies/features.html) (last visited Mar. 21, 2011) (open architecture software); and (5) the iCub (European Union), see *Who I Am*, ICUB.ORG, <http://www.icub.org> (last visited Mar. 21, 2011) (“open source cognitive humanoid robotic platform”).

24. See ZITTRAIN, *FUTURE OF THE INTERNET*, *supra* note 18, at 19 (identifying a “crucial element of the PC’s success” as the fact that “it is generative: it is open to reprogramming and thus repurposing by anyone”).

R

R

R

some consumers purchase—a series of robot appliances, each dedicated to a particular task.<sup>25</sup> No secondary professional market for software or hardware can accompany an entirely closed robotics industry.<sup>26</sup>

Many contemporary technologies, including telephones, televisions, computers, and the Internet, have thrived despite well-documented hurdles to openness.<sup>27</sup> In Part IV, I will predict that open robotics will confront an additional hurdle: the potential for crippling legal liability, which may lead entrepreneurs and investors to abandon open robots in favor of robots with more limited functionality. This possibility flows from a key difference between computers and robots. Although robots, like computers have no set function,<sup>28</sup> robots are in a position to cause physical damage and injury directly, which computers cannot do.<sup>29</sup>

Legal liability for computer-caused injury was a nonstarter,<sup>30</sup> and U.S. courts quickly headed off the prospect of software liability through doctrines such as economic loss.<sup>31</sup> People also came to expect and accept that computers would have glitches.<sup>32</sup>

---

25. See, e.g., *Trust Me, I'm a Robot*, *ECONOMIST*, June 10, 2006, at 78 (“It is more likely, [Colin Angle of iRobot] believes, that robots will be relatively dumb machines designed for particular tasks. Rather than a humanoid robot maid, ‘it’s going to be a heterogeneous swarm of robots that will take care of the house,’ he says.”); cf. ZITTRAIN, *FUTURE OF THE INTERNET*, *supra* note 18, at 19–20 (describing a counterfactual in which, if the personal computer had not been open to reprogramming, people would instead use different dedicated all-in-one units for different tasks). R

26. Cf. Zittrain, *Generative Internet*, *supra* note 18, at 1976 (describing the PC as “easily reconfigurable by its users for any number of purposes” and explaining that “[t]he audience writing software for PCs . . . is itself massive and varied. This diverse audience has driven the variety of applications powering the rapid technological innovation to which we have become accustomed” (footnote omitted)). R

27. See, e.g., ZITTRAIN, *FUTURE OF THE INTERNET*, *supra* note 18, at 36–38 (describing the first Internet worm, which “was the first large-scale demonstration of a vulnerability of generativity”). R

28. This is true by definition. Cf. Zittrain, *Generative Internet*, *supra* note 18, at 1980–81 (defining “generativity”—a technology’s ability “to produce unprompted change driven by large, varied, and uncoordinated audiences”—as “a function of a technology’s capacity for leverage across a range of tasks, adaptability to a range of different tasks, ease of mastery, and accessibility”). R

29. See *infra* notes 163–66 and accompanying text. R

30. See, e.g., *Transp. Corp. of Am. v. Int’l Bus. Machs. Corp.*, 30 F.3d 953, 955–56, 960 (8th Cir. 1994) (rejecting claim against computer manufacturer for economic loss resulting from computer failure). R

31. See *infra* text accompanying note 193. R

32. See David E. Jordan, *The Tortious Computer—When Does EDP Become Errant Data Processing?*, 4 *COMPUTER L. SERV.* § 5-1, art. 2, at 4, 8 (1972) (acknowledging an “implicit acceptance of the fallibility of computers” and suggesting that computer users may be “consciously accepting the risks of defects and operational difficulties in new equipment, in preference to delaying purchase until the ‘bugs’ have been worked out”). R

Lawsuits alleging *physical* harm from computers and software, however, can and do gain traction.<sup>33</sup> Such incidents usually involve a dedicated medical, navigation, or other system not performing as it should.<sup>34</sup> There has yet to be a test case for liability where a nondedicated robotic platform<sup>35</sup> caused physical harm. The resulting legal uncertainty could discourage the flow of capital into robotics or otherwise narrow robot functionality, placing the United States behind other countries with a higher bar to litigation and a head start on research, development, and production.<sup>36</sup>

Finally, in Part V, I will propose a tentative compromise between the need to foster innovation and the need to incentivize safety. Specifically, I will argue that Congress should shield manufacturers and distributors of open robotic platforms from suit for what consumers do with their personal robots, just as it immunizes gun manufacturers from suit for what some people do with guns<sup>37</sup> and websites operators for what users upload and post.<sup>38</sup> A selective immunity would give open robotics some breathing room until industry standards, norms, or other solutions emerge. In this Part, I will also briefly explore the

---

33. See *infra* text accompanying notes 196–205. Computers and software with physical ramifications, such as those that control a car’s navigation, acceleration, or brakes, are generally single purpose. Cf., e.g., Karim Nice, *How Car Computers Work*, HOWSTUFFWORKS, <http://auto.howstuffworks.com/under-the-hood/trends-innovations/car-computer.htm> (last visited Mar. 21, 2011) (noting that “[c]ars today might have as many as 50 microprocessors on them,” such as the engine control unit, the antilock braking system module, and the transmission controller). These computers and software are supposed to do one task, safely. When they fail to do that task, it is easier to make the case for manufacturer’s liability. See *infra* notes 167–77 and accompanying text. As I will argue in Part IV, we cannot assume that consumers, juries, and courts will distinguish between the many possible causes of a multipurpose personal robot’s malfunction that has injured someone.

34. For examples of cases that illustrate this point, see sources cited *infra* notes 200–05.

35. By “robotic platform,” I mean a basic system comprised of a processor, sensors, and one or more actuators. Robotic platforms constitute functioning robots but may require the addition of task-specific hardware. See SINGER, *supra* note 1, at 25 (describing one such platform).

36. See *infra* text accompanying notes 271–81.

37. See Protection of Lawful Commerce in Arms Act (“PLCAA”), 15 U.S.C. § 7901(b)(1) (2006) (listing prohibition of “causes of action against manufacturers, distributors, dealers, and importers of firearms or ammunitions products, and their trade associations, for the harm solely caused by the criminal or unlawful misuse of firearm products or ammunition products by others when the product functioned as designed and intended” as one of the purposes of PLCAA).

38. See, e.g., Online Copyright Infringement Liability Limitation Act (“OCILLA”), 17 U.S.C. § 512(a)(1) (2006) (shielding service providers from liability for copyright infringement when the infringing content’s transmission was initiated by a third party); cf. Communications Decency Act (“CDA”) of 1996, 47 U.S.C. § 230(c)(1) (2006) (“No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”).

R

R

R

R

R

possibility of a small-scale market for individual robot insurance, with rates and premiums calibrated to the robot's capacity to cause harm.

The time to think through this problem is now. Roboticians and investors are already making decisions that will determine the fate of the personal robotics industry in the United States.<sup>39</sup> Indeed, the first multipurpose robots have already hit the commercial market.<sup>40</sup> Meanwhile, other countries have already recognized the enormous promise of personal and service robots, and as a result they have increased investment and set aggressive goals.<sup>41</sup> By taking a wait and see approach, the United States risks missing out on this decade's transformative technology.<sup>42</sup>

## II. FROM OPENNESS TO INNOVATION

Over the course of its relatively short history, cyberlaw has been host to several key discussions. Among the earliest was the debate around cyberspace's supposed exceptionalism.<sup>43</sup> This debate has several aspects. There is the question, for instance, whether we need new law to deal with cyberspace or whether existing laws are adequate.<sup>44</sup>

---

39. See COMPUTING CMTY. CONSORTIUM WORKSHOP ON EMERGING TECHS. & TRENDS, A ROADMAP FOR U.S. ROBOTICS: FROM INTERNET TO ROBOTICS 1 (May 21, 2009) [hereinafter ROADMAP FOR U.S. ROBOTICS], available at <http://www.us-robotics.us/reports/CCC%20Report.pdf> (arguing that although there have been "tremendous advancements in robotics technology" over the past five years, the United States "lags behind other countries in recognizing the importance of robotics technology" and "U.S. investment, outside unmanned systems for defense purposes, remains practically non-existent" (emphasis omitted)).

40. See *supra* notes 8–10 and accompanying text.

41. See, e.g., OLIVER BROCK & RODERIC GRUPEN, FINAL REPORT OF THE NSF/NASA WORKSHOP ON AUTONOMOUS MOBILE MANIPULATION 6 (Aug. 8, 2005), available at <http://www-robotics.cs.umass.edu/~gruppen/AMMReport-2005-08-08.pdf> (reporting that countries in Europe and Asia have made "significant financial investments in research activities associated with humanoid robotics and mobile manipulation").

42. See ROADMAP FOR U.S. ROBOTICS, *supra* note 39, at 1 ("Unless this situation can be addressed in the near future, the United States runs the risk of abdicating our ability to globally compete in these emerging markets and putting the nation at risk of having to rely on the rest of the world to provide a critical technology that our population will become increasingly dependent upon."); cf. Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925, 956–57 (2001) (criticizing a "wait and see" approach to allowing cable companies to eliminate Internet service provider competition because "[i]t may be impossible to measure the loss of innovation that results").

43. David W. Opderbeck, *Deconstructing Jefferson's Candle: Towards a Critical Realist Approach to Cultural Environmentalism and Information Policy*, 49 JURIMETRICS J. 203, 239 (2009) ("The first generation of cyberlaw scholarship was split between exceptionalists and unexceptionalists, who respectively viewed cyberspace either as a newly constructed autonomous realm or as nothing but people sitting in front of computer terminals.").

44. See, e.g., David G. Post, *Governing Cyberspace: Law*, 24 SANTA CLARA COMPUTER & HIGH TECH. L.J. 883, 891–92 (2008) (explaining the exceptionalists' view that the "signifi-

R

R



The question arose very early in the context of computers,<sup>45</sup> culminating in an exchange between Judge Frank Easterbrook and Professor Lawrence Lessig about the Internet in the late 1990s.<sup>46</sup> Judge Easterbrook contended that there was no more a need for a separate law of cyberspace than there was a need for a separate “Law of the Horse.”<sup>47</sup> Professor Lessig responded by detailing the lessons of cyberspace for law generally.<sup>48</sup>

A distinct debate arose from early claims that cyberspace would disrupt existing notions of sovereignty.<sup>49</sup> Professor James Boyle coined the term “libertarian gotcha” to encompass the idea that governments rely on the Internet for its economic promise while simultaneously being incapable of governing activity there.<sup>50</sup> As Professor Lessig describes in his seminal book *Code*, scholars went so far as to predict that citizens of the web would be able to select how they would be governed by choosing between competing online communities.<sup>51</sup> Professor Lessig wrote *Code* in part as a response to this debate, arguing not only that cyberspace could be regulated but also that the par-

---

cant effects principle” used to determine jurisdiction in international cases is insufficient vis-à-vis the Internet).

45. In 1963, for instance, Harvey Levin opined that any problems arising from computer systems were factual and would “fit within the recognized principles of tort law.” Harvey B. Levin, *Automation and the Law of Torts*, PRAC. LAW., Dec. 1963, at 83, 90; see also Jordan, *supra* note 32, at 4 (“There do not appear to be any conceptual problems in the extension of product liability into the field of computers.”).

R

46. Compare Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 215–16 (arguing in favor of facilitating the ability of “participants in this evolving world to make their own decisions” rather than trying to “match an imperfect legal system to an evolving world that we understand poorly”), with Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 501–02 (1999) (disagreeing with Judge Easterbrook’s belief that there is no value to “thinking in particular about how law and cyberspace connect”). The reference to “The Law of the Horse” dates back to Karl Llewellyn’s discussion of idiosyncratic contract rules. Lessig, *supra*, at 501 n.1.

47. See Easterbrook, *supra* note 46, at 207–08 (asserting that although there are many cases that deal with horses in some way, “[a]ny effort to collect these strands into a [law school] course on ‘The Law of the Horse’ is doomed to be shallow and to miss unifying principles,” and analogizing “The Law of the Horse” to “Property in Cyberspace”).

R

48. Lessig, *supra* note 46, at 502 (“By working through these examples of law interacting with cyberspace, we will throw into relief a set of general questions about law’s regulation outside of cyberspace.”).

R

49. See generally LAWRENCE LESSIG, *CODE: VERSION 2.0*, at 294–310 (2006) (explaining the notion of conflicting sovereignties in the context of cyberspace and mapping out three possible resolutions to the conflict). Professor Lessig explains that cyberspace inhabitants are simultaneously subject to norms of “a community in real space,” as well as those of “a cyberspace community.” *Id.* at 298–99.

50. *Id.* at 3.

51. *Id.* at 288.

ticular way in which it is subject to regulation may render it uniquely susceptible to control.<sup>52</sup>

Today, technology policy is dominated by another set of debates, unified—if at all—by a common concern over the best conditions for innovation and competition.<sup>53</sup> Though the technologies at issue diverge, a significant number of commentators consistently evidence a need for greater openness to third party innovation.<sup>54</sup>

Several distinct conversations take place under this mantle. One involves the types of devices consumers may connect to a given network. AT&T originally fought the use of non-AT&T equipment on its network, citing operational concerns.<sup>55</sup> Cable companies continue to make essentially the same argument in connection with television set-top boxes.<sup>56</sup> The counterargument to these claims is that opening telephone and cable networks to third party device manufacturers is safe, permits healthy competition, and incentivizes device innovation.<sup>57</sup>

---

52. See *id.* at 5 (introducing the notion that “‘code is law,’” which demands an understanding of how, in cyberspace, “a different ‘code’ regulates—how the software and hardware (i.e., the ‘code’ of cyberspace) that make cyberspace what it is also regulate cyberspace as it is”). Professor Lessig also suggested that a preference for open source code over proprietary or closed code would help safeguard the conditions for democracy. *Id.* at 149–51. This preference results because “[t]o the extent that code is open code, the power of government is constrained. Government can demand, government can threaten, but when the target of its regulation is plastic, it cannot rely on its target remaining as it wants.” *Id.* at 150.

53. See, e.g., Frank Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, 104 Nw. U. L. REV. 105, 124 (2010) (“Innovation has been the central focus of Internet law and policy. While leading commentators sharply divide on the best way to promote innovation, they routinely elevate its importance.” (footnote omitted)).

54. See, e.g., *id.* at 125 (“Innovation is the goal; competition is the means for achieving it. . . . [Indeed,] Lessig and other advocates of network neutrality worry that the owners of the ‘pipes’ that carry communications may impede . . . innovation by favoring their own applications.”).

55. See *In re Use of the Carterfone Device in Message Toll Tel. Serv.*, 13 F.C.C.2d 420, 424 (1968) (describing AT&T’s argument that the telephone companies “must have absolute control over the quality, installation, and maintenance of all parts of the [telephone] system in order effectively to carry out [their] responsibility [to establish, operate and improve the system]”). As of this writing, Apple’s popular iPhone was also limited by default to a single provider. See Shayndi Raice & Yukari Iwatani Kane, *Verizon Finally Lands the iPhone*, WALL ST. J., Jan. 8, 2011, at B1 (“The iPhone is finally coming to Verizon.”).

56. See, e.g., *Gen. Instrument Corp. v. FCC*, 213 F.3d 724, 730–31 (D.C. Cir. 2000) (explaining cable companies’ argument that a federal regulation requiring separation of security and other set-top cable box functions would jeopardize security).

57. See, e.g., *In re Implementation of Section 304 of the Telecomms. Act of 1996*, 13 F.C.C. Rcd. 14775, 14776 (1998) (defining “navigation devices” as “the equipment used to access video programming and other services from multichannel video programming systems” and explaining that the purpose of Section 629 of the Act and the FCC rules

A second conversation concerns the conditions under which an Internet provider may block, slow down, or otherwise discriminate against traffic over its network.<sup>58</sup> Professor Tim Wu coined the term “net neutrality”<sup>59</sup> to stand for the principle that network providers should respect the original, application-neutral architecture of the Internet.<sup>60</sup> This debate also centers on whether excessive network management will dampen competition and innovation.<sup>61</sup> Professor Barbara van Schewick, for instance, has developed a technological and economic model detailing precisely how variance from the end-to-end principle and other design aspects of the early Internet is likely to affect innovation by startups and other firms.<sup>62</sup>

Noting a trend away from PCs that can run any software and toward tethered appliances that run only what the provider allows, Professor Jonathan Zittrain focuses on an analogous concern about the nature of computing devices.<sup>63</sup> Innovation is also at the heart of Professor Zittrain’s argument: He shows how tethered appliances such as the iPhone are less “generative” than PCs, meaning that such devices are not capable of supporting the same level of creativity and innovation.<sup>64</sup> Professor Zittrain suggests that this development reflects the

---

adopted were “to expand opportunities to purchase [navigation devices] from sources other than the service provider”); Kevin Werbach, *Higher Standards: Regulation in the Network Age*, 23 HARV. J.L. & TECH. 179, 193–94 (2009) (arguing that the FCC’s landmark decision in *Carterfone* to allow interconnection of third party devices with the telephone network ultimately sparked competition and innovation in network-attached devices).

58. See, e.g., Susan P. Crawford, *The Internet and the Project of Communications Law*, 55 UCLA L. REV. 359, 395–98 (2007) (arguing that network discrimination, the practice of “allowing network-access providers to treat some traffic or some users differently,” is economically destructive).

59. Preston Gralla, *Apple Is Number One Danger to Internet Freedom, Says Columbia Professor*, COMPUTERWORLD (Nov. 15, 2010, 11:16 AM), [http://blogs.computerworld.com/17354/apple\\_is\\_number\\_one\\_danger\\_to\\_internet\\_freedom\\_says\\_columbia\\_professor](http://blogs.computerworld.com/17354/apple_is_number_one_danger_to_internet_freedom_says_columbia_professor).

60. See Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. ON TELECOMM. & HIGH TECH. L. 141, 145–46 (2003) (defining and making the case for “a neutral network,” which is “an Internet that does not favor one application (say, the world wide web), over others (say, email)”).

61. *Id.*; Pasquale, *supra* note 53, at 125–28.

62. See generally BARBARA VAN SCHEWICK, *INTERNET ARCHITECTURE AND INNOVATION* (2010) (explaining the author’s model for study of the Internet’s architecture and design principles and how constraints on the architecture impact innovation).

63. See ZITTRAIN, *FUTURE OF THE INTERNET*, *supra* note 18, at 3 (“The future is not one of generative PCs attached to a generative network. It is instead one of sterile *appliances* tethered to a network of control.”). *But see* Sharon Eisner Gillet et al., *Do Appliances Threaten Internet Innovation?*, IEEE COMM. MAG., Oct. 2001, at 46, 47, 50 (concluding that whether Internet appliances—devices that connect to the Internet and have a fixed function—pose a threat to innovation “depends on the class of appliance”).

64. ZITTRAIN, *FUTURE OF THE INTERNET*, *supra* note 18, at 2–3. Zittrain also reintroduces a concern over the capacity of tethered appliances to support “‘perfect’ law enforcement.” *Id.* at 110–23.

R

R

R

tension between the ideal of generativity and the need to lock down platforms because of risks to individual and national information security.<sup>65</sup>

Another debate centers around user-generated content, especially the extent to which websites should be held responsible for the unlawful content that users post.<sup>66</sup> This debate is to some extent obviated by federal law, which protects websites for user copyright violations under certain conditions<sup>67</sup> and under which most other questions of liability are preempted.<sup>68</sup> Nevertheless, arguments regularly surface over the scope of these laws and how they are policed.<sup>69</sup> Innovation tends to be at the forefront of these exchanges, as well: Websites would not provide unfettered communications platforms or support user-generated content, the argument runs, if they could be held liable for anything anyone said or did on those platforms.<sup>70</sup>

The preceding is not intended as an exhaustive description of the expansive field of cyberlaw.<sup>71</sup> But it does suggest a certain recurrent insight: The more open a platform, network, or device is to third party

---

65. See *id.* at 43 (arguing that there may come a “breaking point” at which there are so many breaches of cybersecurity that “people will come to prefer security to generativity”).

66. See, e.g., Assaf Hamdani, *Who’s Liable for Cyberwrongs?*, 87 CORNELL L. REV. 901, 901–09, 949–52 (2002) (introducing a framework for liability of Internet service providers after concluding that the Digital Millennium Copyright Act of 1998 did not sufficiently address the divergence in its regulation of Internet service providers); Nancy S. Kim, *Web Site Proprietorship and Online Harassment*, 2009 UTAH L. REV. 993, 997 (arguing that website sponsors should be liable in tort for online harassment on grounds of “unreasonable business models” and “irresponsible and harmful business practices”).

67. See OCILLA, 17 U.S.C. § 512 (2006) (providing a safe harbor for Internet service providers hosting third party content as long as the providers implement a takedown procedure).

68. See CDA, 47 U.S.C. § 230(e) (2006) (explaining the effect of the Act on other laws); see also *supra* note 38 (noting that § 230(c)(1) exempts service providers from liability).

69. Cf. *supra* note 66.

70. The preamble to the CDA lists as a purpose of the statute “preserv[ing] the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation.” 47 U.S.C. § 230(b)(2); see also Eric Goldman, *Unregulating Online Harassment*, 87 DENV. U. L. REV. ONLINE 59, 60 (2010), <http://www.denverlawreview.org/how-to-regulate/2010/2/22/unregulating-online-harassment.html> (arguing that “Congress made a great (non)regulatory decision” in enacting § 230, which “correlates with the beginning of the dot com boom—one of the most exciting entrepreneurial periods ever”).

71. For instance, it makes no mention of privacy, security, or digital rights management (“DRM”) under copyright law. For a thorough discussion of privacy in the digital age, see DANIEL J. SOLOVE, *THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET* 4 (2007) (“This book will take a journey through the ways in which private lives are being exposed online, and it will examine the implications. . . . I will propose a framework for how we can address these problems—by recognizing a new and broader notion of privacy and by reaching a better balance between privacy and free speech.”). For a discussion of the perils of DRM that is skeptical of its protection, see generally Julie E.

contribution, the more innovation it supports.<sup>72</sup> At a minimum, open networks, devices, and platforms support secondary markets.<sup>73</sup> Few would risk entering the business of developing new set-top cable boxes without a guarantee that they would work properly when connected to the cable system. Fewer novel applications would be funded if investors suspected that those applications would be blocked or slowed by Internet service providers or rejected by major platform owners.<sup>74</sup>

### III. TOWARD AN OPEN ROBOTICS

In short, few stories of transformative technology seem able to avoid the question of openness.<sup>75</sup> Personal robotics is no exception. It too faces a choice between a closed and an open model.<sup>76</sup> Closed, proprietary robotics will move at whatever pace robotics companies are individually capable of setting.<sup>77</sup> Innovation within open robotics could move at a dramatically faster pace and lead to an accompanying vibrant market for third party software, components, and accessories.<sup>78</sup> Companies like Willow Garage are betting on an open model.<sup>79</sup> They believe that the application or use that causes a critical mass to adopt robots will come from unexpected quarters.<sup>80</sup>

---

Cohen, *Some Reflections on Copyright Management Systems and Laws Designed to Protect Them*, 12 BERKELEY TECH. L.J. 161 (1997).

72. See, e.g., Zittrain, *Generative Internet*, *supra* note 18, at 1976 (explaining that the “massive and varied” audience writing software for personal computers “has driven the variety of applications powering the rapid technological innovation to which we have become accustomed”).

R

73. ZITTRAIN, *FUTURE OF THE INTERNET*, *supra* note 18, at 15–17.

R

74. See, e.g., Pasquale, *supra* note 53, at 125 (“YouTube might never have developed if Verizon could have throttled it in favor of its own video sharing site . . .”).

R

75. See, e.g., ZITTRAIN, *FUTURE OF THE INTERNET*, *supra* note 18, at 84–85 (discussing the benefits of generativity to the development of both computers and the Internet).

R

76. According to a recent European report, “One requirement for a robotics breakthrough is that the market has to become a diverse ecosystem of actors like the PC industry.” Petri Mannonen et al., *Cut the Last Cord by Nanolution*, in *BIT BANG: RAYS TO THE FUTURE*, *supra* note 5, at 103, 129.

R

77. Cf. ZITTRAIN, *FUTURE OF THE INTERNET*, *supra* note 18, at 2 (contrasting the generative Apple II PC with the closed nature of the iPhone, whose innovations come from Apple alone).

R

78. Cf. *id.* at 15–17 (describing this process for the personal computer).

79. See N.V., *Helping Hands*, *ECONOMIST: BABBAGE BLOG* (May 27, 2010, 8:12 PM), [http://www.economist.com/blogs/babbage/2010/05/techview\\_robot\\_every\\_home](http://www.economist.com/blogs/babbage/2010/05/techview_robot_every_home) [hereinafter N.V., *Helping Hands*] (suggesting that Willow Garage’s open source software, reflective of its open source business model, “is in a strong position to become the industry’s de facto standard—in short, the Microsoft Windows of robotics”).

80. *Id.* (describing Willow Garage’s giveaway of eleven robots and software development kits to research groups as predicated on “[t]he hope . . . that someone, somewhere, will come up with the killer app that kick-starts the whole of the personal-robot industry”).

These visions are neither cleanly delineated nor mutually exclusive. The robotics industry could offer single function robots using proprietary software while simultaneously offering one or more open robotic platforms. Indeed, this model is already in use: iRobot offers the Roomba but also the Create, an open platform for experimentation.<sup>81</sup> Moreover, a system is unlikely to be entirely closed or entirely open by my definition.<sup>82</sup> For instance, the commercially available Parrot AR.Drone and iRobot AVA prototypes are hard physically to alter but allow for third party applications.<sup>83</sup> The important question is whether, overall, robotics will be sufficiently open to promote adoption and innovation on a scale comparable with computers and the Internet.<sup>84</sup>

#### A. Closed Versus Open Robots

Closed robots resemble any contemporary appliance: They are designed to perform a set task.<sup>85</sup> They run proprietary software and are no more amenable to tinkering than a dishwasher.<sup>86</sup> Open robots are just the opposite. By definition, they invite third party contribution.<sup>87</sup>

Robots are open insofar as they have three related characteristics: (1) they lack a set function; (2) they accept third party software;<sup>88</sup> and

---

81. See *supra* note 20. iRobot also offers the Warrior, which, as P. W. Singer describes, “is really just a mobile platform, with a [Universal Serial Bus (“USB”)] port on top. USB ports are the universal connectors used to plug anything into a computer, from your mouse to a printer.” SINGER, *supra* note 1, at 25. Singer goes on to describe how a Warrior could be fitted with weapons for battle, or with an iPod and loudspeakers for a “mobile rave party.” SINGER, *supra* note 1, at 25.

82. See *infra* Part III.B.

83. See, e.g., Lance Ulanoff, *iRobot’s AVA Is an App-Ready Robot*, PCMAG.COM (Jan. 6, 2011, 1:35 PM), <http://www.pcmag.com/article2/0,2817,2375313,00.asp> (describing the compatibility of AVA with third party applications); PARROT AR.DRONE, <http://ar-drone.parrot.com/parrot-ar-drone/usa> (last visited Mar. 23, 2011).

84. Cf. ZITTRAIN, FUTURE OF THE INTERNET, *supra* note 18, at 18 (discussing the important contribution of generative technologies to the development of computer technology).

85. iRobot, for instance, sells robots designed for pool cleaning, floor washing, vacuum cleaning, shop sweeping, and gutter cleaning. iROBOT: CLEANING ROBOTS, <http://store.irobot.com/shop/index.jsp?categoryId=2804605> (last visited Mar. 6, 2011). These products are current as of 2011; more may be developed, others discontinued. This Article concerns the direction of companies like iRobot with respect to consumer robotics.

86. This limitation has not stopped some people from finding ways to tinker with the functions of these single-task robots. For example, to learn how to make a Roomba sing and connect to the Internet, see TOD E. KURT, HACKING ROOMBA (2006). *But see infra* text accompanying notes 119–20 (describing efforts by Sony to stop tinkering with its AIBO product).

87. Cf. *supra* note 20 (discussing the openness of iRobot’s Create).

88. By “third party,” I mean to exclude the manufacturer and its affiliates and subcontractors.

R

R

R

R

R

R

(3) they are modular in hardware design.<sup>89</sup> This combination of factors, coupled with a sufficient degree of standardization, could support the conditions enjoyed in the early days of the PC and the Internet.<sup>90</sup> They will help make personal robots more generative, to borrow a concept from Professor Zittrain.<sup>91</sup> In addition, they may accelerate innovation and consumer adoption of robots.<sup>92</sup>

### 1. Multifunctionality

Early computers came bundled with customized proprietary software.<sup>93</sup> Customers tended to be businesses in need of processing power to accomplish one particular service.<sup>94</sup> The rise of the personal home computer owes its beginnings to a different trend—individuals and firms that began to create platforms that were cheaper and less powerful but also much more versatile.<sup>95</sup> Personal computer sales were driven as much by potential as contemplated uses,<sup>96</sup> and demand would increase every time a new use was discovered and popularized.<sup>97</sup> The result was a continuous circle of innovation and adoption.<sup>98</sup> In other words, it was the PC's flexibility that fostered its

89. See *infra* Part III.A.1–3.

90. See ZITTRAIN, *FUTURE OF THE INTERNET*, *supra* note 18, at 3, 14–15 (describing the PC as lacking a set function and being capable of running third party software and explaining that both PCs and the Internet revolutions were launched by these attributes of openness). R

91. Technologies are generative to the extent that they have five qualities: (1) “a capacity for leverage,” (2) “adaptability,” (3) “ease of mastery,” (4) “accessibility,” and (5) “transferability.” See Zittrain, *Generative Internet*, *supra* note 18, at 1981–82 (describing the first four qualities); ZITTRAIN, *FUTURE OF THE INTERNET*, *supra* note 18, at 73 (adding the fifth criterion of transferability, which measures “how easily changes in the technology can be conveyed to others”). R  
R

92. Cf. ZITTRAIN, *FUTURE OF THE INTERNET*, *supra* note 18, at 3 (describing the PC and Internet revolutions as functions of those technologies' generative nature, which invited innovation, and asserting that both technologies overwhelmed their respective nongenerative competitors). R

93. *Id.* at 12.

94. See *id.* (explaining that “for years after” IBM's 1969 announcement that it would sell its computers and software independently, “many large firms continued to rely on custom-built, externally maintained applications designed for specific purposes”).

95. *Id.* at 13.

96. *Id.*

97. See *id.* at 15 (correlating the PC's increased popularity with its increased functionality).

98. As Professor Zittrain explains, “PC makers were selling potential functionality as much as they were selling actual uses, and many makers considered themselves to be in the hardware business only.” *Id.* at 13. He notes further: “The essence—and genius—of separating software creation from hardware construction is that the decoupling enables a computer to be acquired for one purpose and then used to perform new and different tasks without requiring the equivalent of a visit to the mechanic's shop.” *Id.* at 14.

widespread adoption as compared to machines specifically dedicated to one task.<sup>99</sup>

The same path is open to personal robotics. Under a one-robot, one-function scenario, we have to rely on the creativity of the few firms in a position to design, mass produce, and market each robot.<sup>100</sup> We end up with the series of appliances and toys we already see on the market today.<sup>101</sup> Under a multifunction scenario, consumers and other third parties, including sophisticated entrepreneurs, will help determine the range of applications.<sup>102</sup>

According to the openness argument, a market for multifunctional robots will turn out a wider variety of attractive robotic applications, increasing the likelihood that more people will purchase them. The result is a perpetual cycle. The more people purchase robots, the greater the demand for new applications, which in turn drives more innovation.

2. *Nondiscrimination*

That early PCs were multifunctional increased their adoption; that they were nondiscriminatory encouraged a secondary market for third party software.<sup>103</sup> We could imagine a multifunctional platform that only runs proprietary software.<sup>104</sup> But then we would have to rely on manufacturers to develop and roll out all new applications.<sup>105</sup> We could also imagine a hybrid model—the iPhone App Store, for instance—where platform owners select software for approval.<sup>106</sup> The

99. *Id.* at 15.

100. *Cf. supra* note 85 and accompanying text.

101. *Cf., e.g., supra* note 85 and accompanying text.

102. *Cf. ZITTRAIN, FUTURE OF THE INTERNET, supra* note 18, at 2 (describing how consumers and entrepreneurs created applications unforeseen by manufacturers that helped spur sales of the Apple II PC).

103. By “third party software,” I mean software developed by a firm that did not develop the underlying platform. This definition does not imply that a robotics platform manufacturer cannot write code for its own robot, only that it must also be open to code from other sources. *See generally* Lothar Determann, *Dangerous Liaisons—Software Combinations as Derivative Works? Distribution, Installation, and Execution of Linked Programs Under Copyright Law, Commercial Licenses, and the GPL*, 21 BERKELEY TECH. L.J. 1421, 1425 (2006) (explaining that companies with established computer platforms may wish to prevent their platform’s use by third party software, while new market entrants tend to encourage such use in order to establish their platforms).

104. *Cf., e.g., ZITTRAIN, FUTURE OF THE INTERNET, supra* note 18, at 12 (explaining that the bundling of early IBM hardware with software meant that “any improvements to the computer’s operation had to happen through a formal process of discussion and negotiation between IBM and the client,” with the result that firms could not easily switch vendors since doing so would require the new vendor to “redo the entire project from scratch”).

105. *See supra* text accompanying note 100.

106. VAN SCHEWICK, *supra* note 62, at 350.

R  
R  
R

R

R  
R



risk, however, is that platform providers will block applications that compete with their own version of the application or that they intend to develop in the future.<sup>107</sup>

An open robotics means a corresponding market for robotics software right from the beginning.<sup>108</sup> Willow Garage is an innovative robotics startup in Silicon Valley with a commitment to an open source approach.<sup>109</sup> In an effort to jump-start robotics, Willow Garage developed a personal robot platform called the PR2, complete with a robot operating system (“ROS”).<sup>110</sup> Willow Garage employees were even able to program a PR2 to bring any one of a selection of beer from the common refrigerator.<sup>111</sup> Willow Garage then gave several PR2s away to researchers to experiment with and program.<sup>112</sup> Within just months of receiving its free PR2, a lab at the University of California, Berkley wrote code that allowed the robot to fold towels<sup>113</sup> and bundle socks.<sup>114</sup>

107. As Professor Barbara van Schewick explains,

[U]nder certain conditions network providers may have an incentive to exclude an application that competes with one of their own applications. Apple’s behavior toward iPhone applications illustrates this possibility. Before any application can be sold in the iPhone App Store, Apple must approve it. . . . Apple has rejected several applications for the iPhone, claiming that they duplicated functionality provided by existing Apple applications.

*Id.* (footnotes omitted). She goes on to note that Apple has also rejected applications it intended later to develop. *Id.*

108. *Cf.* N.V., *Helping Hands*, *supra* note 79 (noting that Bill Gates organized a research group whose “mission was to create a set of software tools that would allow anyone interested in robotics . . . to write applications that would work with different kinds of hardware”).

109. For more information, see *About Willow Garage*, WILLOW GARAGE, <http://www.willowgarage.com/pages/about-us/overview> (last visited Mar. 21, 2011). The exact definition of “open source” software is contested. David McGowan, *Legal Implications of Open-Source Software*, 2001 U. ILL. L. REV. 241, 242 n.1. I use it to mean software where the source code is accessible to third parties for addition and alteration.

110. ROS, WILLOW GARAGE, <http://www.willowgarage.com/pages/software/ros-platform> (last visited Mar. 21, 2011).

111. admin, *supra* note 10.

112. See Press Release, Willow Garage, *supra* note 10. Importantly, software developed on the PR2’s ROS can be exported to other robotic platforms. See ROS: Introduction, ROS.ORG, <http://www.ros.org/wiki/ROS/Introduction> (last visited Mar. 21, 2011) (explaining that “the primary goal of ROS is to support code reuse in robotics research and development”).

113. Carol Ness, *Researchers Develop a Robot That Folds Towels*, UC BERKELEY NEWS CENTER (Apr. 2, 2010), [http://www.berkeley.edu/news/media/releases/2010/04/02\\_robot%20.shtml](http://www.berkeley.edu/news/media/releases/2010/04/02_robot%20.shtml).

114. *Laundry Robot Achieves Another Landmark, This Time Pairing Your Socks*, BERKELEY ENGINEERING (Aug. 24, 2010), <http://coe.berkeley.edu/news-center/berkeley-engineering-in-the-news/laundry-robot-achieves-another-landmark-this-time-pairing-your-socks>.

R

R

R

Sony AIBO, the robotic pet, serves as a cautionary counterexample. AIBO began as a closed system that ran only proprietary software—AIBO-ware—that allowed users to “raise” AIBO over time and teach it certain voice commands.<sup>115</sup> Sony eventually published a programming code (“R-CODE”) that permitted users to teach the AIBO new behaviors.<sup>116</sup> Users loved R-CODE and quickly bypassed the controls Sony had in place in order to share AIBO programs with one another online.<sup>117</sup> Many people did so, leading to an entire AIBO subculture.<sup>118</sup>

Sony learned of the practice and was not pleased. The company sent a cease-and-desist letter to the popular AIBO forum AiboHack, asking the website to take down the traded code as a copyright violation.<sup>119</sup> Sony arguably never recovered from the resulting consumer backlash, and it shut down the AIBO line in 2006.<sup>120</sup> Prior to this closure, however, Sony released a programming kit for noncommercial use.<sup>121</sup> This kit has since expanded into multiple versions and has

---

115. Christopher Soghoian, *Caveat Venditor: Technologically Protected Subsidized Goods and the Customers Who Hack Them*, 6 NW. J. TECH. & INTELL. PROP. 46, 56 (2007) (describing the AIBO “add-on software,” which allowed AIBO to learn tricks and assume different personality types, as proprietary).

116. See RICARDO A. TÉLLEZ, R-CODE SDK TUTORIAL 3–4 (Sept. 4, 2004), available at [http://www.ouroboros.org/rcode\\_tutorial\\_lv2.pdf](http://www.ouroboros.org/rcode_tutorial_lv2.pdf) (explaining what users could program AIBO to do using the R-CODE script, which “is a powerful tool that allows the implementation of real complicated behaviours”).

117. See Peter Rojas & Phillip Torrone, *Speak, AIBO, Speak!*, POPSCI (July 12, 2004, 11:54 AM), <http://popsci.com/gear-gadgets/article/2004-07/speak-aibo-speak> (explaining how AIBO enthusiasts encouraged the shift from Sony’s aibopet.com to the hacker site aibohack.com, which includes files and instructions about how to reprogram old and new AIBO models).

118. There are many websites devoted to AIBO. For some examples, see AIBO-LIFE, <http://www.aibo-life.org> (last visited Mar. 21, 2011); AIBOHACK, <http://www.aibohack.com> (last visited Mar. 21, 2011); and AIBOWORLD, <http://www.aiboworld.com> (last visited Mar. 21, 2011).

119. Dave Wilson et al., *Sony Dogs Aibo Enthusiast’s Site*, L.A. TIMES, Nov. 1, 2001, at C1.

120. See Eric A. Taub, *For Sony’s Robotic Aibo, It’s the Last Year of the Dog*, N.Y. TIMES, Jan. 30, 2006, at C4 (describing Sony’s decision to discontinue the AIBO after seven years on the market in order to “improve its financial position”).

121. Yoshiko Hara, *Sony Opens Aibo Software to Spur Robotics R & D*, ELECTRONIC ENGINEERING TIMES, May 13, 2002, at 14. Another example of “opening” comes from the popular robotic vacuum cleaner Roomba and its progeny. So many users were “hacking” the device that iRobot released the stripped-down platform Create for users to experiment with, see *supra* note 20, as well as an official Roomba open interface (“ROI”) specification, see generally IROBOT CORP., IROBOT ROOMBA SERIAL COMMAND INTERFACE (SCI) SPECIFICATION (2005), available at [http://www.irobot.com/images/consumer/hacker/Roomba\\_SCI\\_Spec\\_Manual.pdf](http://www.irobot.com/images/consumer/hacker/Roomba_SCI_Spec_Manual.pdf) (providing the specifications); see also *Roomba Open Interface (ROI)*, UVA WISE, [http://www.mcs.uvawise.edu/wiki/index.php/Roomba\\_Open\\_Interface\\_\(ROI\)](http://www.mcs.uvawise.edu/wiki/index.php/Roomba_Open_Interface_(ROI)) (last visited Mar. 21, 2011) (explaining that the ROI specification was formerly known as the Serial Command Interface Specification). Today, multiple forums exist for users to share their creations. See, e.g., *Robotic Hacking*, ROBOT REVIEWS, <http://www.robot>

been picked up by various research institutions around the world.<sup>122</sup> AIBO has been an official robot of the popular RoboCup tournament,<sup>123</sup> and Sony continues to hold an international AIBO conference.<sup>124</sup>

The widespread availability of robotic platforms capable of running nonproprietary software is more likely to lead to a global robot software industry.<sup>125</sup> Such an industry could take many forms. Anyone could write and share code, or only trusted partners of the platform could be entrusted to do so. Consumers could buy task-specific software permanently or rent it for the day.<sup>126</sup> Importantly, however, the purpose of at least some software would be to enable consumer innovation—that is, to allow consumers to put their robots to new uses.<sup>127</sup>

The open nature of the market has several potential advantages. First, we might get more well-developed software more quickly: Open source robot software can be released early and improve over time—an assumption Professor Zittrain calls the “procrastination principle.”<sup>128</sup> Second, we might get more secure software. To the extent we

---

reviews.com/chat/viewforum.php?f=4 (last visited Mar. 21, 2011) (providing a discussion forum centered around iRobot’s Roomba, Scooba, and Create). There is even a popular handbook called *Hacking Roomba*. See KURT, *supra* note 86.

122. For example, members of the Carnegie Mellon University Computer Science Department developed Tekkotsu, a software package for robots that “was originally written for the Sony AIBO.” *About Tekkotsu*, TEKKOTSU, <http://www.Tekkotsu.org/about.html> (last visited Mar. 21, 2011).

123. ROBOCUP, <http://www.robocup.org/> (last visited Mar. 23, 2011); see *About Our Robots*, UNIV. NEW S. WALES RUNSWIFT, <http://cgi.cse.unsw.edu.au/~robocup/2010site/index.php?p=about> (last visited Mar. 21, 2011) (noting use of the AIBO in RoboCups from 1999 to 2008).

124. Anne Hart, *Lonely Women Cherish Robot Dogs*, EXAMINER.COM (Dec. 5, 2010, 4:54 PM), <http://www.examiner.com/women-s-issues-in-sacramento/lonely-older-women-cherish-robot-dogs?render=print>.

125. Cf. Valentina Vadi, *Sapere Aude! Access to Knowledge as a Human Right and a Key Instrument of Development*, 12 INT’L J. COMM. L. & POL’Y 345, 357–58 (2008) (describing the open source movement and its pragmatic view that nonproprietary software will have economic and technical benefits).

126. Some companies have already begun developing business plans centered on renting out specific software. See Fran Foo, *Nivio Offers Monthly Rental on Software*, AUSTRALIAN, July 20, 2010, at 38 (describing one such company).

127. Some humanoid robots, such as Nao already come with simplified programming tools. See, e.g., *Step into the Future Classroom: NAO!*, ALDEBARAN ROBOTICS, <http://www.aldebaran-robotics.com/en/naoeducation> (last visited Jan. 11, 2011) (boasting a “user-friendly programming environment[ that] students and teachers can use at any programming level”).

128. See ZITTRAIN, *FUTURE OF THE INTERNET*, *supra* note 18, at 31 (“The procrastination principle rests on the assumption that most problems confronting a network can be solved later or by others. It says that the network should not be designed to do anything that can be taken care of by its users.”).

R

R

are worried about robot security, open source software may be easier to vet for vulnerabilities.<sup>129</sup> This increased security, in turn, could lead to greater rates of adoption, since consumers and firms will be less concerned about the risk that their robots will be compromised by hackers.<sup>130</sup>

### 3. Modularity

Another aspect of open robotics is hardware modularity, which is the ability to swap out or add new parts.<sup>131</sup> Open robotic platforms will be modular in design and in use.<sup>132</sup> As Professor Barbara van Schewick explains, “The goal of modularity [of design] is to create architectures whose components can be designed independently but still work together.”<sup>133</sup> That is, design modularity seeks to create products where “users of the product can replace or ‘mix and match’ components at a later stage.”<sup>134</sup> Many PCs are modular in this way.<sup>135</sup>

One example of modular design is the KUKA youBot from Germany,<sup>136</sup> a commercially available robot consisting of a motorized

---

129. Although the claim is subject to debate, many believe open source software is more secure than closed source software. See, e.g., Tom Espiner, *Trend Micro: Open Source Is More Secure*, ZDNET (June 13, 2006, 11:44 PM), <http://www.zdnet.com/news/trend-micro-open-source-is-more-secure/148445> (quoting the chief technical officer of an antivirus vendor as stating that open source software has security advantages). There is a distinct concern that widespread introduction of robotics may also present governments greater opportunities for control, for example, through surveillance, manipulation, and outright coercion. See, e.g., Noel Sharkey et al., *The Coming Robot Crime Wave*, COMPUTER, Aug. 2010, at 116, 116 (describing increased government use of robots for police functions, such as micro-helicopters used for surveillance and soon-to-be-armed ground robots for hostage rescue). But see LESSIG, *supra* note 49, at 150–51 (arguing that the power of government is constrained when code is open code, which “means open control—there is control, but the user is aware of it”). Professor Lessig argues that open software supports the democratic process by making government regulation more transparent and constrained. See LESSIG, *supra* note 49, at 150–52 (contrasting the government’s regulatory power over open and closed code).

130. Cf., e.g., Denning et al., *supra* note 12, at 1 (revealing security vulnerabilities in three commercially available home robots). For a detailed discussion of the privacy issues robots present, see M. Ryan Calo, *Robots & Privacy*, in ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS (Patrick Lin et al. eds., forthcoming 2011).

131. VAN SCHEWICK, *supra* note 62, at 38.

132. See *id.* at 39 (describing modularity in design and in use). There is a third type of modularity: modularity in production that refers to the ability to produce components independently for later assembly. *Id.*

133. *Id.* at 38.

134. *Id.* at 39.

135. *Id.* at 40.

136. Markus Waibel, *Scoop: KUKA’s youBot Mobile Manipulator Unveiled*, IEEE SPECTRUM: AUTOMATON BLOG (June 11, 2010), <http://spectrum.ieee.org/automaton/robotics/industrial-robots/scoop-kukas-youbot>; see also KUKA, *supra* note 23.

R

R

R

R

R

platform, a robotic arm, and a gripper.<sup>137</sup> The KUKA youBot has no predetermined function beyond research and education.<sup>138</sup> It runs a variety of software modules, including multiple operating systems.<sup>139</sup> The KUKA youBot is also modular. Components of KUKA—a new gripper, for instance—can be switched out.<sup>140</sup>

Modular robots have several advantages. First, they can lead to more innovation by reducing the overall costs of innovating<sup>141</sup> and, as in the context of phones and set-top boxes, by inviting more participation in the robotics ecosystem.<sup>142</sup>

Second, they can lead to broader adoption. In addition to running any compatible software program, open robots are physically extensible and hence more versatile.<sup>143</sup> Should an independent party design a new robot component that permits additional functionality—for instance, a night vision camera—consumers will not have to wait until the product is purchased or licensed by a robotics manufacturer and built into the next model.<sup>144</sup>

There is less of a penalty for adopting modular robots early. Imagine, for example, that some third party company or individual designs a significantly better gripper for a robot, one that permits the robot to perform a very delicate task it could not perform directly out

---

137. Waibel, *supra* note 136.

138. *Id.* (noting research and education as the youBot's primary purpose).

139. *Id.*

140. *Id.* (noting that the gripper is detachable).

141. VAN SCHEWICK, *supra* note 62, at 118–38 (describing three costs of innovation and explaining how modularity reduces them). Modularity may also lessen subsequent development error because designers need only understand the module they are working on, rather than the entire system. *Id.* at 41. This could also increase the security and safety of robots, thereby also affecting adoption.

142. This increased participation could occur in a number of ways. For instance, consumers could swap out riskier components for new, safer ones. *Cf. supra* note 129 (describing the possible security advantages to open source software).

143. *See, e.g.,* VAN SCHEWICK, *supra* note 62, at 41 (discussing how modularity allows independent innovators to create new hardware attachments and programs for preexisting PCs and their operating systems).

144. Robotics Group offers just such a component—a mobile platform with a pre-installed night vision camera. *Robotics Group 4x4 Mobile Platform w/ Night Vision Camera*, ROBOTSHOP, <http://www.robotshop.com/robotics-4x4-mobile-platform-night-vision-camera-2.html> (last visited Mar. 21, 2011). Again, I am not suggesting that open robotics be free of intellectual property constraints. Indeed, the inability to patent software or hardware would provide a serious disincentive to innovation. *See* Seth A. Cohen, *To Innovate or Not to Innovate, That Is the Question: The Functions, Failures, and Foibles of the Reward Function Theory of Patent Law in Relation to Computer Software Platforms*, 5 MICH. TELECOMM. & TECH. L. REV. 1, 19 (1999) (explaining how the patent system can deter innovation by overprotecting innovations). I am only suggesting that a significant proportion of robotic platforms be open to third party software and hardware, including software and hardware that is proprietary.

R

R

R

R

of the box.<sup>145</sup> If the robot is modular, consumers will merely have to replace the gripper to gain the new functionality.<sup>146</sup> If not, they will have to replace the entire robot with the next version.<sup>147</sup>

It may be perfectly feasible to replace a cell phone or even a laptop every year, but replacing personal robots with such frequency could be much more expensive.<sup>148</sup> This increased expense could act as a disincentive to purchase a robot in the first instance. Why not defer such a large investment until robots can do more? Of course, a system could arise in which consumers trade, upgrade, or lease robots, as with vehicles.<sup>149</sup> But, such a system seems unlikely to arise out of nothing and without a robust personal robotics market already in place.

### B. Tradeoffs

Open robotics may pave the way to more rapid innovation and adoption. Yet openness is not itself sufficient. Moreover, a “perfect” openness is neither attainable nor desirable. One example of extreme modularity, for instance, might be robotic kits, which permit users to substitute out nearly any part of their robots.<sup>150</sup> Robots built from kits tend to be very limited in functionality and in their ability to run software.<sup>151</sup>

---

145. See, e.g., Kristina Grifantini, *The Year in Robotics*, TECH. REV. (Dec. 29, 2009), <http://www.technologyreview.com/computing/24231/?a=f> (describing advances in gripping and grasping technology made during the prior year).

146. Cf. *supra* note 143.

147. Modularity permits innovation by parties other than the robot’s platform manufacturer. VAN SCHEWICK, *supra* note 62, at 121 (“[A]utonomous changes can often be realized independently by actors other than the system architect.”). But, it also permits a company to change its own product. See *id.* at 120–21 (“Since autonomous changes do not incur any costs of system adaptation, the threshold for innovation is considerably lower than for systemic changes, making it more likely that the innovation will be realized.”).

148. Cf. Hiroko Tabuchi, *Robots Unplugged*, N.Y. TIMES, July 13, 2009, at B1 (discussing the market failure of several personal robots, in part because of high retail prices).

149. Swisslog, among other companies, has instituted a leasing program for its autonomous mobile robots, which are used in hospitals. *Swisslog’s Autonomous Mobile Robots Available for Lease*, PRWEB (May 17, 2010), <http://www.prweb.com/releases/2010/05/prweb4001324.htm>.

150. See, e.g., *Robotics Kits*, MACHINE SCI., <http://www.machinescience.org/store/home.php?cat=249> (last visited Mar. 22, 2010) (selling robotic kits).

151. E.g., GARETH BRANWYN, ABSOLUTE BEGINNER’S GUIDE TO BUILDING ROBOTS 152 (2004) (describing Tab Robotics’ “Build Your Own Robot” kit as “fast and easy to build, but limited in function”).

Part of the advantage of buying a ready-made robotic platform is that a certain measure of functionality, including low-level programming routines, is already in place. See, e.g., WILLOW GARAGE, CALL FOR PROPOSALS: PR2 BETA PROGRAM: A PLATFORM FOR PERSONAL ROBOTICS 5 (2010), available at <http://www.willowgarage.com/sites/default/files/cfp/CFP2010.pdf> (“Researchers and developers can use the existing system as a base, extending

R

R

Moreover, open robotics will not support innovation without a sufficient degree of standardization, which locks in certain facets of software and hardware architecture, at least temporarily.<sup>152</sup> One example is the universal serial bus (“USB”) standard in computing.<sup>153</sup> Although this standard facilitates the design and adoption of cameras, printers, and other peripherals,<sup>154</sup> it inhibits, at least temporarily, the development of another connection standard that might be more efficient.<sup>155</sup> Such tradeoffs have been successfully navigated in the context of PCs,<sup>156</sup> and they will again need to be navigated in the context of personal robotics.

The vision, then, is of a handful of popular robotics platforms, each of which is open to third party programmers and hardware designers. Robotic platforms will ideally vary in size, expense, durability, and potential functionality, just as in any other market for consumer

---

it as needed, and developing new components where appropriate. To make a rough analogy, ROS does for robots what Linux does for personal computers: providing a basic system that is open-source at its core, so that researchers and developers can dig in and change any part they deem necessary.”).

152. See VAN SCHEWICK, *supra* note 62, at 43 (explaining how varying degrees of standardization impact the potential for innovation). Modularity may also affect the overall performance of the system. *Id.*

153. See Marshall Brain, *How USB Ports Work*, HOWSTUFFWORKS, <http://www.howstuffworks.com/usb.htm> (last visited Mar. 21, 2011) (explaining that nearly all computers sold today have USB ports, which enable users to connect other devices, such as a mouse or printer, to their PCs).

154. See *id.* (“Just about every peripheral made now comes in a USB version.”).

155. This technological inertia is implicit in the idea of standardization. See, e.g., Barry Fagin, *Standardization/Innovation Trade-Offs in Computing: Implications for High-Tech Antitrust Regulation*, KNOWLEDGE, TECH., & POL’Y, Fall 1999, at 80, 85–91 (describing the trade-offs between standardization and innovation in computing and suggesting that the benefits of one are inversely related to the other). But see Erik Harris, Note, *Discovery of Portable Electronic Devices*, 61 ALA. L. REV. 193, 223 n.181 (2009) (arguing that standardization led to innovation in the computer industry because “[w]hen minor players do not need to re-invent or re-define the standard, they are free to focus on the innovation that gives them a real competitive edge”). Of course, there could be multiple standards operating simultaneously, each permitting innovation within its own ecosystem. Such is the case today with computer operating systems, browser plug-ins, phones, and applications. For example, developers may decide to code applications either for the iPhone, Android, or both. Note that Android, a more open and versatile system, has eclipsed Apple’s iPhone in sales. See Lyons, *supra* note 7 (“Android now has leapt past Apple to become the biggest smartphone platform in the United States, the third-biggest worldwide, and by far the fastest growing.”); Mike Jennings, *Android, Amazon and the Case Against Third-Party App Stores*, PC PRO BLOG (Oct. 19, 2010), <http://www.pcpro.co.uk/blogs/2010/10/19/android-amazon-and-the-case-against-third-party-app-stores> (comparing the “open and versatile nature” of Android with Apple’s “walled garden”).

156. See, e.g., Fagin, *supra* note 155, at 88–89 (contrasting the adoption of computer programming languages that were “significant improvements over existing alternatives” with the failure of computing languages whose adoption would have required “a large scale programming language change” that would engender a “huge amount of resource loss”).

R

R

R

electronics.<sup>157</sup> This mimics the present state of personal computing.<sup>158</sup> The key is to ensure that a sufficient number of platforms remain open to third party innovation in order to spark a continuous cycle of creativity and demand.

#### IV. ROBOTS AS PHYSICAL PCs

Insofar as openness is a catalyst for innovation and adoption,<sup>159</sup> we may want to remove major disincentives to openness in the context of personal robotics. With respect to computers and the Internet, such disincentives include platform lock down and various types of discrimination by firms.<sup>160</sup> The same is true of robotics.<sup>161</sup> Consumers, scholars, and lawmakers should be wary of closed robotics in all the same ways, and for all the same reasons, as they might be in other technologies.

There is, however, an additional disincentive to openness in the field of personal robotics—one that is not discussed in the cyberlaw literature on openness and innovation. Open robotics may expose robotics platform manufacturers and distributors to legal liability for accidents in a far wider set of scenarios than closed robotics.<sup>162</sup> Indeed, one or more high profile products liability cases could move nearly every serious player to a closed model.

That there will be injuries and damage is hardly in doubt. Hundreds of robot-related accidents, including fatalities, have occurred in factories and other workplaces.<sup>163</sup> A number of very serious accidents

---

157. In the computer market, for example, compare Dell's \$280 Inspiron Mini 10 Netbook, a ten inch "lightweight mobile network," *Inspiron Mini 10 (1018) Netbook*, DELL, <http://www.dell.com/us/p/inspiron-mini1018/pd> (last visited Mar. 6, 2011), with Apple's \$2,000 twenty-seven inch iMac, a desktop computer contained entirely within the display unit, *iMac*, APPLE STORE, [http://store.apple.com/us/browse/home/shop\\_mac/family/imac?mco=MTcyMTgwNTQ](http://store.apple.com/us/browse/home/shop_mac/family/imac?mco=MTcyMTgwNTQ) (last visited Mar. 6, 2011).

158. See *supra* note 156 and accompanying text.

159. See *supra* Part III.A. But see *supra* text accompanying note 152 (noting that openness alone cannot foster innovation).

160. See, e.g., *supra* notes 55–56 and accompanying text.

161. See, e.g., *supra* text accompanying notes 115–20.

162. See *infra* notes 178–87 and accompanying text.

163. There is a long history of accidents involving factory robots. See, e.g., *Killer Robots: Coming Soon to a Factory Near You*, ECONOMIST, June 27, 1987, at 89 ("In one incident in 1984—a black year in which robots killed four people [in Japan]—a robot under inspection suddenly moved forward, and ran over its inspector. In another incident in the same year, a robot arm swung at a worker, giving him a deadly automated karate chop."). In more recent years, reports of robot-related injuries have begun to surface outside the context of manufacturing. See, e.g., Paul McCann, *TV Robot Injures Studio Workers*, TIMES (London), Jan. 8, 2000 ("During filming recently, a 170lb robot came to life after it was switched off and careened out of control, injuring a stage technician.").

R  
R

R  
R  
R



have occurred on the battlefield or during military testing.<sup>164</sup> Many efforts are underway to make robots used in the home safer—for instance, by using lighter material to build robots intended to interact with the general public.<sup>165</sup> Despite these efforts, perfect safety is not likely, a point no one seriously contests. Moreover, some people may purposefully use robots to cause damage or injury.<sup>166</sup>

Liability for damage or injury caused by a personal robot should be relatively straightforward in a closed world. The robot is a product capable of performing one or more specific tasks; if it fails to perform these tasks, or if it performs them unsafely, the manufacturer could generally be pursued in court.<sup>167</sup> To reduce the risk of liability, the manufacturer could warn of anticipated dangers, such as electric

---

164. See, e.g., SINGER, *supra* note 1, at 38, 125 (describing incidents of dangerous military robot malfunctions); Noah Shachtman, *Robot Cannon Kills 9, Wounds 14*, WIRED DANGER ROOM (Oct. 18, 2007, 9:00 AM), <http://www.wired.com/dangerroom/2007/10/robot-cannon-ki> (describing a fatal robot malfunction during a shooting exercise in South Africa).

165. See, e.g., Alan S. Brown, *Nimble New Robot Is Safe Around Humans*, LIVE SCI. (Nov. 2, 2006, 9:57 AM), [http://www.livescience.com/technology/061102\\_human\\_robot.html](http://www.livescience.com/technology/061102_human_robot.html) (describing a small and light robot “designed to work next to humans” as so “puny” that a child could “arm wrestle it to the table”).

166. See Sharkey et al., *supra* note 129, at 114, 114–15 (exploring how robots might be used to commit or facilitate crimes).

167. To oversimplify, products liability law, which can vary from state to state, permits recovery for physical injury or damages where a product design is unsafe, and the product is used in a normal and foreseeable manner. See, e.g., *Schemel v. Gen. Motors Corp.*, 384 F.2d 802, 804–05 (7th Cir. 1967) (explaining that a “manufacturer is not an insurer,” but is subject to liability for physical harm caused by lawful use of a product whose design makes its probable use dangerous to its intended users), *overruled on other grounds by Huff v. White Motor Corp.*, 565 F.2d 104 (7th Cir. 1977); see also RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 1 (1998) (“One engaged in the business of selling or otherwise distributing products who sells or distributes a defective product is subject to liability for harm to persons or property caused by the defect.”); DAVID G. OWEN, PRODUCTS LIABILITY LAW 1 (2005) (“Products liability law governs liability for the sale or other commercial transfer of a product that causes harm because it was defective . . .”). The defect must also be the proximate cause of the injury, which some courts allow a plaintiff to prove by showing that the defect was a “substantial factor” in causing her injury. See *Codling v. Paglia*, 298 N.E.2d 622, 628 (N.Y. 1973) (“[U]nder a doctrine of strict products liability, the manufacturer of a defective product is liable to any person injured or damaged if the defect was a substantial factor in bringing about his injury or damages . . .”).

I am assuming that early personal robotics damages claims will be grounded in products liability, just as factory robot cases have been. See, e.g., *Jones v. W+M Automation, Inc.*, 818 N.Y.S.2d 396, 398 (N.Y. App. Div. 2006) (products liability action stemming from a head injury from gantry loading system). Some actions, however, have been brought as intentional torts. See, e.g., *Miller v. Rubbermaid, Inc.*, No. CV 2005 10 6197, 2007 WL 1695109, at \*2, \*4–5 (Ohio Ct. App. June 13, 2007) (considering an intentional tort action against an employer following the death of a process technician crushed while teaching a robot due to a malfunction); *Pettit v. Clarion Techs.*, No. WM-04-014, 2005 WL 2048929, at \*1 (Ohio Ct. App. Aug. 26, 2005) (reversing summary judgment for an employer in an intentional tort action after a maintenance manager suffered severe injuries from a fall into an injection molding press after malfunction repair).

R

R

shock from submersion in water.<sup>168</sup> Because both the hardware and the software come from the same place, courts will not have to perform a complex analysis to determine responsibility.<sup>169</sup> Additionally, no aspect of a closed robot is intended to be modified.<sup>170</sup> If it is modified, then the manufacturer may invoke the alteration as a defense.<sup>171</sup>

Consider the popular robotic vacuum cleaner Roomba.<sup>172</sup> According to a recent news report, a Roomba vacuumed up and killed a poisonous snake in Israel.<sup>173</sup> Imagine that, instead of a snake, the Roomba had run over and damaged the tail of a household pet. Roomba has one task: to vacuum the floor.<sup>174</sup> The company that manufactures the Roomba, iRobot, can reasonably anticipate what

---

168. A warning will generally be considered legally valid if a reasonable consumer could understand and follow it, thereby avoiding injury. *See Harless v. Boyle-Midway Div., Am. Home Prods.*, 594 F.2d 1051, 1054 (5th Cir. 1979) (noting that a valid warning label must “reasonably be expected to catch the attention of the reasonably prudent man in the circumstances of its use” and must be “of such a nature as to be comprehensible to the average user and to convey a fair indication of the nature and extent of the danger to the mind of a reasonably prudent person” (quoting jury instruction with approval)).

169. Under the component part doctrine, for instance, the manufacturer of a nondefective part would not be liable if the part is incorporated into a defective robotic system. *See Brett W. Roubal, Note, Protecting Suppliers of Safe Component Parts and Raw Materials Through the Component Part Doctrine and the Sophisticated Purchaser Doctrine: In re Temporomandibular Joint (TMJ) Implants Products Liability Litigation*, 31 CREIGHTON L. REV. 617, 625–26 (1998) (explaining that the component parts doctrine shields manufacturers of “inherently safe component parts” from strict product liability “when their parts are incorporated into a finished product that the component part manufacturer did not build or design”); *see also W+M Automation, Inc.*, 818 N.Y.S.2d at 398 (affirming dismissal of claims against companies that “established as a matter of law that they manufactured only nondefective component parts”).

170. *See supra* text accompanying notes 85–86.

171. *See* RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2 cmt. p (“Product misuse, modification, and alteration are forms of post-sale conduct by product users or others that can be relevant to the determination of the issues of defect, causation, or comparative responsibility.”). Of course, because *normal* use includes more than just *intended* use, manufacturers must foresee some level of carelessness. *See, e.g., Reid v. Spadone Mach. Co.*, 404 A.2d 1094, 1098 (N.H. 1979) (affirming a jury finding of product liability where unsafe practices were foreseeable because the product design encouraged such practices and adequately warned against those practices), *overruled on other grounds by Daigle v. City of Portsmouth*, 534 A.2d 689 (N.H. 1987).

172. *See supra* text accompanying note 20. Surgical robots are another, nonhypothetical example of closed robots that have been linked to physical injuries. *See John Carreyrou, Surgical Robot Examined in Injuries*, WALL ST. J., May 5, 2010, at A1 (reporting on several “robotic surgeries” in which injuries occurred).

173. Evan Ackerman, *Heroic Israeli Roomba Saves Children from Deadly Viper*, BOTJUNKIE (Nov. 20, 2009, 2:19 PM), <http://www.botjunkie.com/2009/11/20/heroic-israeli-roomba-saves-children-from-deadly-viper>.

174. It is, after all, marketed as the “iRobot Roomba Vacuum Cleaning Robot.” *See Cleaning Robots—Vacuum Cleaning*, iROBOT, [http://store.irobot.com/category/index.jsp?categoryId=3334619&cp=2804605&ab=CMS\\_IRBT\\_Supercat\\_070109](http://store.irobot.com/category/index.jsp?categoryId=3334619&cp=2804605&ab=CMS_IRBT_Supercat_070109) (last visited Mar. 21, 2011).

R

R

might go wrong and either provide warnings or modify the design. Should the Roomba's design lead to an injury due to its normal use, then iRobot may face liability.<sup>175</sup> Should the consumer modify or "hack" the Roomba to perform a function it was not designed to perform—such as reenact the 1980s video game Frogger, in which a frog crosses a highway during traffic<sup>176</sup>—then the consumer is arguably responsible in the event of an accident.<sup>177</sup>

In an open world, liability could be much harder to determine. There are problems, for instance, with foreseeability because the manufacturer could not necessarily anticipate the universe of potential problems that might stem from third party innovation and provide warnings or modify the platform design in response.<sup>178</sup> One might assume that this difficulty would inure to the manufacturer's benefit because defendants will not generally be found strictly liable in tort where the injury in question was not foreseeable.<sup>179</sup> But even for causes of action that require fault, a defendant need not have foreseen the exact mechanism of harm, only the general category.<sup>180</sup>

175. See *supra* note 167 and accompanying text.

176. Some Roomba users actually modified the Roomba in this way. See Daniel Terdiman, *Roomba Takes Frogger to the Asphalt Jungle*, CNET NEWS (Mar. 15, 2006, 10:01 AM), [http://news.cnet.com/Roomba-takes-Frogger-to-the-asphalt-jungle/2100-1043\\_3-6049922.html](http://news.cnet.com/Roomba-takes-Frogger-to-the-asphalt-jungle/2100-1043_3-6049922.html) (describing "Roomba Frogger," a "tricked-out" version of the robot "dressed in a cut-up green T-shirt to look like a frog").

177. See *supra* note 171 and accompanying text. Again, liability would turn in part on reasonable foreseeability. In fact, it appears that iRobot was aware of the hacking and responded by launching another product, the Create, specifically devoted to modification and reprogramming. See *supra* note 20.

178. See Peter M. Asaro, *Robots and Responsibility from a Legal Perspective 2* (Jan. 20, 2007) (unpublished manuscript) (on file with author), available at <http://www.peterasaro.org/writing/ASARO%20Legal%20Perspective.pdf> ("[T]here is a limit to what robot engineers and designers can do to limit the potential uses and harms caused by their products because other parties, namely the consumers and users of robots, will choose to do all sorts of things with them . . .").

179. See Curtis E.A. Karnow, *Liability for Distributed Artificial Intelligences*, 11 BERKELEY TECH. L.J. 147, 173–74, 178 (1996) (noting that "causation is a necessary element of any civil tort lawsuit" and explaining that proximate cause depends upon "reasonable foreseeability"); see also *Barker v. Lull Eng'g Co.*, 573 P.2d 443, 455–56 (Cal. 1978) (finding that for a manufacturer to be held strictly liable for a defective product, either the product must have "failed to perform safely as an ordinary consumer would expect when used in an intended or reasonably foreseeable manner," or its design must have proximately caused the injury and the manufacturer fails to establish that "the benefits of the challenged design outweigh the [inherent] risk of danger" (emphasis added)).

180. *E.g.*, *Tieder v. Little*, 502 So. 2d 923, 926 (Fla. Dist. Ct. App. 1987) ("It is not necessary . . . that the defendant foresee the exact sequence of events which led to the accident sued upon . . . it must be shown that the said general-type accident was a reasonably foreseeable consequence of the defendant's negligence."). As an evolving standard, foreseeability will depend on public perception of what robots can do. See Karnow, *supra* note 179,

R

R

R

R

Some states even shift the burden of proof to the manufacturer-defendant to prove that the harm at issue was *not* foreseeable.<sup>181</sup>

There are also potential problems with determining proximate cause. It is extremely difficult to discover whether software, as opposed to hardware, is responsible for the glitch that led to an accident.<sup>182</sup> If the software is responsible, it would be hard to determine whether the precise cause was the operating system or the application (and, if the latter, which application).<sup>183</sup> This analysis is all the more difficult where the software is open source (since no single author is responsible) and the hardware can be easily modified.

Additionally, in an open world, manufacturers would not necessarily be able to invoke the common defense of product misuse.<sup>184</sup> The open personal robot (like the PC) is not designed to perform predetermined tasks.<sup>185</sup> Thus, the manufacturer is unlikely to defend itself successfully by arguing that the consumer used the robot improperly.<sup>186</sup> Nor could the manufacturer rely on the fact that the robot's platform had been modified, since an open robot is intended to be

---

at 180 ("What is 'reasonably foreseeable,' and so what qualifies as a 'proximate cause,' depends on custom and what people generally believe.").

181. See, e.g., *Barker*, 573 P.2d at 455 ("[O]nce the plaintiff makes a prima facie showing that the injury was proximately caused by the product's design, the burden should appropriately shift to the defendant to prove . . . that the product is not defective.").

182. See Nancy G. Leveson & Clark S. Turner, *An Investigation of Therac-25 Accidents*, COMPUTER, July 1993, at 18, 18 ("Most [computer-related] accidents are system accidents; that is, they stem from complex interactions between various components and activities. To attribute a single cause to an accident is usually a serious mistake.").

183. *Id.* Nor is it possible to debug software completely—that is, to anticipate how it will behave in all circumstances. See *id.* at 29 ("Virtually all complex software can be made to behave in an unexpected fashion under certain conditions."); *id.* at 38 (explaining that one mistake leading to the recurrence of computer-related accidents was "the assumption that fixing a particular error (eliminating the current software bug) would prevent future accidents" because "[t]here is always another software bug"); see also Karnow, *supra* note 179, at 162 (acknowledging that there are "*inherent* problems with software reliability" and that it is "practically impossible to test software thoroughly").

184. Cf. Yueh-Hsuan Weng et al., *The Legal Crisis of Next Generation Robots: On Safety Intelligence* § 2.3 (presented at The ACM 11th Int'l Conf. on Artificial Intelligence and Law at Stanford Law Sch., June 4–8, 2007), available at [http://works.bepress.com/weng\\_yueh\\_hsuan/2](http://works.bepress.com/weng_yueh_hsuan/2) (describing the difficulty of assessing the safety risks posed by robots with autonomous intelligence that enables them to adapt to complex environments).

185. Cf. Jordan, *supra* note 32, at 10 (noting that a computer manufacturer might sell the equipment without knowing how the user intends to use it).

186. Cf. Lehman-Wilzig, *supra* note 15, at 448 ("While the inherent risk of a lawn mower is clear, not so that of a computer which is capable of a huge number of diverse functions."). It is possible that roboticists will eventually be able to avoid strict liability on the ground that it is patently obvious that open robots are unavoidably unsafe or dangerous in ordinary use. Cf. *Killeen v. Harmon Grain Prods., Inc.*, 413 N.E.2d 767, 770 (Mass. App. Ct. 1980) ("Toothpicks . . . present obvious dangers to users, but they are not unreasonably dangerous, in part because the very obviousness of the danger puts the user on notice.").

R

R

R

modified. In fact, the capacity to be modified could even support a finding of liability.<sup>187</sup>

Of course, all these issues—foreseeability, proximate cause, misuse, and so on—also exist with respect to PCs and software.<sup>188</sup> But despite early predictions of strict liability for computers,<sup>189</sup> the opposite result was obtained.<sup>190</sup> Confronted with the problem of glitch-ridden, multifunctional computers running third party software, courts moved quickly to curb the problem by limiting liability on the ground that computer limitations are obvious.<sup>191</sup> Courts also routinely characterize software as a “good” (rather than a service), as these terms are defined by the Uniform Commercial Code,<sup>192</sup> and invoke the economic loss doctrine to limit damages to the terms of the

---

187. *But see* Meesler v. Simmons Gun Specialties, Inc., 687 P.2d 121, 125 (Okla. 1984) (“Liability for injuries sustained by a user of an altered product may be imposed on a manufacturer or seller if the injuries were caused by a defect in the product as manufactured and sold. The seller or manufacturer may not be held liable if an alteration is responsible for the defect, and is the intervening and superseding cause as opposed to the concurrent cause of the injuries.”).

188. For an argument that software manufacturers should face liability for security-related software failures, see Kevin R. Pinkney, *Putting Blame Where Blame Is Due: Software Manufacturer and Customer Liability for Security-Related Software Failure*, 13 ALB. L.J. SCI. & TECH. 43, 82 (2002) (endorsing a strict tort liability standard for software manufacturers, who would be able to use a contributory negligence defense against consumers in certain circumstances). For an early argument that computer programs are subject to standard products liability law, see Vincent M. Brannigan & Ruth E. Dayhoff, *Liability for Personal Injuries Caused by Defective Medical Computer Programs*, 7 AM. J.L. & MED. 123, 144 (1981) (“[C]ourts will find most medical computer programs to be products subject to strict liability . . .”).

189. *See, e.g.*, JOHN C. LAUTSCH, AMERICAN STANDARD HANDBOOK OF SOFTWARE BUSINESS LAW 263–64 (1985) (asserting that computers “will inevitably become a focus of liability” and arguing that “the true products liability dimensions of software writing [is] starkly apparent”); L. Nancy Birnbaum, *Strict Products Liability and Computer Software*, 8 COMPUTER/L.J. 135, 144 (1988) (arguing that strict liability inevitably will be imposed because defective software is capable of producing catastrophes); Brannigan & Dayhoff, *supra* note 188, at 144 (expecting courts to treat medical software like ordinary products subject to strict products liability); David A. Hall, Note, *Strict Products Liability and Computer Software: Caveat Vendor*, 4 COMPUTER/L.J. 373, 374–75 (1983) (explaining that, while courts have not addressed application of products liability to computer programs, increased computer use makes the issue ripe for adjudication).

190. *See, e.g.*, Donald R. Ballman, *Software Tort: Evaluating Software Harm by Duty of Function and Form*, 3 CONN. INS. L.J. 417, 419 (1997) (noting that “under current law, software manufacturers can significantly limit, if not eliminate any liability for damage which errors in their products create”).

191. *See, e.g.*, *Transp. Corp. of Am. v. Int’l Bus. Machs. Corp.*, 30 F.3d 953, 960 (8th Cir. 1994) (barring tort recovery under the economic loss doctrine for lost data following failed disc drive and noting that “[p]otential failure of the disk drive was contemplated by the parties”).

192. Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425, 435–36 & nn.69–72 (2008).

sales contract in the event of a malfunction.<sup>193</sup> These same courts steadfastly uphold broad warranty disclaimers, concluding that the software is not warranted for any particular purpose, even when it was clearly designed for one, such as word processing.<sup>194</sup>

The upshot is that you cannot sue Microsoft or Dell because Word froze and you lost your term paper. Today, most people would not even think to do so. Early adverse case law, coupled with a general understanding that computers and software are imperfect, appears to have created a presumption against holding computer or software companies responsible for the perils of personal computing.<sup>195</sup>

Such expedients to limit liability are only possible with respect to computers and software, however, to the extent that they do not cause physical injury.<sup>196</sup> The economic loss doctrine, for instance, expressly confines itself to situations where no corporeal injury has resulted.<sup>197</sup> Other product doctrines are similarly limited. As Michael Scott explains,

A majority of courts hold that where a contract between a buyer and seller exists, a negligence claim is unavailable and the aggrieved party is limited to a breach of contract claim.

. . .  
. . .

*The only exception to this rule is where the negligent conduct has caused physical damage to persons, property, or other tangible things (other than economic loss).*<sup>198</sup>

Where software or computer glitches lead to physical damage or injury, lawsuits can and do gain traction.<sup>199</sup> For instance, in an early

---

193. Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cyber-crime*, 20 BERKELEY TECH. L.J. 1553, 1580 (2005).

194. *Id.* at 1562–66 (discussing the “broad enforceability” of one-sided software agreements imposed by software manufacturer-licensors disclaiming warranties and limiting liability); Scott, *supra* note 192, at 437 (“No reported decision has unequivocally held that a software vendor has breached an express warranty.”).

195. See Jordan, *supra* note 32, at 4, 6, 8 (explaining that computer fallibility is well recognized by the public as to protect manufacturers against certain liability claims).

196. See Ballman, *supra* note 190, at 427–28 (explaining that “the UCC’s ‘unconscionability’ doctrine prevents the software manufacturer from evading liability in cases where personal injury occurs,” but that “economic or property damage is virtually exempt”).

197. Rustad & Koenig, *supra* note 193, at 1580.

198. Scott, *supra* note 192, at 456–57 (emphasis added).

199. Rustad & Koenig, *supra* note 193, at 1578 (“Courts have had little difficulty extending product liability for bad software when the design defect causes physical injury or death.”).

R  
R  
R  
R  
R  
R

case often cited in the context of software liability, the court entered judgment against a manufacturer of faulty navigational charts.<sup>200</sup> Although the suit was based entirely on faulty information, a physical accident had ultimately resulted.<sup>201</sup> Lawsuits have also proceeded against producers of computers and software that deliver radiation in medical testing<sup>202</sup> or control the fuel-delivery systems of vehicles.<sup>203</sup> In such cases, the computer and software were paradigmatically closed. They were built or assembled by one entity and dedicated to a particular, known task. One system was supposed to deliver a safe amount of radiation and failed to do so.<sup>204</sup> Another was designed to control a vehicle's fuel-delivery system.<sup>205</sup> The plaintiffs were not in a position to modify the software, and in any case, it is unlikely that they attempted to do so.

Open personal robots represent, arguably for the first time, the combination of a quality of openness with the capacity to do physical harm. How consumers and courts will react to an accident involving a personal robot is unknown. Norms tolerating unpredictability may not transfer to the context where computers become physical. In the event of a lawsuit, defendants and jurists will not be able to invoke the economic loss doctrine—or any other existing doctrine that limits liability to contract—because the harm at issue is physical.

It is also necessary to consider the optics. Many Americans may be uncomfortable or uncertain about robots and wary of robot proliferation in their lives.<sup>206</sup> Meanwhile, early adopters of robots are likely to include the elderly, the disabled, and others in need of home

---

200. *Halstead v. United States*, 535 F. Supp. 782 (D. Conn. 1982), *aff'd sub nom. Salomey v. Jeppesen & Co.*, 707 F.2d 671 (2d Cir. 1983).

201. *Id.* at 784–85, 790–91 (describing a plane crash resulting in three deaths).

202. *See Leveson & Turner, supra* note 182, at 21–35 (discussing various lawsuits related to the malfunction of Therac-25 medical radiation machines). **R**

203. *See Gen. Motors Corp. v. Johnston*, 592 So. 2d 1054, 1055–56 (Ala. 1992) (describing the plaintiff's argument that a defective fuel-delivery system caused his vehicle to stall, resulting in the death of his grandson).

204. *Cf. Leveson & Turner, supra* note 182, at 18 (referencing “software-related accidents” caused by the Therac-25, a computerized radiation therapy machine). **R**

205. *Johnston*, 592 So. 2d at 1056.

206. *See, e.g., Christoph Bartneck, Killing a Robot, in PROCEEDINGS OF THE WORKSHOP ON MISUSE AND ABUSE OF INTERACTIVE TECHNOLOGIES 2 (2006), available at <http://www.bartneck.de/publications/2006/killingARobot/bartneckAbuseCHI2006.pdf> (“Humans might feel uncomfortable with robots that become undistinguishable from humans.”). This is reflected in the countless books and movies about machines establishing themselves over humans as the dominant “species.” *See, e.g., THE MATRIX* (Warner Bros. 1999) (depicting a future in which robots have imprisoned humans to be used as energy sources).*

assistance<sup>207</sup>—individuals who make understandably sympathetic plaintiffs.<sup>208</sup> Because robots are expensive and require significant investment to design, build, and distribute, robot platform manufacturers, if not secondary participants such as software programmers and hardware designers, are likely to have deep pockets.<sup>209</sup>

This combination of factors—uncertain liability and norms coupled with sympathetic plaintiffs and well-capitalized defendants—could act as a significant disincentive to investment in the robotics market. Where firms do enter the robotics market, the inability to predict legal liability becomes an incentive to build limited robots with controlled parameters, proprietary software, and parts that are not intended to be modified. In short, the possibility that robot manufacturers or distributors will be hauled into court every time one of their robots causes an injury—regardless of what software it was running, what the consumer was doing, or whether it had been modified—may lead many potential investors to avoid the industry or to approach the construction of robots only with great caution.

## V. THE CASE FOR SELECTIVE IMMUNITY

I have argued that a sufficiently open robotics market may be the best way to foster innovation and adoption.<sup>210</sup> I have also explored why open robots face an additional hurdle involving legal liability that, for various reasons, open computers and closed robots generally do not.<sup>211</sup> This Part begins a conversation about how to avoid disincentives to open robotics while preserving incentives for safety. I advance a two-step proposal for the short term. First, we should consider immunizing manufacturers of open robotic platforms from lawsuits

---

207. Cf., e.g., ROADMAP FOR U.S. ROBOTICS, *supra* note 39, at 29–30 (asserting the potential of “[s]ocially assistive robots” to enhance quality of life for “the elderly, individuals with cognitive impairments, those rehabilitating from stroke and other neuromotor disabilities, and children with socio-developmental disorders such as autism”).

208. Cf., e.g., Amber E. Dean, *Lead Paint Public Entity Lawsuits: Has the Broad Stroke of Tobacco and Firearms Litigation Painted a Troubling Picture for Lead Paint Manufacturers?*, 28 PEPP. L. REV. 915, 934 (2001) (noting that lead paint suits are compelling to some plaintiffs’ attorneys because “the victim . . . is typically a small child who is poisoned merely by sucking his thumb”); Yxta Maya Murray, Note, *Employer Liability After Johnson Controls: A No-Fault Solution*, 45 STAN. L. REV. 453, 462 (1993) (describing the development of a “market share” theory of liability in California courts as a way to find in favor of “highly sympathetic” plaintiffs).

209. See, e.g., Press Release, iRobot, iRobot Reports Third-Quarter Financial Results, Increases Full-Year Expectations (Oct. 27, 2010), <http://investor.irobot.com/phoenix.zhtml?c=193096&p=irol-newsArticle&ID=1488073&highlight=> (announcing third-quarter revenue of \$94.2 million, a twenty percent increase since the previous year’s third quarter).

210. See *supra* Part III.

211. See *supra* Part IV.



arising out of users' changes to robots, at least temporarily.<sup>212</sup> Second, we should consider whether robot owners can carry insurance against the possibility of accidents.<sup>213</sup>

### A. Immunity

Robotics is already flourishing in several contexts. For instance, there is extensive adoption of robotics in industrial manufacturing.<sup>214</sup> Manufacturers of industrial robots are not shielded from liability,<sup>215</sup> but because industrial robots are paradigmatically closed in the sense I have discussed, arguments for and against recovery are fairly straightforward. Moreover, to the extent operation of a nondefective robot by the end-user or her employer leads to injury, state workers' compensation regimes will tend to limit employer liability and may avoid the need to address difficult issues of causation or foreseeability.<sup>216</sup> In addition, robotics is widely deployed in warfare.<sup>217</sup> Some battlefield robots are admittedly open; however, liability tends not to be an issue. Government contractors are shielded from lawsuits for robot use and malfunction because they must follow very detailed specifications.<sup>218</sup>

Assuming the expansion of robotics to be a positive development—and some may consider this characterization to be a big assumption—we should investigate how we might grant immunity to

---

212. See *infra* Part V.A.

213. See *infra* Part V.B.

214. See SINGER, *supra* note 1, at 8 (“[A]ssembly-line factory robotics is an \$8 billion a year industry, growing at a 39 percent pace in the United States.”). R

215. See *supra* notes 167–68 and accompanying text; *cf.* Reid v. Spadone Mach. Co., 404 A.2d 1094, 1098 (N.H. 1979) (noting that the evidence at trial was sufficient to find that a cutting machine was defectively designed), *overruled on other grounds by* Daigle v. City of Portsmouth, 534 A.2d 689 (N.H. 1987). R

216. *Cf.* William A. Dreier, *Beyond Workers' Compensation: Workplace Comparative Fault and Third-Party Claims*, 20 GA. ST. U. L. REV. 459, 459 (2003) (“With few exceptions, workers' compensation bars suits against employers and co-workers, but not against third parties who, through their negligence or the operation of defective products, may have contributed to an employee's injury.” (footnote omitted)).

217. See SINGER, *supra* note 1, at 32 (noting that by 2006 the United States' invasion of Iraq included 5,000 robots and describing projections that there would be as many as 12,000 robots by 2008). R

218. See Hunt v. Blasius, 384 N.E.2d 368, 371 (Ill. 1978) (“An independent [government] contractor owes no duty to third persons to judge the plans, specifications or instructions which he has merely contracted to follow. . . . [This is so] unless they are so obviously dangerous that no competent contractor would follow them.”); *Robotic Arms with Controllers*, FEDBIZOPPS.GOV (Aug. 23, 2010, 4:22 PM), <https://www.fbo.gov/index?s=opportunity&mode=form&id=f9247888bf9a357ae78272f89940f332&tab=core&tabmode=list&=> (soliciting robotic arms and controllers and providing an example of detailed specifications that government contractors must meet).

open platform manufacturers.<sup>219</sup> What would immunity for personal robotics manufacturers look like? One option is blanket immunity for all robot manufacturers. Faced with the bankruptcy of the general aviation industry, Congress intervened by immunizing small plane and small plane part manufacturers from lawsuits for a period of eighteen years.<sup>220</sup> The General Aviation Revitalization Act (“GARA”) effectively transformed general aviation into a caveat emptor market and permitted the industry to reemerge.<sup>221</sup>

The problem with blanket immunity in the context of robotics is that it would remove not only the legal disincentive to the production of open robots but also an incentive to make them safe. A leading rationale underlying products liability is to incentivize manufacturers to improve their product safety,<sup>222</sup> although the empirical truth of this assumption remains to be adequately proven.<sup>223</sup>

---

219. A hesitation to build open robots may slow the industry down. It may also lead to excessive limitations on end-user behavior that fall short of what is optimal for society. *Cf.* Hamdani, *supra* note 66, at 916–18 (arguing that because the incentives facing Internet service providers diverge from those facing their users, subjecting providers to strict liability for what users do would lead to excessive censorship of user activity). Hamdani points out that “[w]hile [Internet service providers] possess the technical ability to prevent user misconduct, they do not capture the full value of the conduct they are entrusted with policing,” which leads to overly restrictive enforcement behaviors. *Id.* at 956. This same result is obtained with open robotic platforms because it is the user, not the roboticist, who derives value from robot use.

R

220. *See* General Aviation Revitalization Act (“GARA”) of 1994, Pub. L. No. 103-298, § 2(a), 108 Stat. 1552, 1552 (1994) (codified at 49 U.S.C. § 40101 notes (2006)) (immunizing from civil action manufacturers of aircrafts and aircraft components for a period of eighteen years, subject to certain exceptions); *see also* Scott David Smith, Note, *The General Aviation Revitalization Act of 1994: The Initial Necessity for, Outright Success of, and Continued Need for the Act to Maintain American General Aviation Predominance Throughout the World*, 34 OKLA. CITY U. L. REV. 75, 108–10 (2009) (explaining that the “devastating effects products-liability law had exacted on the [general aviation] industry” led Congress to enact GARA).

221. *See* Smith, *supra* note 220, at 110–11 (noting that “[s]ince GARA’s passage, there has been a significant turnaround in the [general aviation] market,” and providing a statistical evaluation of GARA’s success).

R

222. In other words, the assumption is that the manufacturer will improve product safety to avoid liability. *See* RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2 cmt. a (1998) (“The emphasis [on products liability law] is on creating incentives for manufacturers to achieve optimal levels of safety in designing and marketing products.”); Pinkney, *supra* note 188, at 70 (“[S]oftware manufacturers facing strict liability will efficiently adjust every aspect of their behavior.”). Recognition of this effect dates back to at least 1947, when Judge Learned Hand devised his famous formula for negligence:  $B < PL$ . *See* *United States v. Carroll Towing Co.*, 159 F.2d 169, 173 (2d Cir. 1947) (L. Hand, J.) (“[L]iability depends upon whether [the burden of adequate precautions] is less than [the gravity of the resulting injury] multiplied by [the probability of injury] . . .”).

R

223. *Compare* A. Mitchell Polinsky & Steven Shavell, *The Uneasy Case for Product Liability*, 123 HARV. L. REV. 1437, 1458–59 (2010) (concluding that “a skeptical attitude about the effect of product liability on product safety for widely sold products is warranted”), *with* John C.P. Goldberg & Benjamin C. Zipursky, *The Easy Case for Products Liability Law: A*

Certainly, there are incentives other than judicially imposed liability that could make robots safer, including government regulation and the manufacturer's desire to attract consumers, to avoid public derision, and generally to do the right or moral thing.<sup>224</sup> But the possibility of a long trial followed by a costly decision or settlement clearly weighs in the calculus.<sup>225</sup> Moreover, as a normative matter, we do not want manufacturers to hide behind blanket immunity for inherently unsafe or carelessly designed platforms.

I propose a more narrow intervention—one closer to the immunity enjoyed by firearms manufacturers<sup>226</sup> and website operators.<sup>227</sup> For a time, lawsuits on the basis of what individuals did with guns (namely, shoot one another) posed a serious threat to the firearms industry.<sup>228</sup> It did not matter whether these suits were successful on the merits (many might not have been); it mattered only that the industry kept confronting them, thus incurring substantial litigation and public relations costs.<sup>229</sup> Congress perceived the need to intervene, and in 2005 Congress passed the Protection of Lawful Commerce in

---

*Response to Professors Polinsky and Shavell*, 123 HARV. L. REV. 1919, 1927–34 (2010) (criticizing the empirical basis for Polinsky and Shavell's skepticism about the ability of tort liability to deter product dangerousness).

224. See Polinsky & Shavell, *supra* note 223, at 1443–52 (discussing the impact of market forces and government regulation on safety incentives). R

225. See Goldberg & Zipursky, *supra* note 223, at 1930–31 (suggesting, in response to Polinsky and Shavell's supposed assertion to the contrary, that there is reason to believe that government regulation, market forces, and the tort system are not independent factors, but actually influence each other). *But see* Polinsky & Shavell, *supra* note 223, at 1454 (“Even though product liability might lower a product risk in the absence of market forces and regulation, it will turn out to be superfluous if a desirable safety precaution has already been taken because of these two factors.”). R

226. See PLCAA, 15 U.S.C. § 7901(b)(1) (2006) (noting that one of the statute's purposes is “[t]o prohibit causes of action against manufacturers, distributors, dealers, and importers of firearms . . . for the harm solely caused by the criminal or unlawful misuse of firearms products . . . by others when the product functioned as designed and intended”).

227. See *supra* notes 67–68 and accompanying text. R

228. See, e.g., David B. Kopel, *Protecting Makers of Weapons Boosts Democracy, Rights*, SECOND AMENDMENT PROJECT (Aug. 30, 2001), <http://www.davidkopel.com/2A/Lawsuits/Merrillv-Navegar.htm> (“Navegar is merely the latest firearms company to be driven out of business by abusive lawsuits.”).

229. See *id.* (“Companies are being destroyed not by jury verdicts, but by litigation expenses.”).

Arms Act,<sup>230</sup> which generally immunizes gun makers and distributors from lawsuits for what people do with guns.<sup>231</sup>

Personal robotics technology has the potential to be far more beneficial and transformative than personal firearms technology. Similar to firearms, however, personal robots have a potential to be misused, to cause injury, and to generate public outcry.<sup>232</sup> To preempt a clampdown on robot functionality, Congress should consider immunizing manufacturers of open robotic platforms from lawsuits for the repercussions of leaving robots open.<sup>233</sup>

Specifically, consumers and other injured parties should not be able to sue roboticists, much less recover damages, where the injury resulted from one of the following: (1) the use to which the consumer decided to put the robot, no matter how tame or mundane; (2) the nonproprietary software the consumer decided to run on the robot; or (3) the consumer's decision to alter the robot physically by adding or changing hardware. This immunity would include lawful and unlawful uses of the robot. For example, should a consumer run third party "yard work" software that causes the robot to break a neighbor's fence, neither the consumer nor his neighbor would be able to sue the robot's manufacturer. Consider the application on immunity to an unlawful use of the robot, such as the robotic equivalent of a spring gun.<sup>234</sup> The mere fact that a robot is capable of being modified through the addition of a weapon or programmed to use lethal force should not by itself form the basis of a pleading or complaint against the manufacturer.

---

230. Protection of Lawful Commerce in Arms Act, Pub. L. No. 109-92, 119 Stat. 2095 (codified at 15 U.S.C. §§ 7901–03); see PLCAA, 15 U.S.C. § 7901(a)(3), (6) (recognizing that "[l]awsuits have been commenced against manufacturers, distributors, dealers, and importers of firearms that operate as designed and intended, which seek money damages and other relief for the harm caused by the misuse of firearms by third parties, including criminals" and explaining that imposing liability on the firearm industry for harm caused solely by third parties is, among other things, an "unreasonable burden on interstate and foreign commerce").

231. PLCAA, 15 U.S.C. §§ 7902–03 (prohibiting federal and state civil actions against firearm and ammunition manufacturers and sellers "resulting from the criminal or unlawful misuse" of "qualified product[s]" as defined by the statute).

232. See *supra* note 166 and accompanying text.

233. It may prove difficult to determine exactly what constitutes an "open robotic platform" entitled to immunity. We could use the qualities detailed in Part III as touchstones, such that completely open platforms would clearly be included. The exact contours of immunity, however, are best reserved for future work.

234. In *Katko v. Briney*, the defendants rigged a shotgun to fire when someone opened the door to the bedroom of their farmhouse. 183 N.W.2d 657, 658 (Iowa 1971). The plaintiff, who prevailed, was a trespasser whose foot was blown off as a result. *Id.* at 658, 662. We can imagine a similar scenario involving a robot set to attack an intruder.

This basic strategy has a track record of success in fostering innovation. An analogous intervention in favor of website providers arguably made the contemporary Internet possible. Early in the development of the commercial web, it was unclear whether websites would be held liable for user postings. Most notably, a New York court concluded that the online service Prodigy could be held liable as a publisher for defamation taking place on its electronic bulletin boards.<sup>235</sup> Congress intervened by passing Section 230 of the Communications Decency Act of 1996,<sup>236</sup> which immunizes websites for user postings by providing that websites cannot be considered the publishers of third party content.<sup>237</sup>

Section 230, along with a similar—albeit more limited—safe harbor for copyright infringement,<sup>238</sup> has operated to prevent a wide variety of lawsuits for users' activities on websites.<sup>239</sup> This restriction on litigation has permitted social networks, video-sharing sites, and other services to flourish, despite an enormous volume of traffic and unpredictable user behavior.<sup>240</sup> In the absence of such immunity, start-ups and investors might have hesitated to create open communications platforms out of fear that they would be held liable for unlawful conduct taking place on the website.<sup>241</sup> Notably, the United States was the first jurisdiction to put intermediary liability in place, and American companies continue to dominate the Internet field.<sup>242</sup>

---

235. *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710, at \*4–5 (N.Y. Sup. Ct. May 24, 1995), *superseded by statute*, CDA, 47 U.S.C. § 230 (1996), *as recognized in* *Gucci Am., Inc. v. Hall & Assocs.*, 135 F. Supp. 2d 409 (S.D.N.Y. 2001).

236. Communications Decency Act of 1996, Pub. L. No. 104-104, § 509, 110 Stat. 133, 137–39 (codified at 47 U.S.C. § 230).

237. *See supra* note 38.

238. *See supra* note 38.

239. *See, e.g., Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1120–21 (9th Cir. 2003) (finding a “computer match making service” to be statutorily immune from liability for “false content in a dating profile provided by someone posing as another person,” pursuant to § 230(c)(1)); *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 328 (4th Cir. 1997) (affirming § 230 immunity of interactive computer service provider alleged to have “unreasonably delayed in removing defamatory messages posted by an unidentified third party, refused to post retractions of those messages, and failed to screen for similar postings thereafter”).

240. *See, e.g., Goldman, supra* note 70, at 60 (asserting that the enactment of § 230 was a “great (non)regulatory decision” in that it “correlates with the beginning of the dot com boom”).

241. *Cf. Zeran*, 129 F.3d at 330 (noting the importance of § 230 to “freedom of speech in the new and burgeoning Internet medium” and explaining that Congress enacted its immunity provisions in part “to maintain the robust nature of Internet communication”).

242. *See Goldman, supra* note 70, at 60 (suggesting that the status of the United States as a global leader in user-generated content, entrepreneurial activity, and innovation owes much to § 230).

R

R

R

R

The immunity I propose is selective: Manufacturers of open robots would not escape liability altogether. For instance, if the consumer runs the manufacturer's software and the hardware remains unmodified, or if it can be shown that the damage at issue was caused entirely by negligent platform design, then recovery should be possible.<sup>243</sup> The immunity I propose only applies in those instances where it is clear that the robot was under the control of the consumer, a third party software, or otherwise the result of end-user modification. Because this issue will not always be easy to prove,<sup>244</sup> we should expect litigation at the margins. I am thus arguing for a compromise position: A presumption against suit unless the plaintiff can show the problem was clearly related to the platform's design.

Perhaps legal intervention is also necessary with respect to third party robot *software*. Software companies could argue that they, no less than roboticists, would face disincentives to create and market software in the face of liability for anything that subsequently goes wrong.<sup>245</sup> After all, it may be very hard to determine whether it was a particular piece of software—as opposed to another piece of software, or the software's interaction with hardware or other software—that caused the problem.<sup>246</sup> And because of the risk of physical injury, robot software companies may not be able to hide behind simple warranties as have computer software companies.<sup>247</sup>

Nevertheless, I do not believe that immunity from lawsuit is necessarily appropriate for robotic software. Nearly any industry would benefit if it did not have to worry about litigation,<sup>248</sup> but there are key

---

243. The proposed immunity would operate similarly to the waning defense of contributory negligence in tort, which prevents the plaintiff from recovering if he contributed to the harm. For a discussion of the origins of and policy underlying the contributory negligence doctrine, see James McMillan, *Contributory Negligence and Statutory Damage Limits—An Old Alternative to a Contemporary Movement?*, 42 IDAHO L. REV. 269, 274–77 (2005). Suggesting that one of the biggest problems with the contributory negligence doctrine was its failure to account for cases of simultaneous negligence, McMillan argues that “in cases of ‘sequential’ negligence, contributory negligence is a perfectly defensible doctrine.” *Id.* at 298–99.

244. See *supra* Part IV.

245. See Scott, *supra* note 192, at 469 (“Opponents of strict liability for software vulnerabilities argue that the specter of potentially massive damage awards would inhibit innovation and cause vendors to avoid developing products in these areas.”).

246. See *supra* note 183 and accompanying text.

247. See *supra* text accompanying note 194–95.

248. Sometimes courts or lawmakers grant immunity merely to incentivize a needed product. The government uses immunity, for instance, as an incentive for drug makers to develop vaccines, see SUSAN THAUL, CONG. RESEARCH SERV., RL 31793, VACCINE POLICY ISSUES 10 (2005) (listing several legislative enactments granting immunity to manufacturers in order to incentivize vaccines production), which are generally less profitable than other

R

R

R

differences between software and open platforms. Immunity for roboticists encourages an open robotics ecosystem, which benefits everyone, including software companies.<sup>249</sup> Moreover, whereas open robotics platforms are designed to provide third parties freedom of use,<sup>250</sup> to the extent that software is made for a particular purpose (despite warranties to the contrary), software developers are in a better position to anticipate the uses to which their product will be put.<sup>251</sup> Indeed, many commentators argue that the computer software industry is mature enough for software developers to face liability for accidents.<sup>252</sup>

Finally, we may want to revisit immunity for manufacturers of open robots if personal robotics flourishes as hoped. The widespread proliferation of personal robots—with the resulting opportunities for observation and research—may lead to a better understanding of their capacity for harm. We may even arrive at industry standards that would provide guidance to courts, consumers, and future roboti-

---

drugs, *see* David Brown, *Severe Vaccine Shortages Termed “Unprecedented,”* WASH. POST, Apr. 20, 2002, at A1.

249. *See, e.g., supra* text accompanying notes 108–11.

250. *See supra* text accompanying notes 89–92.

251. Of course, this outcome is not always the case. While some software might be designed to allow the consumer to program her robot more easily; other software might be intentionally autonomous and unpredictable. As Curtis Karnow acknowledges, situations like these make for very difficult cases:

The legal system thinks it knows how to handle unpredictable systems.

However, some systems may be designed to be unpredictable. . . . “Fixing” these unpredictable systems to operate predictably will eviscerate and render them useless.

Under these circumstances, the law may hesitate to make a simple assignment of responsibility.

Karnow, *supra* note 179, at 153–54.

252. *See, e.g.,* Rustad & Koenig, *supra* note 193, at 1570 (arguing that software vendors should be liable for damages resulting from foreseeable cybercrimes due to negligent design or inadequate software security); Scott, *supra* note 192, at 462 (arguing that the software industry, which employs “highly trained and skilled programmers” whose “programming is routinized, scrutinized, and supervised by experienced software development managers,” has matured to such an extent that it would be reasonable to hold software vendors liable for product defects); Frances E. Zollers et al., *No More Soft Landings for Software: Liability for Defects in an Industry That Has Come of Age*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 745, 746 (2005) (“[The software industry] has matured to become a dominant sector of the economy. Consequently, it is appropriate to consider liability for defective software in the same light as liability for defective automobiles, pharmaceuticals, and other products.”). The aesthetics are also different. Regardless of who or what is responsible for, say, a collision between a robot and a person in a grocery store, the headline is nonetheless likely to add a more ominous spin: “Robot crashes into man at grocery store.”

R  
R

R  
R  
R

cists.<sup>253</sup> We may not get to this point at all, however, in the absence of legal intervention.<sup>254</sup>

### B. Insurance

If manufacturers and distributors of open robotic platforms are granted immunity for claims arising from user modifications, third party software, and user programming decisions, and if software companies find a way to contract liability away,<sup>255</sup> then liability may fall on users. Robots may be expensive, but users will likely have limited resources. Indeed, the spectacle of uncompensated victims of robot accidents might be just as chilling on the development and use of open robotics as the threat of liability itself.<sup>256</sup> As such, it is worthwhile to explore other ways to compensate victims in the near term.

One option is to encourage or require insurance. Should we follow this route, I propose consideration of several factors relevant to the need for insurance and the amount of insurance coverage. First, the level of insurance should depend on the nature of the robot being insured. Many robots—for instance, small robots used primarily for entertainment—would only need to be insured minimally, if at all.<sup>257</sup> Larger robots with more autonomous functioning—for instance, se-

---

253. Standards eventually evolved for industrial and manufacturing robots. See Christopher Harper & Gurvinder Virk, *Towards the Development of International Safety Standards for Human Robot Interaction*, 2 INT'L J. SOCIAL ROBOTICS 229, 231–32 (2010), available at <http://www.springerlink.com/content/k6r222j243303912/> (reviewing revisions in safety standards for robots in manufacturing). Such standards will be harder to implement with respect to personal robots to the extent that the latter is more open, but doing so will not be impossible. See *id.* at 232–33 (discussing developing standards for nonmedical personal care robots). Indeed, Japan is in the process of developing personal robotics standards, due for public release in 2012. See Martyn Williams, *Panasonic Robot Gives 16-Finger, Automated Hair Washing*, COMPUTERWORLD (Sept. 24, 2010, 3:05 PM), <http://news.idg.no/cw/art.cfm?id=44564365-1A64-6A71-CE11BC59B7A67A80> (predicting that guidelines on the issues of safety standards and liability laws for robots “could be published in Japan as early as 2012”).

254. A presumption against liability for open robots may also have a signaling function, such that people would come to understand that robots are unpredictable and imperfect. See Cass R. Sunstein, *On the Expressive Function of Law*, 144 U. PA. L. REV. 2021, 2025 (1996) (discussing the symbolic content of law and arguing that “the expressive function of law makes most sense in connection with efforts to change norms and that if legal statements produce bad consequences, they should not be enacted even if they seem reasonable or noble”). Were we to open up the possibility of litigation with this assumption in place, perhaps it would filter out the early plaintiffs’ weaker claims.

255. See *supra* note 194 and accompanying text.

256. Cf. Polinsky & Shavell, *supra* note 223, at 1443–50 (discussing market-driven incentives for manufacturers to avoid product risk, such as when consumers avoid unsafe products or pay less for them).

257. Some level of insurance, however small, for any machine properly characterized as a home robot would probably be prudent, at least initially. Even very small robots could



curity robots that patrol a parking lot—would require greater coverage. Indeed, researchers have already begun to classify robots for insurance purposes according to their general capacity to cause damage.<sup>258</sup> This capacity turns on a number of ascertainable factors, such as the robot's mobility, strength, autonomy, and ability to exert control over its environment.<sup>259</sup>

Second, we should consider the uses to which the consumer anticipates putting the robot. Users who use robots for relatively dangerous activities, such as house perimeter security, should probably purchase substantial insurance coverage, whereas those who purchase robots largely for a sense of companionship need take out less coverage, if any. Other factors could include the presence of children or pets in the house or the overall likelihood that the robot will come into contact with strangers.

Any insurance system would no doubt have its flaws. One challenge to personal robot insurance in the context of open robotics, for instance, is that open robots are always changing.<sup>260</sup> A user could initially buy minimal insurance only to later purchase a dangerous hardware module requiring a higher level of insurance, without making the necessary insurance adjustment. Purchase of new software could have a similar effect, with new software rendering a seemingly innocuous robot quite dangerous, or vice versa.

Perfection, however, is not necessarily the goal.<sup>261</sup> Despite the inevitability of some injury and damage, there is little reason to assume that personal robots will regularly harm people or property. After all, commercially available robotic platforms, as well as those under development, have built-in safety features and, in any event, generally lack the capacity for devastation.<sup>262</sup> That being so, it should

---

cause injury and trigger a stifling legal response. *Cf., e.g., supra* text accompanying notes 176–77.

258. See Anniina Huttunen et al., *Liberating Intelligent Machines with Financial Instruments* 5–7 (July 1, 2010) (unpublished manuscript), available at <http://ssrn.com/abstract=1633460> (classifying intelligent machines into different “risk-categories”).

259. *Id.* at 6–7.

260. See *supra* Part III.A.

261. An exhaustive discussion of how best to structure robot insurance is outside the scope of this Article. This part simply presents some preliminary thoughts on the issue in case we decide as a society to head in this direction.

262. See Robotics Indus. Assoc., *RIA Conference to Introduce New Robot Safety Standard Draft*, ROBOTICS ONLINE (July 13, 2010), [http://www.robotics.org/content-detail.cfm/Industrial-Robotics-News/RIA-Conference-to-Introduce-New-Robot-Safety-Standard-Draft/content\\_id/2261](http://www.robotics.org/content-detail.cfm/Industrial-Robotics-News/RIA-Conference-to-Introduce-New-Robot-Safety-Standard-Draft/content_id/2261) (discussing new and practical safety topics to be covered by the “in-depth” industry conference). For example, popular robots such as WowWee’s Rovio and iRobot’s Roomba, currently available for the home, remain low to the ground and only weigh a few pounds. See *Rovio*, WOWWEE, <http://www.wowwee.com/en/support/rovio> (last visited

not be difficult to categorize robotic platforms to a sufficient degree to ensure that early victims will be compensated for their injuries.

## VI. CONCLUSION

Robotics could be the next transformative technology. Whether personal robotics will realize its full potential, however, turns on the degree to which robotics is open to third party innovation. There are several obstacles to openness, many of which are explored elsewhere in cyberlaw. But open robotics faces another, somewhat novel threat: the potential for crippling litigation that cannot be guarded against without dramatically limiting robotic functionality.

I have suggested that one way to mitigate the legal threat to open robotics is to immunize manufacturers of open robotics platforms for the actions and improvements of third parties.<sup>263</sup> This strategy has seen success in the context of firearms and Internet content<sup>264</sup> and could be designed to preserve incentives for safety. The immunity could eventually sunset and be supplemented by a market for consumer robot insurance.<sup>265</sup>

Of course, another way to approach the issue of liability for personal robotics would be to wait until cases surface of their own accord. The well-known advantages of this ad hoc approach include the ability to proceed incrementally and to apply precedent to actual facts.<sup>266</sup> Courts were thus able to domesticate liability in the context of computers.<sup>267</sup> For example, five years before Congress intervened,<sup>268</sup> at least one court anticipated the problem of holding websites accountable for content posted by third party users and looked to the First Amendment to limit liability.<sup>269</sup>

---

Mar. 23, 2011) (claiming that the Rovio weighs only five pounds); *iRobot Roomba 530*, iROBOT, <http://store.irobot.com/product/index.jsp?productId=3881234&cp=2804605.2501652&view=compare&s=D-StorePrice-IRBT&parentPage=family> (last visited Mar. 21, 2011) (claiming that the Roomba 530 weighs only 8.3 pounds).

263. See *supra* Part V.A.

264. See *supra* text accompanying notes 226–40.

265. See *supra* Part V.B.

266. See Nuno Garoupa & Thomas S. Ulen, *The Market for Legal Innovation: Law and Economics in Europe and the United States*, 59 ALA. L. REV. 1555, 1588 (2008) (noting that “a common law judge’s decision of a dispute is not an instantiation of an explicit theory for resolving disputes of the type before him or her” because “common law judges work incrementally, fitting seemingly new fact patterns into existing precedent”).

267. See *supra* text accompanying notes 191–94.

268. See *supra* text accompanying notes 235–37.

269. See *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135, 139–42 (S.D.N.Y. 1991) (“The requirement that a distributor [here an Internet bulletin board operator] must have knowledge of the contents of a publication before liability can be imposed for distributing that publication is deeply rooted in the First Amendment . . .”).

R

R  
R

There are several problems with waiting. First, there could be incalculable costs to innovation as investors and entrepreneurs wait for a test case. It would be difficult to say where general aviation would be today had Congress not waited for the industry to bankrupt before passing GARA.<sup>270</sup> Second, given initial robotics applications such as eldercare, the facts of a lawsuit are not likely to be favorable to the manufacturer-defendant. Extremely sympathetic early plaintiffs could lead to a high profile and recovery and hence a heavy disincentive. Third, in the time it takes for domestic courts to sort out liability, other countries with a higher bar to litigation and a head start may leap far ahead.<sup>271</sup> The unprecedented economic success of the United States has turned in part on its ability to drive technological innovation.<sup>272</sup> Most of the transformative technologies of the twentieth century, including computers and the Internet, originated in America.<sup>273</sup> Other countries are, to some extent, still catching up.<sup>274</sup>

The robotics revolution will take a coordinated, global effort.<sup>275</sup> It is possible that, absent a shift in priorities, the United States will not be a comparatively serious player in this effort.<sup>276</sup> Countries such as Japan have invested heavily in robotics.<sup>277</sup> Japan has also begun to develop personal robotics standards, due out as early as 2012.<sup>278</sup> Even if these standards prove infeasible or unhelpful, Japanese products liability law is less developed than that of the United States, and litiga-

---

270. See *supra* text accompanying notes 219–21.

271. See *supra* text accompanying notes 39–42.

272. See SINGER, *supra* note 1, at 238 (acknowledging that technological innovation was “America’s pathway to power”).

273. See ZITTRAIN, *FUTURE OF THE INTERNET*, *supra* note 18, at 11–12, 26–30 (describing the American origins of computers and the Internet). *But see id.* at 29 (noting that a University of Tasmania employee wrote the piece of code that permitted early PCs to connect to the Internet by modem).

274. Christopher Mims described one example of this “catch-up” in a 2009 article: “The Chinese purchased 39.6 million [PCs] in 2008. . . . But the vast majority of PCs sold in China are running central processing units created by the US companies Intel and AMD.” Christopher Mims, *People’s Processor: Embrace China’s Homegrown Computer Chips*, WIRED MAG. (Dec. 21, 2009, 10:00 AM), [http://www.wired.com/magazine/2009/12/st\\_essay\\_china](http://www.wired.com/magazine/2009/12/st_essay_china).

275. *Cf.* SINGER, *supra* note 1, at 244–45 (noting that China’s approach to technology development depends in part upon its “openness to ideas and technology from abroad”).

276. See, e.g., *id.* at 241 (“Not only do U.S. military robotics developers and makers face huge competition, but many think that they are already behind the field in certain areas. . . . Warned one scientist, ‘The small U.S. humanoid robot community is at risk of being overwhelmed by foreign research, development and commercialization.’”).

277. *Id.* at 242 (noting that “[a]bout a third of all the world’s industrial robots are in Japan” and asserting that “Japan’s success with robotics and [artificial intelligence] comes from a long history of strong government support”).

278. See *supra* note 253.

R

R

R

R

R

R

tion faces greater cultural barriers.<sup>279</sup> The same story can be told about South Korea, which has set an official state goal of having a robot in every home by 2020,<sup>280</sup> as well as China, the European Union, and several other countries.<sup>281</sup>

It is for these reasons this Article has set aside the usual concerns of robotics and the law regarding the nature of personhood and agency in favor of a discussion of the short-term prospects of commercial robotic products. On our current course, we may never reach those other interesting questions. To ensure that we do, cyberlaw must begin to concern itself with how the law should receive personal robotics—lest we risk losing out on a key technology of our age.

---

279. For an overview of modern Japanese products liability law and its origins, see Mark A. Behrens & Daniel H. Raddock, *Japan's New Product Liability Law: The Citadel of Strict Liability Falls, but Access to Recovery Is Limited by Formidable Barriers*, 16 U. PA. J. INT'L BUS. L. 669 (1995). An analysis of how Japanese law might apply to open and closed robots is beyond the scope of this Article.

280. SINGER, *supra* note 1, at 243–44 (describing investment in the Korean robotics industry). **R**

281. *See id.* at 244–46 (describing robotics investment in China); *see also* ROADMAP FOR U.S. ROBOTICS, *supra* note 39, at 1 (“Unfortunately, the United States lags behind other countries in recognizing the importance of robotics technology. While the European Union, Japan, Korea, and the rest of the world have made significant R&D investments in robotics technology, the U.S. investment, outside unmanned systems for defense purposes, remains practically non-existent.”). **R**