MACHINES AS THE NEW OOMPA-LOOMPAS: TRADE SECRECY, THE CLOUD, MACHINE LEARNING, AND AUTOMATION

JEANNE C. FROMER*

ABSTRACT

In previous work, I wrote about how trade secrecy drives the plot of Roald Dahl's novel Charlie and the Chocolate Factory, explaining how the Oompa-Loompas are the ideal solution to Willy Wonka's competitive problems. Since publishing that piece I have been struck by the proliferating Oompa-Loompas in contemporary life: computing machines filled with software and fed on data. These computers, software, and data might not look like Oompa-Loompas, but they function as Wonka's tribe does: holding their secrets tightly and internally for the businesses for which these machines are deployed.

Computing machines were not always such effective secret-keeping Oompa Loompas. As this Article describes, at least three recent shifts in the computing industry—cloud computing, the increasing primacy of data and machine learning, and automation—have turned these machines into the new Oompa-Loompas. While new technologies enabled this shift, trade secret law has played an important role here as well. Like other intellectual property rights, trade secret law has a body of built-in limitations to ensure that the incentives offered by the law's protection do not become so great that they harm follow-on innovation—new innovation that builds on existing innovation—and competition. This Article argues that, in light of the technological shifts in computing, the incentives that trade secret law currently provides to develop these contemporary Oompa-Loompas are excessive in relation to their worrisome effects on follow-on innovation and competition by others. These technological shifts allow businesses to circumvent trade secret law's central limitations, thereby overfortifying trade secrecy protection. The Article then addresses how trade secret law might be changed—by removing or diminishing its protection—to restore balance for the good of both competition and innovation.

 Thanks to Arnaud Ajdler, Audrey Ajdler, Clark Asay, Barton Beebe, Jeremy Bock, Richard Brooks, Bryan Choi, Rochelle Dreyfuss, Nick Feamster, Adam Feibelman, Brett Frischmann, Shane Greenstein, Eric Jardine, Kristin Johnson, Sonia Katyal, Benedict Kingsbury, William Lehr, Ann Lipton, Florencia Marotta-Wurgler, Jonathan Mayer, Julia Powles, Sally Richardson, Jason Schultz, Oleg Sokolsky, Christopher Sprigman, Katherine Strandburg, Katrina Wyman, and Christopher Yoo, and participants at workshops at New York University, Tulane University, and University of Pennsylvania law schools and at the *New York University Law Review* Symposium on "Data Law in a Global Digital Economy" for their focused comments. I gratefully acknowledge support from the Filomen D'Agostino and Max E. Greenberg Research Fund.

INTRODUCTION

In previous work, I wrote about how trade secrecy drives the plot of Roald Dahl's novel *Charlie and the Chocolate Factory*.[1] In the book, Willy Wonka's competitors send spies to work undercover in Wonka's factory so they can discover and then co-opt Wonka's secret candymaking processes for inventive treats, like ice cream that never melts.[2] Wonka fears financial ruin from this spying, so he shuts down his factory and fires all of his employees.[3] Yet some time later, Wonka's factory mysteriously restarts operations without any employees ever going in or out of the factory's gates.[4] The contest at the heart of the novel—in which the five people who find golden tickets in their Wonka candy bars win a visit to the factory—attracts so much enthusiasm and attention in large part because people want to see how the factory is operating without any visible employees.[5]

The contest winners solve the mystery when they enter the factory and learn that a tribe of Oompa-Loompas, tiny song-loving people from Loompaland, is living and working in Wonka's factory.[6] Wonka had lured these Oompa-Loompas to his factory from the dangerous jungles of Loompaland by offering them in exchange for their labor an unlimited supply of cacao beans and chocolate, which they love but could not get in their homeland.[7] For two reasons, the Oompa-Loompas are the ideal solution to Wonka's competitive problems. First, the Oompa-Loompas live in the factory, meaning they would not have occasion to leak Wonka's secret candymaking processes to outsiders.[8] Second, Wonka's competitors could no longer

---

[1] *See* Jeanne C. Fromer, *Trade Secrecy in Willy Wonka's Chocolate Factory*, *in* THE LAW AND THEORY OF TRADE SECRECY: A HANDBOOK OF CONTEMPORARY RESEARCH 3 (Rochelle C. Dreyfuss & Katherine J. Strandburg eds., 2011) (citing ROALD DAHL, CHARLIE AND THE CHOCOLATE FACTORY (Puffin ed. 1998) (1964)).

[2] DAHL, *supra* note 1, at 15–16.

[3] *Id.* at 16.

[4] *Id.* at 14, 16–18.

[5] *Id.* at 20.

[6] *Id.* at 69–71.

[7] *Id.*

[8] *Id.*; *see* Fromer, *supra* note 1, at 5 (discussing this benefit to Wonka).

send in spies under the guise of employment because outside spies could not pass themselves off as the distinctive-looking Oompa-Loompas.[9] As a result, Wonka's inventions are robustly secret (at least until he lets his contest winners into his factory, but that is another story).[10]

Since publishing that piece, which I had intended to be a standalone work about the over-the-top world of Willy Wonka, I have been struck by the proliferating Oompa-Loompas in contemporary life: computing machines filled with software and fed on data. These computers, software, and data might not look like Oompa-Loompas, but they function as Wonka's tribe does: holding their secrets tightly and internally for the businesses for which these machines are deployed.[11]

Computing machines were not always such effective secret-keeping Oompa-Loompas. As this Article describes, at least three recent shifts in the computing industry—cloud computing, the increasing primacy of data and machine learning, and automation—have turned these machines into the new Oompa-Loompas. While new technologies enabled this shift, trade secret law has played an important role here as well. Like other intellectual property rights, trade secret law has a body of built-in limitations to ensure that the incentives offered by the law's protection do not become so great that they harm follow-on innovation—new innovation that builds on existing innovation—and competition. This Article argues that, in light of the technological shifts in computing, the incentives that trade secret law currently provides to develop these contemporary Oompa-Loompas are excessive in relation to their worrisome effects on follow-on innovation and competition by others. These technological shifts allow businesses to circumvent trade secret law's central limitations, thereby overfortifying trade secrecy protection. The Article then addresses how trade secret law might be changed—by removing

---

[9] Fromer, *supra* note 1, at 5.

[10] *See id.* at 5–8 (analyzing this part of Dahl's novel).

[11] Contemporary readers would consider Dahl's original (but later revised) depiction of the Oompa-Loompas racist, with the Oompa-Loompas shown as African Pygmy people and Wonka treating them as slaves. *See* Chryl Corbin, *Deconstructing Willy Wonka's Chocolate Factory: Race, Labor, and the Changing Depictions of the Oompa-Loompas*, 19 BERKELEY MCNAIR RES. J. 47, 51–53 (2012). In no way does this Article seek to import any such racist underpinnings into its analysis. As this Article unpacks, today's machines, like the Oompa-Loompas, can be prevented from leaving a business, making them effective secret-keepers. While this Article addresses the implications of such technological secret-keeping, it does not draw any normative conclusions about the important relationship between trade secret law and labor law.

or diminishing its protection—to restore balance for the good of both competition and innovation.

I
Trade Secret Law as an Intellectual Property Right

This Part provides an overview of U.S. trade secret law before situating it as an intellectual property right. Like its patent and copyright cousins, trade secret law grants rights as incentive to innovate but not so extensively that it undermines follow-on creation and competition.

A. Overview

U.S. trade secret law originated in nineteenth-century common law.[12] As the U.S. Supreme Court has recognized, the principal policies underpinning the protection of trade secrets are "[t]he maintenance of standards of commercial ethics and the encouragement of invention."[13] Until recently, U.S. trade secret law was principally state-based. Every state but New York has enacted a form of the Uniform Trade Secrets Act (whereas New York grounds its trade secrecy protections in its common law).[14] In 2016, Congress enacted the first federal civil trade secret protection in the Defend Trade Secrets Act to supplement state trade secret laws.[15] Its substantive components are principally similar to and based upon the Uniform Trade Secrets Act.[16]

The Uniform Trade Secrets Act defines a "trade secret" as any information—"including a formula, pattern, compilation, program, device, method, technique, or process"—that "derives independent

---

[12] Jeanne C. Fromer, *A Legal Tangle of Secrets and Disclosures in Trade:* Tabor v. Hoffman *and Beyond*, *in* Intellectual Property at the Edge: The Contested Contours of IP 271 (Rochelle Cooper Dreyfuss & Jane C. Ginsburg eds., 2014).

[13] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 481 (1974); *see also* Michael Risch, *Why Do We Have Trade Secrets?*, 11 Marq. Intell. Prop. L. Rev. 1, 5–6 (2007) (noting that one justification for trade secrets is to enforce "commercial ethics"). Another view, articulated by Robert Bone, insists that trade secret law has no independent justification for its existence. Rather, he argues that "trade secret law is merely a collection of other legal norms—contract, fraud, and the like—united only by the fact that they are used to protect secret information." Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 Calif. L. Rev. 241, 245 (1998). To Bone, this mishmash derives from the historical context in which the doctrine emerged. *Id.*

[14] *See, e.g.*, Aaron Nicodemus, *Massachusetts Adopts Uniform Trade Secrets Law*, Bloomberg L. (Aug. 16, 2018), https://www.bna.com/massachusetts-adopts-uniform-n73014481815.

[15] Pub. L. No. 114-153, 130 Stat. 376 (2016) (codified at 18 U.S.C. § 1836 (2012)).

[16] *See* Deerpoint Grp., Inc. v. Agrigenix, LLC, 345 F. Supp. 3d 1207, 1227 (E.D. Cal. 2018) (stating that the federal law is largely modelled after the Uniform Trade Secrets Act).

economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use," and "is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[17]

Not all third-party acquisitions or uses of trade secrets are considered problematic under the law. Only "misappropriation" is prohibited.[18] Although misappropriation can take various forms, the most common types are acquisition, use, or disclosure of another's trade secret by "improper means" or by a person with "a duty to maintain its secrecy or limit its use."[19] Improper means include, but are not limited to, criminal or tortious behavior, such as trespass, fraud, and bribery.[20] They might also encompass some lawful conduct, such as aerial photography of a manufacturing plant under construction.[21] Misappropriation via breach of a duty to maintain secrecy typically arises by virtue of employment or contractual obligations to a trade secret holder.[22]

By definition, a trade secret is protectable as long as it remains secret. That means that trade secrecy protection is potentially infinite in duration, much longer than patent and copyright laws' limited terms of protection.[23]

In practice, however, trade secrecy protection does not always last forever because there are legitimate ways—through acts that are not misappropriation—to acquire or use trade secrets.[24] One such legitimate way is by independent invention or discovery of the secret.[25] Another is via reverse engineering—"by starting with the known product and working backward to find the method by which it was developed."[26] Reverse engineering is considered a proper means

---

17 UNIF. TRADE SECRETS ACT § 1(4), 14 U.L.A. 5 (1985).

18 *Id.* §§ 2–3.

19 *See id.* § 1(2).

20 William E. Hilton, *What Sort of Improper Conduct Constitutes Misappropriation of a Trade Secret*, 30 IDEA 287, 294 (1990).

21 E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1017 (5th Cir. 1970) (holding aerial photography is an improper means).

22 Steven Wilf, *Trade Secrets, Property, and Social Relations*, 34 CONN. L. REV. 787, 794–95 (2002).

23 *See* Michael Abramowicz & John F. Duffy, *The Inducement Standard of Patentability*, 120 YALE L.J. 1590, 1622 (2011) ("Indeed, trade secrecy protection can theoretically provide even more powerful incentives than patents because trade secrecy rights are potentially infinite in duration.").

24 *See* Chicago Lock Co. v. Fanberg, 676 F.2d 400, 404 (9th Cir. 1982) (listing acceptable ways of using trade secrets, such as independent invention and inadvertent disclosure).

25 UNIF. TRADE SECRETS ACT § 1 cmt., 14 U.L.A. 539 (1985).

26 *Id.*

of acquiring a trade secret only if "[t]he acquisition of the known product [is] also . . . by a fair and honest means, such as purchase of the item on the open market."[27] As Robert Bone explains, "independent discovery and reverse engineering [a]re perfectly lawful because . . . . [a] marketed product 'communicate[s]' its contents to the public, so anyone [i]s free to infer those contents from the publicly available product, just as he [i]s free to discover the information from any other publicly available source."[28]

As courts have long held, trade secrecy protection does not extend so far as to give an employer rights in an employee's general knowledge and skill.[29] Because the law does not want to discourage labor mobility—at least too severely—the law permits an employee to take to future employers his or her general knowledge and skill—even to the extent it was acquired at the hands of a previous employer to which the employee has obligations of confidentiality.[30] As one court has memorably put it, "[a]ny other rule would force a departing employee to perform a prefrontal lobotomy on himself or herself."[31] Essentially, the law distinguishes unprotectable general knowledge and skill from specific confidential knowledge, protected as a trade secret, which an employee cannot take to future employment.[32] Although it can be extraordinarily hard to differentiate the two,[33] trade secret law emphasizes that some of an employee's knowledge is never protectable as a trade secret.

B. Trade Secret Law as a Body of Rights and Limitations

As might be apparent from this overview of trade secrecy protection, trade secret law, like other intellectual property rights, contains both a grant of rights and limitations on those rights. This is by design.

---

[27] *Id.*

[28] Bone, *supra* note 13, at 257.

[29] *See, e.g.*, GTI Corp. v. Calhoon, 309 F. Supp. 762, 768 (S.D. Ohio 1969). *See generally* Camilla A. Hrdy, *The General Knowledge, Skill, and Experience Paradox*, 60 B.C. L. REV. (forthcoming 2019) (tracing the origins of this exception to nineteenth-century English common law, and observing that "[c]ourts within virtually every state and federal circuit have purported to recognize this general rule").

[30] *Cf. GTI Corp.*, 309 F. Supp. at 768; SI Handling Sys., Inc. v. Heisley, 753 F.2d 1244, 1261–62 (3d Cir. 1985). Camilla Hrdy further maintains that this exception to trade secrecy protection applies even to information that is otherwise secret. Hrdy, *supra* note 29.

[31] Fleming Sales Co. v. Bailey, 611 F. Supp. 507, 514 (N.D. Ill. 1985).

[32] *GTI Corp.*, 309 F. Supp. at 768.

[33] *See* Kurt M. Saunders & Nina Golden, *Skill or Secret?—The Line Between Trade Secrets and Employee General Skills and Knowledge*, 15 N.Y.U. J.L. & BUS. 61, 75–84 (2018); *see also* Edmund W. Kitch, *The Expansion of Trade Secrecy Protection and the Mobility of Management Employees: A New Problem for the Law*, 47 S.C. L. REV. 659, 664–65 (1996) (describing scenarios in which employees' general knowledge made them marketable).

As noted above, trade secret law is principally thought to promote commercial ethics and innovation.[34] It promotes commercial ethics by forbidding the appropriation or use of trade secrets via improper means and breaches of duties. And it promotes innovation in two interrelated ways. First, by protecting information generated in the innovation process, trade secret law provides an incentive to innovate in the first place.[35] Second, by offering legal protection to information for which a business has undertaken *reasonable* efforts to keep secret, trade secret law reduces both the investment that businesses might otherwise allocate to protect a secret absolutely and the transaction costs for transfers of secret information.[36] In that sense, Mark Lemley observes that the "law develops as a substitute for the physical and contractual restrictions those companies would otherwise impose in an effort to prevent competitors from acquiring their information."[37] Those resources can be directed instead to support innovation.

Trade secret law's purpose of promoting innovation is undermined if its protection extends too far. Specifically, if there were no way at all to acquire or use trade secrets once they qualify for protection, society would be hurt.[38] A trade secret holder could forbid beneficial uses of the secret by others for all time, just as it might use its competitive position to price uses of its secret at out-of-reach prices for many.[39] Moreover, the trade secret holder might not realize all of the valuable applications of its secret information, something that

---

[34] *See, e.g.*, Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 481 (1974); *see also supra* note 13 and accompanying text.

[35] Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 330 (2008). Patent law also provides an incentive to innovate in the first place. For an exploration of the two bodies of law side by side, including possible conflicts between the two, see generally Fromer, *supra* note 12; Jeanne C. Fromer, *The Intellectual Property Clause's Preemptive Effect*, *in* INTELLECTUAL PROPERTY AND THE COMMON LAW 265 (Shyamkrishna Balganesh ed., 2013); Lemley, *supra* at 313.

[36] *See* Lemley, *supra* note 35, at 333–36; *see also* Michael J. Burstein, *Exchanging Information Without Intellectual Property*, 91 TEX. L. REV. 227, 273 (2012) ("[T]he property-like aspects of trade secrecy can help overcome Arrow's paradox in much the same way that patent or copyright can.").

[37] Lemley, *supra* note 35, at 313.

[38] *See* Rochelle Cooper Dreyfuss, *Trade Secrets: How Well Should We Be Allowed to Hide Them? The Economic Espionage Act of 1996*, 9 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1, 2, 33–35 (1998) (noting that society would miss out on potential innovations); Deepa Varadarajan, *Trade Secret Fair Use*, 83 FORDHAM L. REV. 1401, 1404 (2014) ("[T]rade secret law lacks limiting doctrines sufficiently attuned to a defendant's follow-on improvements or to First Amendment interests, like creating a well-informed citizenry and fostering open debate over matters of public interest." (footnote omitted)).

[39] Dreyfuss, *supra* note 38, at 34–35. For example, if third parties could not disassemble a commercially sold device or software to detect its inner—otherwise secret—workings, they would not be able to create compatible products or software, improvements to the existing product, or cheaper versions.

third parties might perceive and capitalize on if they are allowed to use the secret in certain ways.[40]

Some scholars worry that trade secrecy protection can go too far not just on its own internal terms but also if used as a substitute for patent protection. That is, businesses might use trade secrecy to protect otherwise patentable inventions instead of seeking a patent. The cause for concern is typically that patent law requires patentees to disclose their inventions in exchange for a limited term of patent protection.[41] As a result, the public benefits from an increased storehouse of valuable knowledge on which it can build.[42] When businesses resort to trade secrecy instead of patent for an invention, the public is denied access to information about the secret invention and use of the invention after the patent term would end; the pace of innovation can concomitantly slow, to the detriment of society.[43] That said, trade secret law is a viable alternative to patent law only for non-self-disclosing inventions.[44] When an invention is self-disclosing, trade secret law will not provide protection against reverse engineering, thus making patent protection and its requisite disclosures the only plausible choice for protection.[45]

Because of concerns that trade secret law might extend too far and preempt the use of patent law in harmful ways, trade secret law is designed with specific limitations.[46] In particular, trade secret law

---

[40] *Id.* at 34–35.

[41] 35 U.S.C. §§ 112, 154(a) (2012).

[42] *See* Sean B. Seymore, *The Teaching Function of Patents*, 85 NOTRE DAME L. REV. 621, 627 (2010) (arguing that making patents more readable will stimulate innovation). *See generally* Jeanne C. Fromer, *Patent Disclosure*, 94 IOWA L. REV. 539 (2009) (arguing patent disclosure helps fulfill the central goal of stimulating innovation).

[43] *See* Bone, *supra* note 13, at 266; David D. Friedman, William M. Landes & Richard A. Posner, *Some Economics of Trade Secret Law*, 5 J. ECON. PERSP. 61, 64 (1991) ("[T]he common law has plugged several economic holes in the patent statute. It has not done so costlessly; patenting results in the disclosure of socially valuable information, and trade secret protection does not."); Fromer, *supra* note 42. In reality, trade secrecy and patent protection are not always substitutes. Oftentimes, a business can get a patent on an invention and keep all information about the invention that is neither self-disclosing nor required to be disclosed by law as a trade secret. *E.g.*, Brenda M. Simon & Ted Sichelman, *Data-Generating Patents*, 111 NW. U. L. REV. 377, 383 (2017). In that sense, patent and trade secrecy protection can be complementary.

[44] *See* Lemley, *supra* note 35, at 313; Katherine J. Strandburg, *What Does the Public Get? Experimental Use and the Patent Bargain*, 2004 WIS. L. REV. 81, 111.

[45] Strandburg, *supra* note 44, at 111.

[46] In this way, it is just like other forms of intellectual property: Out of the same concerns that too-strong protection would undermine the beneficial creation and innovation the law seeks, patent and copyright laws are designed to be limited in time and scope in particular ways. *See, e.g.*, Dreyfuss, *supra* note 38, at 2, 33–34; Jeanne C. Fromer, *Expressive Incentives in Intellectual Property*, 98 VA. L. REV. 1745, 1752 (2012); Lemley, *supra* note 35, at 314, 330.

allows third parties to gain the knowledge and information in a trade secret through independent discovery or reverse engineering. By deeming these means to be legitimate ways to acquire or use a trade secret, the law ensures that some third-party uses of the secret are allowable. Additionally, trade secret law allows employees to carry their general knowledge and skill to new jobs, indicating that not all information connected to trade secrets is off-limits for use, even for those with duties to guard these secrets.[47] These limitations also make patent protection more attractive than trade secrecy protection in many instances, by making protection less vulnerable to circumvention via these limitations.[48] Consider the societal benefits offered by a third party's reverse engineering or independent discovery of a trade secret. As permissible paths toward learning another's trade secret, the information third parties obtain by reverse engineering and independent discovery can be used legitimately in the marketplace.[49] These third parties help society by providing more competition in the marketplace for the innovation connected to a business's trade secret.[50] These third parties also often can use the knowledge they have gained via reverse engineering or independent discovery to improve on the existing secret via cost reductions, further advances in technology, or new applications, all to society's benefit.[51] And this knowledge is not something which third parties stumble over for free: Third parties that opt to reverse engineer or independently discover a trade secret typically must invest significant amounts of time and resources to unearth the secret's inner workings.[52] That means that

---

[47] *See* Dan L. Burk & Brett H. McDonnell, *The Goldilocks Hypothesis: Balancing Intellectual Property Rights at the Boundary of the Firm*, 2007 U. ILL. L. REV. 575, 609 (noting this movement is good for industry). The European Union also contains these three important limitations—independent discovery, reverse engineering, and exclusion of general knowledge—in its directive on trade secrecy protection. Directive 2016/943, of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, 2016 O.J. (L 157) 1.

[48] Dreyfuss, *supra* note 38, at 16–17, 32.

[49] *See* Leo J. Raskind, *Reverse Engineering, Unfair Competition, and Fair Use*, 70 MINN. L. REV. 385, 395–96 (1986); Simon & Sichelman, *supra* note 43, at 407. Rochelle Dreyfuss makes the case that reverse engineering is yet more important than independent discovery because "[i]f reverse engineering were prohibited, trade secrets would endure until they were rediscovered—which could be for [excessively] long [times]." Dreyfuss, *supra* note 38, at 16.

[50] Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1588 (2002).

[51] Dreyfuss, *supra* note 38, at 34–35; Friedman, Landes & Posner, *supra* note 43, at 67, 70; J.H. Reichman, *Legal Hybrids Between the Patent and Copyright Paradigms*, 94 COLUM. L. REV. 2432, 2521–22 (1994).

[52] Friedman, Landes & Posner, *supra* note 43, at 70; Reichman, *supra* note 51, at 2521–22; Samuelson & Scotchmer, *supra* note 50, at 1582.

this limitation does not undermine the benefits of trade secrecy protection too readily.[53]

Now consider the benefit society gets from employees being able to take their general knowledge and skill to new employers. Not only does it promote labor mobility by enabling individuals to seek reemployment in areas of expertise, but it also promotes competition and innovation. Employees are carriers of knowledge and skill that they have accrued through their employment experiences.[54] Each time an employee takes a new job, that employee brings along heightened general knowledge to his or her employer's advantage (even without the use of specific secret information which the employee has a duty to a previous employer not to disclose or use).[55] Society benefits from these interfirm knowledge spillovers that employee carriers cause. As Ron Gilson explains, "[t]hese knowledge spillovers supercharge the innovative capacity of [a region] . . . , facilitating the development of new technologies that create a new industrial life cycle."[56] Even individual employers generally benefit from these spillovers of knowledge, assuming they profit from new employees bringing their general knowledge and skill at least as much as they lose from ex-employees taking the knowledge and skill gained in their employ elsewhere.[57] In fact, scholars explain the success of Silicon Valley by employees' frequent job shifts among the region's companies, where they deploy and transfer the general knowledge and skill they have gained elsewhere.[58]

Because of the benefits to innovation they bestow on society as critical limitations on otherwise excessive trade secrecy protection, reverse engineering, independent discovery, and the free use of an employee's general knowledge and skill are critical components of trade secret law. These limitations ensure that trade secret law does not extend such broad protection that it undermines the innovation benefits the law seeks to promote.

---

[53] Samuelson & Scotchmer, *supra* note 50, at 1582. The threat of reverse engineering and the costs involved might also encourage secret holders to license their secrets to competitors. *Id.* at 1589.

[54] *See* Ronald J. Gilson, *The Legal Infrastructure of High Technology Industrial Districts: Silicon Valley, Route 128, and Covenants Not to Compete*, 74 N.Y.U. L. Rev. 575, 593 (1999).

[55] *Id.* at 582–83.

[56] *Id.* at 586.

[57] *Id.* at 596.

[58] One explanation is that the business culture in Silicon Valley encourages employees to hop from one start-up company to the next, AnnaLee Saxenian, Regional Advantage: Culture and Competition in Silicon Valley and Route 128, at 34–37, 111–17 (1994), but a more convincing explanation is that California law (alone in the United States) encourages this mobility by banning all non-competition agreements. Gilson, *supra* note 54, at 578.

II
MACHINES AS THE NEW OOMPA-LOOMPAS

Until recently, trade secret law was of somewhat limited relevance for software and computing innovation.[59] Since the 1980s, software has been made and sold independently of the hardware on which it runs. Even though such software is written by programmers in source code—text listing commands in a computer programming language that is understandable by programmers—it has until recently principally been distributed in object code, a compiled form of the source code—often binary code of zeroes and ones—to be executed directly on a computer but which is not easily read and understood, even by expert programmers.[60] Established techniques in the software industry have enabled programmers to reverse engineer object code, obtaining some approximation of the corresponding source code.[61] Therefore, even though businesses could keep their source code secret, sales of the corresponding object code have left the source code plausibly vulnerable to legitimate discovery via reverse engineering.[62] Moreover, with software engineers and programmers frequently changing jobs in the high-technology sector, they carry their general knowledge and skill sharpened at one company to another.[63] For these reasons—along with the reality over the past few decades that patent and copyright could frequently protect software instead—businesses have long been reluctant to rely heavily on trade secrecy protection for their software.[64]

---

[59] The earliest software, in the mid-twentieth century, was integrated tightly into hardware, which was the primary focus of computer industry marketing and sales. Bradford L. Smith & Susan O. Mann, *Innovation and Intellectual Property Protection in the Software Industry: An Emerging Role for Patents?*, 71 U. CHI. L. REV. 241, 242 (2004). During this phase, "software's tight integration with hardware and the . . . industry's vertical structure led . . . firms to rely primarily on trade secret protection and contract law to guard their innovations against appropriation by others." *Id.* After this early stage, industry conditions changed because software was disaggregated from hardware. As discussed in this Part, current industry conditions are reverting to an amplified version of the primordial state—in which software was closely integrated with hardware—and the corresponding preference for stronger trade secrecy protection.

[60] *Id.* at 242, 248.

[61] *See* Samuelson & Scotchmer, *supra* note 50, at 1608–09; Samuel J. LaRoque, Comment, *Reverse Engineering and Trade Secrets in the Post-*Alice *World*, 66 KAN. L. REV. 427, 439–40 (2017) (discussing the reverse engineerability of code written in the Java programming language as compared to other languages in the context of evaluating the elevated desirability of protecting software with trade secrecy after the Supreme Court, in *Alice Corp. v. CLS Bank International*, 573 U.S. 208 (2014), made it harder to protect software instead with patents).

[62] Samuelson & Scotchmer, *supra* note 50, at 1608–09.

[63] Gilson, *supra* note 54, at 585–86.

[64] Samuelson & Scotchmer, *supra* note 50, at 1607–13.

That said, businesses have found ways to rely successfully on trade secret law to protect aspects of software that were disclosed to the public.[65] Businesses can sell their software publicly but nonetheless protect it with trade secrecy by limiting its use and disclosure by license.[66] And businesses have been increasingly including prohibitions on reverse engineering of their software in their licenses,[67] making trade secrecy protection a pervasive and heftier possibility. Because these contractual prohibitions eliminate trade secrecy's reverse-engineering safety valve, many scholars decry them as anticompetitive and counterproductive to innovation.[68]

Until recently, then, software companies relying on trade secrecy for software have sought to use contract to make trade secrecy more muscular than it would naturally be. Contractual restrictions on disclosure and reverse engineering diminish an otherwise critical intrinsic weakness of trade secrecy for software: software's openness to independent discovery and reverse engineerability. The propensity to turn to contract law to make software secret is based on the assumption that, without it, software is public, or at least discoverable.

Nevertheless, as explored in this Part, three recent and growing trends in computing—cloud computing, the increasing primacy of data and machine learning, and automation—have turned software from discoverable secret that needs contract to shield it into a true black box, a fully ensconced Oompa-Loompa. These trends have done so by technologically undermining the three critical limitations on trade

---

[65] *See* Michael Risch, *Hidden in Plain Sight*, 31 BERKELEY TECH. L.J. 1635, 1648–49 (2016) (citing cases).

[66] *See* Sonia K. Katyal, *The Paradox of Source Code Secrecy*, 104 CORNELL L. REV. (forthcoming 2019) (arguing that protecting source code through trade secrecy is a rational response to the "uncertain and porous boundaries" of software protection through copyright and patent); Risch, *supra* note 65, at 1649 (discussing the long line of cases upholding the protection of trade secrets); Deepa Varadarajan, *The Trade Secret-Contract Interface*, 103 IOWA L. REV. 1543, 1556 (2018) (describing how firms routinely use confidentiality contracts to help protect trade secrets and how courts consider nondisclosure contracts to be important evidence in trade secret cases).

[67] *See* Florencia Marotta-Wurgler & Robert Taylor, *Set in Stone? Change and Innovation in Consumer Standard-Form Contracts*, 88 N.Y.U. L. REV. 240, 257 (2013).

[68] *See* Rochelle Cooper Dreyfuss, *Do You Want to Know a Trade Secret? How Article 2B Will Make Licensing Trade Secrets Easier (But Innovation More Difficult)*, 87 CALIF. L. REV. 191, 263 (1999) (proposing commentary to Article 2B clarifying the extent of judicial discretion to consider effects on competition); David A. Rice, *Public Goods, Private Contract and Public Policy: Federal Preemption of Software License Prohibitions Against Reverse Engineering*, 53 U. PITT. L. REV. 543, 623 (1992) (alleging that software distribution contracts aim to foreclose competition); Samuelson & Scotchmer, *supra* note 50, at 1581.

secrets: independent discovery, reverse engineering, and the free use of an employee's general knowledge and skill.[69]

Trade secrecy protection has also become more attractive as other forms of intellectual property protection have become less alluring for computing innovation. As Sonia Katyal has traced, patent and copyright laws' increasingly constricted and unpredictable protection for software has made trade secrecy ever more attractive for software producers.[70] For decades, protection for software under copyright and patent laws has waxed and waned—owing to a less-than-ideal fit for software with each form of protection—leaving some unpredictability in choosing either path for protection.[71] Most recently, two Supreme Court decisions left it harder to protect software broadly under patent law.[72] As for copyright law, its coverage of software was long thought to be relatively minimal—protecting principally against piracy but not against non-literal copying or copying of functionality[73]—until recent developments in which one court has prominently allowed copyright to protect arguably functional elements of software.[74] These changes yet further enhance trade secrecy's appeal for computing innovation, especially in light of the changing trends in the industry, to which I now turn.

A. Cloud Computing

Cloud computing denotes a variety of different computing services, all of which spread computer power diffusely over the internet (referred to as the "cloud"), rather than situating it in one's own personal computer, as has traditionally been done.[75] For example, one variety of cloud computing involves storing and accessing one's digital

---

[69] *Cf.* Katyal, *supra* note 66 (noting that source-code secrecy generates a critical paradox—"the very substance of what is secluded often stems from the most public of origins, and often produces the most public of implications," such as for civil liberties—and criticizing "intellectual property law [for] fail[ing] to offer a consistent pathway towards disclosure, leading to a domain where source code is dominated by trade secrecy").

[70] *Id.*

[71] *Id.* (citing cases and law).

[72] Alice Corp. v. CLS Bank Int'l, 573 U.S. 208 (2014); Bilski v. Kappos, 561 U.S. 593 (2010).

[73] Clark D. Asay, *Software's Copyright Anticommons*, 66 EMORY L.J. 265, 273–79 (2017); Pamela Samuelson, *Functionality and Expression in Computer Programs: Refining the Tests for Software Copyright Infringement*, 31 BERKELEY TECH. L.J. 1215, 1224–45 (2016).

[74] *See* Asay, *supra* note 73, at 296–307 (discussing Oracle Am., Inc. v. Google Inc., 750 F.3d 1339 (Fed. Cir. 2014)); Samuelson, *supra* note 73, at 1252–58 (same).

[75] Steve Ranger, *What Is Cloud Computing? Everything You Need to Know About the Cloud, Explained*, ZDNET (Dec. 13, 2008), https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-from-public-and-private-cloud-to-software-as-a; *see also* Orly Mazur, *Taxing the Cloud*, 103 CALIF. L. REV. 1, 8 (2015); Marc Aaron

files remotely in the cloud, such as through Dropbox or Carbonite. Another form—most relevant for this Article's purposes—involves software or platform that is offered via the cloud as a service. Some popular examples are cloud email services, such as Google's Gmail; cloud word processing software, such as Microsoft Office 365 Word and Google Docs; and social-media platforms, such as Facebook and Instagram. With these services, much of the source code and object code underpinning the provided software can be kept inaccessible to users. A user can observe the user interface of the software service, the user's input, and the software service's output, but not much else. The bulk of the software necessary to run the service can be stored, and the bulk of the processing is done, on the provider's secure computers rather than on the user's.[76] Cloud-based services are no insignificant niche of software. Rather, they have grown very popular, and public cloud services revenues are forecast to reach over $350 billion this year.[77]

With the growth of cloud computing, businesses now have a technological path—not only a contractual path—toward robust secrecy of their software. In distributing cloud-based software to consumers, businesses no longer have to release most of the substance of their software, as they once did via object code (or source code). Instead, their software can run mostly in the cloud, out of sight of consumers. In these situations, consumers thus have little to go on to reverse engineer—let alone independently discover—the secrets underlying cloud-based software.[78] With its object code kept hidden, no longer is this software at the mercy of those consumers who have sufficient expertise and devotion to reverse engineer it from object code. Many software providers' switch from distribution of object code, or source code, too, to cloud computing thereby seals off this software from the

---

Melzer, *Copyright Enforcement in the Cloud*, 21 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 403, 404 (2011).

[76] *See* Melzer, *supra* note 75, at 406–07; Risch, *supra* note 65, at 1663.

[77] Louis Columbus, *Cloud Computing Market Projected to Reach $411B by 2020*, FORBES, (Oct. 18, 2017, 6:12 PM), https://www.forbes.com/sites/louiscolumbus/2017/10/18/cloud-computing-market-projected-to-reach-411b-by-2020.

[78] Sharon Sandeen explores the converse phenomenon of whether otherwise secret information that is stored in a third-party's cloud server is protectable as a trade secret. Sharon K. Sandeen, *Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection*, 19 VA. J.L. & TECH. 1 (2014). Other works explore the implications of cloud computing for different forms of intellectual property regimes or other laws altogether. *E.g.*, Jared A. Harshbarger, *Cloud Computing Providers and Data Security Law*, 16 J. TECH. L. & POL'Y 229 (2011) (data security); Mazur, *supra* note 75 (tax and copyright); Hien Timothy M. Nguyen, Note, *Cloud Cover: Privacy Protections and the Stored Communications Act in the Age of Cloud Computing*, 86 NOTRE DAME L. REV. 2189 (2011) (privacy).

possibility of reverse engineering, one of the key limitations on trade secrecy protection.

B. The Elevation of Data and Machine Learning

Another key technological shift in recent years has been the elevation of data and machine learning as a central feature of valuable software. As Harry Surden explains, machine learning "involves computer algorithms that have the ability to 'learn' or improve in performance over time on some task."[79] Machine learning either involves only an early burst of learning before deployment or also repeated rounds of subsequent learning as the computer engages with the world.[80] In recent years, these techniques have been among the most successful and prominent ways of imbuing computers with artificial intelligence, or human-like cognitive abilities.[81] They have been used in a wide-ranging set of commercial and research applications, including teaching cars to drive autonomously,[82] devices to speak and understand natural languages like English,[83] computers to make bail decisions based on predictions of whether an arrestee is at risk of flight or commission of another crime,[84] and computers to recognize the objects in an image, be they cats, specific people, or apples.[85] These resulting software applications and devices containing them are valued at billions of dollars, and the sector is expected to grow yet further in value in the coming years as businesses spend increasing sums—also billions of dollars—on machine learning research.[86]

The critical ingredients of machine learning are relevant data and statistical techniques.[87] Machine learning begins with a problem that someone (be it a researcher, business, or government) would like to automate, such as how to teach a car to recognize people and other

---

[79] Harry Surden, *Machine Learning and Law*, 89 WASH. L. REV. 87, 88 (2014).

[80] *See generally* MICHAEL J. KEARNS & UMESH VAZIRANI, AN INTRODUCTION TO COMPUTATIONAL LEARNING THEORY (1994); STUART RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH (3d ed. 2010).

[81] *See* RUSSELL & NORVIG, *supra* note 80.

[82] AI NOW INST., AI NOW REPORT 2018, at 20, 23 (2018), https://ainowinstitute.org/AI_Now_2018_Report.pdf.

[83] Surden, *supra* note 79, at 88.

[84] *See* State v. Loomis, 881 N.W. 2d 749, 754 (Wis. 2016) (describing the COMPAS risk-assessment tool), *cert. denied sub nom.* Loomis v. Wisconsin, 137 S. Ct. 2290 (2017).

[85] Amanda Levendowski, *How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem*, 93 WASH. L. REV. 579, 591–93 (2018).

[86] Louis Columbus, *Roundup of Machine Learning Forecasts and Market Estimates, 2018*, FORBES (Feb. 18, 2018, 7:00 PM), https://www.forbes.com/sites/louiscolumbus/2018/02/18/roundup-of-machine-learning-forecasts-and-market-estimates-2018.

[87] *See* David Lehr & Paul Ohm, *Playing with the Data: What Legal Scholars Should Learn About Machine Learning*, 51 U.C. DAVIS L. REV. 653, 655 (2017).

objects so as not to hit them while driving autonomously, how to predict whether it is safe for society to release an arrestee from jail pending trial, and how to recognize the English words that a speaker is saying.[88] The programmer then acquires data relevant to solving that problem, to use them to train and test a computational model using statistical techniques that fits those data.[89] In the preceding examples, those input data might be, respectively, images taken on the road that contain zero or more objects to avoid hitting, wide-ranging data about arrestees, and English speech.

Acquiring the requisite data is easier said than done. The difficulty ultimately stems from the large—nay, massive—reams of relevant data that are required to learn an accurate model to encode in software.[90] Acquiring this "big data" is incredibly expensive. Either an entity develops access to data by investing intensively to attract millions or billions of users to provide data directly via recurrent interactions with it, as Facebook does by cultivating users' relentless posts of text, images, videos, and links,[91] or, alternatively, wealthy businesses can spend exorbitant sums to get "big data" by buying it from third parties or partnering with them to learn from partner-generated data together.[92]

Once these data are acquired and cleaned, they are typically partitioned into a training set and a test set.[93] Statistical techniques are then used on the training set of data to develop a model that explains the data (say, whether age is a good predictor of recidivism or whether those who buy glue also buy scissors).[94] This model can then be evaluated on the test set of data to see how predictive it is.[95] After the model is fine-tuned, it can be deployed in the real world with new real-world data to make predictions (such as whether something on the road is a human that a car should avoid hitting).[96] The model can optionally be updated from time to time to take into account new learning based on the real-world data being acquired.[97]

---

[88] *See id.* at 668, 672–77; *see also* Surden, *supra* note 79, at 88.

[89] Lehr & Ohm, *supra* note 87, at 677–78.

[90] *Id.* at 678–79; Levendowski, *supra* note 85, at 606.

[91] *See* Levendowski, *supra* note 85, at 606–07.

[92] *Id.* at 607–09.

[93] Lehr & Ohm, *supra* note 87, at 684–86.

[94] *See id.* at 688–98.

[95] *Id.* at 698–700.

[96] *Id.* at 701–02.

[97] *See, e.g.*, Marilyn A. Walker, Jeanne C. Fromer & Shrikanth Narayanan, *Learning Optimal Discourse Strategies: A Case Study of a Spoken Dialogue Agent for Email*, 1998 Ass'n Computational Linguistics Ann. Meeting 1345, http://www.aclweb.org/anthology/P98-2219.pdf.

Two underlying developments in recent years have enabled the extensiveness and utility of machine learning: computing power and big data. Machine learning techniques can require extensive computing resources, so the growth of processing power over recent years has been critical to machine learning's increasing prominence.[98] Moreover, in the digital and networked world in which we live, businesses can more readily collect comprehensive and copious data that can then be used as the requisite input to a wide variety of machine learning algorithms.[99]

The software that deploys models acquired through machine learning operates differently than pre-machine learning iterations of the same software. In particular, software built out of machine learning can personalize or differentiate services offered to different users based on its underlying model of users. For example, if Amazon has developed a model of consumer purchasing behavior, it might set prices differentially based on specific consumer characteristics (rather than hold prices uniform for all users). Or Netflix might recommend specific creative content, not to mention the specific image used to signify each creative work, based on user characteristics such as race or gender, as a way to preferentially deliver content Netflix predicts each user might want.[100]

Putting aside the not insignificant privacy and civil-liberties issues raised by the increasing uses of data and machine learning,[101] these changes also have shifted the technological realities of software's secrecy. The most valuable aspects of any software built using machine learning techniques are its underlying data and model.[102] Both can be kept secret and practically free from independent discovery and reverse engineering, two of trade secrecy protection's key

---

[98] *See* Anupam Datta, Shayak Sen & Yair Zick, *Algorithmic Transparency via Quantitative Input Influence: Theory and Experiments with Learning Systems*, 2016 IEEE SYMP. ON SECURITY & PRIVACY 598, 614, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnumber=7546525.

[99] Levendowski, *supra* note 85, at 606–07.

[100] *See* Lara Zarum, *Some Viewers Think Netflix Is Targeting Them by Race. Here's What to Know.*, N.Y. TIMES (Oct. 23, 2018), https://www.nytimes.com/2018/10/23/arts/television/netflix-race-targeting-personalization.html.

[101] *See, e.g.*, FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015) (exploring the incongruity between the additional secrecy sought by industries and the loss of privacy to individuals); Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008) (advocating a new concept of "technological due process" to preserve traditional procedural protections in a digital era); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93 (2014) (arguing that "individuals affected by Big Data should have similar rights to those in the legal system with respect to how their personal data is used in adjudications").

[102] *See* Levendowski, *supra* note 85, at 590–91.

limitations. As such, it is technologically plausible to protect the valuable parts of software derived through machine learning.

Consider first the data that go into machine learning. Not only are these data typically acquired confidentially by a business in the first instance, but they can also be kept internal and secret down the line.[103] The data can be kept internal because machine learning software needs data as input but has no need to store them in its output, the predictive algorithm it generates.[104] Moreover, it is practically impossible to discover these data independently, as few businesses possess the vast resources required to acquire (or generate) the data in the first place.[105] It is also essentially impossible to reverse engineer these data because they are not discernable from any commercially available software based on machine learning, precisely because they are not contained within the software and because any predictive model built on these data is likely to be too complex to convert back into even a rough approximation of the underlying data.[106] For these reasons, trade secrecy's two key limitations of independent discovery and reverse engineering are unavailable to gain access to the data underpinning machine learning models. As Amanda Levendowski explains, the unavailability of these data also negatively affects competition: "Without the resources to get the vast

---

[103] *See* Neil M. Richards & Jonathan H. King, *Three Paradoxes of Big Data*, 66 STAN. L. REV. ONLINE 41, 42–43 (2013). Brenda Simon and Ted Sichelman study a related issue of how a patentee can leverage the reams of data generated by use of its patented technology for further competitive advantage. *See generally* Simon & Sichelman, *supra* note 43. They think this leveraging of data-generating patents ("inventions [which] by their operation and use may generate large amounts of data beyond the invention itself—for instance, data about users, other persons, or even the world in general") is worrisome. *Id.* at 379. The principal reason is that during the patent term, the patentee also can assert trade secret protection over the generated data without having to worry about independent discovery or reverse engineering, both activities that would constitute patent infringement. *Id.* They worry about anticompetitive effects of this leveraging, and principally suggest changes to patent law to address the concerns they discuss. *Id.* at 380–81, 427–33. In fact, they think that resort to trade secret law alone would cure the problems they raise because "competitors can all use the offensive and defensive aspects of trade secret law—including reverse engineering and independent discovery—which arguably increases innovation incentives and drives down prices." *Id.* at 428. As this Part shows, that is far from the case.

[104] *See supra* notes 87–97 and accompanying text.

[105] *See* Levendowski, *supra* note 85, at 606–09.

[106] Other scholars have noted the opaqueness of predictive models developed through machine learning, either by their nature or through gaming. *See* Jane Bambauer & Tal Zarsky, *The Algorithm Game*, 94 NOTRE DAME L. REV. 1, 27–28 (2018); Emily Berman, *A Government of Laws and Not of Machines*, 98 B.U. L. REV. 1277, 1318 (2018); *supra* text accompanying note 104. These developments extend the complexity of software, well beyond its already increasingly intricate and modular state. *See* Katyal, *supra* note 66 (noting the increasing complexity and modularization of software over time).

amounts [of] data easily acquired by major . . . players, meaningful competition becomes all but nonexistent."[107]

Moreover, the predictive models that machine learning techniques derive from data can also be kept secret by keeping them internal to the organization deploying them.[108] By being kept internal, such models—like the data from which they are constructed—would typically remain off-limits to reverse engineering or independent discovery, particularly if the data on which the model is premised are also unavailable.[109]

In these ways—and like cloud computing's increasing prevalence—the elevation of data and machine learning as central aspects of the software industry has technologically made software and the devices containing it more robustly secret.

C. Automation

A third change making secrecy more technologically robust for software-based devices is businesses' automation of tasks that have principally been done in the past by human employees (or contractors). The automation trend is in an early stage, much more so than the previous two technological trends explored above. That said, businesses have been increasingly replacing their factory workers with robots for production, picking, or packing; store cashiers with automated checkout machines; customer-service representatives with software imbued with natural-language processing capabilities; and so forth.[110] Although the reliability of forecasts on the effects of automa-

---

[107] Levendowski, *supra* note 85, at 609.

[108] *See, e.g.*, AI NOW INST., LITIGATING ALGORITHMS: CHALLENGING GOVERNMENT USE OF ALGORITHMIC DECISION SYSTEMS (Sept. 2018), https://ainowinstitute.org/litigatingalgorithms.pdf (analyzing algorithmic decision systems and their impact on rights and liberties in the context of government benefits, education, social science, and criminal law); *cf.* DILLON REISMAN, JASON SCHULTZ, KATE CRAWFORD & MEREDITH WHITTAKER, AI NOW INST., ALGORITHMIC IMPACT ASSESSMENTS: A PRACTICAL FRAMEWORK FOR PUBLIC AGENCY ACCOUNTABILITY (2018), https://ainowinstitute.org/aiareport2018.pdf (calling for an end to the use of unaudited "black box" systems in core public agencies, and proposing an Algorithmic Impact Assessment framework to support affected communities and stakeholders).

[109] That said, a limited set of machine learning models that are accessible via online query (namely, those that accept partial feature vectors as inputs and include confidence values with predictions) have been shown to be reverse-engineerable, though countermeasures might be employed to minimize this possibility. *See* Florian Tramèr, Fan Zhang, Ari Juels, Michael K. Reiter & Thomas Ristenpart, *Stealing Machine Learning Models via Prediction APIs*, 25TH USENIX SECURITY SYMPOSIUM 601 (2016), https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_tramer.pdf.

[110] *See generally* ERIK BRYNJOLFSSON & ANDREW MCAFEE, THE SECOND MACHINE AGE: WORK, PROGRESS, AND PROSPERITY IN A TIME OF BRILLIANT TECHNOLOGIES (2014) (analyzing the effects of technological displacement due to automation); Cynthia Estlund, *What Should We Do After Work? Automation and Employment Law*, 128 YALE L.J. 254

tion is open to some question,[111] one recent report by the McKinsey Global Institute concluded that up to one-third of the current American labor force stands to have its jobs automated by 2030.[112] This report also predicts that although less than five percent of current jobs are in a position to be fully automated, sixty percent of current jobs could become one-third automated.[113] Some suspect that even though displaced workers might switch careers and that automation will open up new categories of jobs for people, there could be a net loss of employment.[114]

In addition to the myriad of potential societal consequences that a shift toward automation would have on human happiness, subsistence, and inequality,[115] automation that replaces a substantial amount of employment also turns more business knowledge into an impenetrable secret. How so? While a human can leave the employ of one business to take up employment at a competitor,[116] a machine performing this employee's task would never do so. Such machines would remain indefinitely at a business's disposal, keeping all their knowledge self-contained within the business's walls. Increasing automation thereby makes secrecy more robust than ever before. Whereas departing employees can legally take their elevated general knowledge and skill to new jobs, a key path by which knowledge spills across an industry,[117] machines automating employees' tasks will never take their general knowledge and skill elsewhere to competi-

(2018) (charting a path for reforming labor and employment law in response to the impact of automation on jobs); Camilla A. Hrdy, *Intellectual Property and the End of Work*, 70 FLA. L. REV. (forthcoming 2019).

111 *E.g.*, David H. Autor, *Why Are There Still So Many Jobs? The History and Future of Workplace Automation*, 29 J. ECON. PERSP. 3 (2015).

112 MCKINSEY GLOBAL INST., JOBS LOST, JOBS GAINED: WORKFORCE TRANSITIONS IN A TIME OF AUTOMATION 11 (Dec. 2017), https://www.mckinsey.com/~/media/mckinsey/featured%20insights/Future%20of%20Organizations/What%20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20and%20wages/MGI-Jobs-Lost-Jobs-Gained-Report-December-6-2017.ashx. Other reports have similar estimates. *See, e.g.*, Nicolas Yan, *Automated Inequality*, HARV. POL. REV. (Oct. 2, 2016), http://harvardpolitics.com/world/automation (citing two such reports).

113 MCKINSEY GLOBAL INST., *supra* note 112, at 2.

114 *Cf.* Bryan Clagett, *Automation Is in Your Future, and the Future Is Now*, FORBES, (Oct. 18, 2018), https://www.forbes.com/sites/forbescommunicationscouncil/2018/10/18/automation-is-in-your-future-and-the-future-is-now. This period is not the first in which people have worried about a net loss of employment due to technological development, though there is the view that this moment is different than the previous periods that provoked anxiety but no net job loss over time. *See* Joel Mokyr, Chris Vickers & Nicolas L. Ziebarth, *The History of Technological Anxiety and the Future of Economic Growth: Is This Time Different?*, 29 J. ECON. PERSP. 31 (2015).

115 *See generally* BRYNJOLFSSON & MCAFEE, *supra* note 110; Estlund, *supra* note 110.

116 *See supra* Part I.

117 *See supra* notes 28–30 and accompanying text.

tors. Thus, by decreasing the number of employees that might carry their general knowledge and skill to new jobs and in any event the amount of knowledge and skill that each employee might have to take,[118] increasing automation undermines a critical limitation on trade secrecy protection.[119]

In sum, the three computing trends discussed in this Part—cloud computing, the elevation of data and machine learning, and automation—have harnessed technology to make secrets contained within software and computing devices intrinsically robust. These trends thereby alter the longstanding lack of intrinsic secrecy for the software industry. Moreover, they undermine the three critical limitations on trade secrecy protection—independent discovery, reverse engineering, and lack of protection of an employee's general knowledge and skill. As a practical matter, then, these industry trends now mean that secrecy and trade secrecy protection for contemporary software and computing devices can last indefinitely. These developments have thereby turned computing machines into the new Oompa-Loompas: Just as Willy Wonka found a robust way to keep his valuable candymaking processes secret by employing a tribe of Oompa-Loompas, so too today's machines can house their software and data secrets robustly without much risk of exposure.[120] The next Part turns to consider the implications of these shifts for competition and follow-on innovation, ultimately arguing that it is due time to consider how to

---

[118] Automated replacements of employees might be developed either internally or externally. These human developers themselves might have some heightened knowledge and skill instead of the employees replaced by automation. That said, there are surely going to be fewer such people with such knowledge and skill should automation advance. Moreover, given that automated replacements of employees are often trained using machine learning rather than being encoded by the maker of the automation with hard-coded knowledge, the makers of the automation might not even come close to possessing the knowledge and skill that the replaced employees have. *See* Cabe Atwell, *Turning to Machine Learning for Industrial Automation Applications*, ELECTRONIC DESIGN (Dec. 19, 2017), https://www.electronicdesign.com/industrial-automation/turning-machine-learning-industrial-automation-applications (explaining how companies are using machine learning in their industrial automatic and manufacturing facilities).

[119] Camilla Hrdy worries about the labor-destroying forces of automation, and suggests depriving such inventions of patent protection as a way to minimize the incentives to create them. Hrdy, *supra* note 110.

[120] Although there has already been some technological secrecy because it has been mandated by contract, *see supra* text accompanying notes 65–68, secrecy that is inherent to a technology provides the secret holder with more power as it is implausible, if not impossible, to circumvent—unlike contractually mandated secrecy. Moreover, despite the increasing prevalence of contractually mandated secrecy, not all businesses require it. *See supra* text accompanying notes 65–68.

free—or at least loosen businesses' hold on—these computing Oompa-Loompas.[121]

III
Freeing the Oompa-Loompas?

This Part makes the case that the technological changes in the computing industry discussed in the previous Part undesirably shift the balance that trade secret law strikes between incentives to innovate on the one hand and healthy competition and follow-on innovation on the other. As a consequence, it is due time to free these computing Oompa-Loompas, thus restoring a healthier balance for the good of innovation and competition. One path toward such freedom is to rethink trade secret law with regard to software, the data it uses, and the computing devices that contain them. Another option is to invoke other laws to intervene when trade secrecy protection extends too far, thereby undermining trade secrecy's goals. Finally, it is conceivable that industry conditions will shift yet again further down the road in ways that undermine the robust secrecy that the software industry has now built up, with the current concerns eventually resolving themselves.

Trade secrecy protection surely provides a business with an incentive to innovate if the business thinks it can keep the developed information or innovation secret.[122] The longer the business thinks the information or innovation can be kept secret, the stronger the incentive—and the more valuable trade secrecy protection—will be.[123] Put another way, the longer a business thinks the information or innovation it has developed will remain impenetrable due to low chances of independent discovery, reverse engineering, and transfer of an employee's general knowledge and skill to a competitor, the greater the incentive to innovate that trade secrecy protection provides. A business concluding that its secrets are robust not only gets a first-mover advantage but an extended long-term advantage, because the

---

[121] Much of the same might be said generally of processes (such as a chemical or manufacturing process), as they might share two characteristics of these industry trends: difficulty of independent discovery and reverse engineering. One might equally probe how well trade secret law balances incentives to innovation against follow-on innovation and competition in that sphere as well, but that topic is beyond this Article's scope.

[122] *See supra* Section I.B.

[123] *See* Abramowicz & Duffy, *supra* note 23, at 1622 (explaining how trade secrecy rights can theoretically provide more powerful incentives than patents because they are potentially infinite in duration).

business's secret, valuable information blocks—or at least delays—that much more follow-on innovation and competition.[124]

In a situation in which a business discerns such great value from keeping information or innovation secret, the business might have too strong of an incentive to develop that information or innovation and then maintain it as a trade secret. That is, it will likely have sufficient incentive to innovate in the first place and then prefer secrecy over patent, with its limited duration and requirement of disclosure.[125] Moreover, without any significant risks that the developed information or innovation will be disclosed through proper means—independent discovery, reverse engineering, or through transfer of an employee's general knowledge and skill—this form of protection is so strong that it is perpetual.[126] Generally, it is of great worry when protection for innovation is of unlimited duration.[127] In that case, protected creations can often be priced supra-competitively or be restricted in their availability, meaning that consumers who want

---

[124] A historical study finds that the first-mover advantage has generally shrunk over time, from an average of thirty-three years in the beginning of the twentieth century to an average of 3.4 years in the second half of the century. Rajshree Agarwal & Michael Gort, *First-Mover Advantage and the Speed of Competitive Entry, 1887–1986*, 44 J.L. & ECON. 161, 168 (2001). The study attributes this change in part due to greater transfer of knowledge and skills across firms. *See id.* at 164–65. To the extent that a business is able to block or delay this transfer, it thus bolsters its first-mover advantage. *See* David S. Levine & Ted Sichelman, *Why Do Startups Use Trade Secrets?*, 94 NOTRE DAME L. REV. 751, 757 (2018) ("Although startups can maintain a lead-time advantage simply because of the inherent failure of competitors to innovate, a primary reason for choosing trade secrecy is to extend a lead-time advantage by preventing the disclosure of specific information that provides the advantage."). The competitive advantage offered by robust secrecy similarly exacerbates business advantages that originate in network effects, as many data-collecting platforms such as Facebook and Google have. *See infra* note 139 and accompanying text. *See generally* Kenneth A. Bamberger & Orly Lobel, *Platform Market Power*, 32 BERKELEY TECH. L.J. 1051, 1051 (2017) (developing a "framework for considering the market power of platform companies that use digital technology to connect a multisided network of individual users").

[125] *See* Abramowicz & Duffy, *supra* note 23, at 1622.

[126] *See* Andrew A. Schwartz, *The Corporate Preference for Trade Secret*, 74 OHIO ST. L.J. 623, 630–31 (2013) ("[A] trade secret has no built-in expiration date. Rather, trade secret protection has a perpetual duration that lasts as long as the information remains secret. So, if the secret is kept and not honestly discovered by another, the holder's legal monopoly will persist forever."). In fact, the business might be even less likely to share the secret confidentially with others than under circumstances in which it fears a trade secret might be honestly acquired by others. *See* J. Jonas Anderson, *Secret Inventions*, 26 BERKELEY TECH. L.J. 917, 946 (2011) ("[G]iven the scope of trade secret protection, inventors who maintain inventions as trade secrets likely have more incentive to efficiently disclose their inventions to the proper individuals . . . . [T]rade secrecy encourages competition because the exclusivity of trade secrecy can end at any time.").

[127] *See supra* note 46.

access to these creations might not be able to get that access.[128] Moreover, perpetual protection can readily stymie follow-on innovation and competition.[129] When these conditions obtain, the incentive offered by intellectual property protection undermines the overall goals of innovation and competition that the law is trying to promote.[130] Because of the harm from perpetual protection, it has long been thought that trade secret law's safety valves of proper appropriation mean in practice that trade secrecy protection across an industry—particularly for innovation and innovation-related information—would generally not actually last forever.[131]

Given current computing trends,[132] however, trade secrecy protection may be overly attractive—perhaps because the protection is impenetrable—in relation to the harms protection can inflict on the goals of follow-on innovation and competition. Compare the concerns raised by the current attractiveness of robust trade secrecy protection for the software industry with the state of the industry in decades past. Over the past few decades—when trade secrecy protection was generally unattractive for the software industry[133]—the software industry innovated at a rapid pace, so much so that some questioned whether patent and copyright protection—even with their more limited duration of protection than trade secrecy—lasted too long.[134] Indeed, many attribute the rapid pace of innovation to all of those same things that tend to limit trade secrecy protection: reverse engineering, independent discovery, and knowledge transfer as employees rapidly switched between jobs in the industry.[135] This rapid pace of innovation generally was to society's benefit, by providing ever more software

---

128 *See* Christopher A. Cotropia & James Gibson, *The Upside of Intellectual Property's Downside*, 57 UCLA L. REV. 921, 929 n.22 (2010) (explaining that "as long as an intellectual property entitlement has a limited duration, its price will eventually descend to marginal cost, and the entire population of consumers can have access to it").

129 *See supra* Section I.B.

130 *See supra* Section I.B.

131 *See* Anderson, *supra* note 126, at 945–46 (explaining the theory that trade secret law encourages disclosure); Lemley, *supra* note 35, at 313 (positing that trade secret law encourages disclosure in certain ways).

132 *See supra* Part II.

133 *See supra* text accompanying notes 59–64.

134 *See, e.g.*, John R. Allison, Abe Dunn & Ronald J. Mann, *Software Patents, Incumbents, and Entry*, 85 TEX. L. REV. 1579, 1589–90 (2007); Carey R. Ramos & David S. Berlin, *Three Ways to Protect Computer Software*, 16 COMPUTER LAW. 16, 23 (1999); R. Anthony Reese, *A Map of the Frontiers of Copyright*, 85 TEX. L. REV. 1979, 1986–87 (2007).

135 *See* Colleen V. Chien, *Reforming Software Patents*, 50 HOUS. L. REV. 325, 364–68 (2012) (independent invention); Gilson, *supra* note 54, at 594–97 (job mobility); Peter S. Menell, *An Analysis of the Scope of Copyright Protection for Application Programs*, 41 STAN. L. REV. 1045, 1079 (1989) (reverse engineering).

options to consumers. And it meant that market entry into the software industry was relatively easy for new businesses.[136]

However, with secrecy becoming more robust for the software industry and with this shift making it so much more difficult, if not impossible, for independent discovery, reverse engineering, and knowledge transfer from departing employees, the landscape in the software and computing industry seems to be shifting. In recent years, this industry has seen increased resort to trade secrecy, as reflected in both legal scholarship[137] and media reports.[138] With these shifts, the industry might start experiencing a slower pace of innovation, offering fewer software choices for consumers, and enabling fewer competitors to enter the industry. As a corollary, there also might not be sufficient incentive for newcomers or competitors to innovate in the face of an initial mover's robust trade secret. The network effects that pervade this industry also make competition more difficult, and are likely in some part related to the computing trends I have described.[139]

This emerging "new normal" in the software and computing industry is worrisome because of its negative impact on follow-on innovation and competition, to the detriment of society. Can the law do anything to restore balance?

---

136 *See* Julie A. Mark, *Software Copying Policies: The Next Step in Piracy Prevention?*, 2 J.L. & TECH. 43, 48 (1987) (noting "the ease of entry into the software business"); John Soma, *Lessons from AT&T's Flop: How to Grow in the Technology Industry While Avoiding Section 7 Antitrust Obstacles*, 6 J. BUS. ENTREPRENEURSHIP & L. 195, 211 (2013) ("During its early years, the high demand for software and software innovation allowed for entry into the market of many different software producers, and thus industry consolidation was not an issue. Lastly, entry into the software market is arguably easier than entry into the mobile phone industry.").

137 *See, e.g.*, Timothy K. Armstrong, *Symbols, Systems, and Software as Intellectual Property: Time for CONTU, Part II?*, 24 MICH. TELECOMM. & TECH. L. REV. 131, 178 (2018); Levine & Sichelman, *supra* note 124, at 760 (explaining that perceived lack of patentability due to recent Supreme Court cases has driven many innovators away from patents and toward trade secrecy).

138 *See, e.g.*, Eric Rosenbaum, *A Tesla Self-Driving Blind Spot that Few Are Focusing On*, CNBC (Feb. 8, 2018, 9:12 AM), https://www.cnbc.com/2018/02/08/a-tesla-self-driving-blind-spot-that-few-are-focusing-on.html (reporting that Tesla has not secured any patents in recent years related to self-driving, with speculation that it might be resorting to trade secrecy instead); Daisuke Wakabayashi, *Secrets of Knowledge? Uber-Waymo Trial Tests Silicon Valley Culture*, N.Y. TIMES (Jan. 30, 2018), https://www.nytimes.com/2018/01/30/technology/waymo-uber-lawsuit.html (detailing a lawsuit in which Waymo is accusing Uber of misappropriating its trade secrets relating to driverless car technology).

139 For a sampling of writing on network effects in software markets and their effects on competition, see Ariel Katz, *A Network Effects Perspective on Software Piracy*, 55 U. TORONTO L.J. 155 (2005); Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CALIF. L. REV. 479 (1998); Suzanne Van Arsdale & Cody Venzke, Note, *Predatory Innovation in Software Markets*, 29 HARV. J.L. & TECH. 243 (2015).

Consider first the possible changes that might be made to trade secret law to promote vigorous follow-on innovation and competition. Removing the possibility of trade secrecy protection from this sector might have the most immediate intuitive appeal. However, it is worth dwelling on the consequence of doing so: While it might ultimately be worthwhile, it is likely not for the perhaps intuitive reason that it would render currently protected information freely and publicly available.

If information that might otherwise qualify as a trade secret is denied legal protection, the information holder could not enforce a misappropriation claim against a third party, no matter how egregious the third party's behavior of appropriation was.[140] Yet that in and of itself would not thereby make information freely available. That is, the absence of trade secrecy protection does not mean free and public availability. Instead, an absence of trade secrecy protection might temper a business's incentive to innovate because the business would not be able to take legal action to stop misappropriations of any secret information (unless these misappropriations remain prohibited under other laws). This inability to stop misappropriations makes the information less valuable, due to its greater vulnerability.[141]

There are thus three possibilities that might flow from denying trade secrecy protection to classes of information. First, the incentive to innovate that trade secrecy protection had once provided might be so reduced after protection is removed that the business never creates the information it would have otherwise produced had it been protected.[142] Without this information being created in the first instance, it is not clear society is better off. Second, the business might instead turn to other forms of intellectual property protection it views as sufficient to provide the incentive to innovate, such as patent protection. In that situation, society gets the benefit of the information and increased disclosure about it, as patent law requires.[143] Third, the business might not want to disclose its information, such as through patent law, but still might choose to innovate if there is sufficient business incentive to do so.[144] One such incentive might be the first-mover advantages generated by the business's information, which might exceed its costs of innovation.[145] A business might instead or also

---

[140] *See supra* Section I.A.

[141] *See supra* Section I.A.

[142] *See supra* Section I.B.

[143] *See supra* Section I.A.

[144] There is good reason to think that this possible consequence is likely, owing to first-mover advantages and network effects. *See supra* notes 124 and 139.

[145] *See supra* note 124 and accompanying text.

decide to expend more resources than it would have under a regime of trade secrecy protection to ensure that the information it has generated remains an actual secret that cannot be appropriated by others. Recall that trade secrecy protection is given to businesses for information when they have undertaken reasonable efforts to keep that information secret.[146] A key reason for that requirement is that a business would not have to undertake excessive (beyond reasonable) efforts to ensure its information remains secret. Instead, the law provides the business with legal protection if its efforts at secrecy are reasonable even if they did not actually work at maintaining the secret.[147] Without the possibility of trade secrecy protection as a fallback in case a secret is exposed, a business might invest greater resources to maintain information as an actual secret.[148]

It is not completely clear how to evaluate this hypothetical world without trade secrecy. Although the second possibility of choosing patent protection requiring disclosure would likely leave society better off than a world in which that invention is kept as a trade secret, it is less clear that the first option of no innovation in the first place or the third option of greater investments in actual secrecy would. In particular, consider the third option. Greater investments in secrecy would make it less likely that third parties could uncover the business's information, especially for a business engaged in cloud computing, using data and machine learning, or deploying automation, because the information is already robustly secret.[149] Moreover, the greater resources the business is spending on secrecy are redirected away from innovation, which might be wasteful.[150] That said, in the context of this Article, this waste might be socially beneficial. When greater spending on actual secrecy detracts from businesses' investments in innovation, that might help level the competitive playing field against newcomers or smaller players. Of course, leveling

146 *See supra* text accompanying note 17.

147 *See* E.I. DuPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1016–17 (5th Cir. 1970) (forbidding aerial photography of a manufacturing plant under construction as misappropriation of a trade secret, because "[t]o require DuPont to put a roof over the unfinished plant to guard its secret would impose an enormous expense to prevent nothing more than a school boy's trick"); Lemley, *supra* note 35, at 348–50 (discussing the requirement that trade secret owners take reasonable efforts to protect their secrets).

148 For a parody by Coca-Cola of how intensive efforts at actual protection of a secret might be, see cocacola86artgallery, *Secret Secrets of Coca-Cola's Hidden Formula Revealed*, YOUTUBE (Nov. 25, 2008), https://www.youtube.com/watch?v=MYgwcYX5mSM.

149 *See supra* Part II.

150 *See* Edmund W. Kitch, *The Law and Economics of Rights in Valuable Information*, 9 J. LEGAL STUD. 683, 697–98 (1980) (discussing the *DuPont* court's view on the prevention of wasteful expenditure).

the competitive playing field does not make it any easier to independently discover or reverse engineer a business's carefully guarded secrets; it merely removes some of the financial advantage the business might have over its competitors by redirecting its resources away from further innovation.

In sum, society might be well advised to remove trade secrecy protection for businesses operating in cloud computing, using data and machine learning, and deploying devices that automate human labor under certain conditions. We might want confidence that these businesses would instead choose patent protection—requiring disclosure—or "waste" resources on actual secrecy in a way that levels the competitive playing field.[151] Yet we should not remove trade secrecy protections from these businesses on the mistaken ground that the absence of trade secrecy protection would yield freely available information.

To get more freely available information, one might change or supplement trade secret law to require disclosure of source code, object code, input data to machine learning techniques, prediction models output from machine learning techniques, and the like under conditions in which too-strong protection is hindering follow-on innovation or competition.[152] To be sure, a disclosure requirement works only when one knows there is a secret in the first instance.[153] It also might be excessively harsh in undermining incentives to innovate in the first instance.[154] A middle ground might create a compulsory-licensing regime for otherwise secret information, in which innovators are compensated for generating this information, but they cannot keep it completely secret as against licensees.[155] In addition to needing to know that the business's secret information exists, a compulsory-licensing regime could work only if the license price could

---

[151] We also might be comfortable removing trade secrecy protection if the innovation that would not occur at all in the absence of this protection is less costly to society than the benefits to innovation and competition that might otherwise flow.

[152] Any such disclosure requirement might, however, make those concerned with data privacy anxious.

[153] *See* Michael P. Simpson, Note, *The Future of Innovation: Trade Secrets, Property Rights, and Protectionism—An Age-Old Tale*, 70 BROOK. L. REV. 1121, 1157 (2005) ("The most important element of the trade secret is secrecy. It is impossible to forcibly license something that you do not know exists.").

[154] *Cf.* Simon & Sichelman, *supra* note 43, at 382 ("[R]equiring disclosure of data might raise fewer . . . concerns, though the effect on innovation incentives and monitoring challenges make such solutions less than ideal.").

[155] *Cf.* Simpson, *supra* note 153, at 1156–57 (discussing compulsory licensing systems as a proposed solution to patent suppression problems and the difficulty of creating a mandatory licensing scheme for trade secrets).

be set appropriately, to reflect the tradeoff at stake between incentives to innovate and access by competitors.[156]

Another path to achieving similar effect within trade secret law is to change the meaning of its legal requirements as applied to the areas of the software and computing industry that have excessive secrecy. For example, perhaps it makes sense to narrow what counts as misappropriation (and correspondingly broaden what counts as proper means of appropriation) to allow for more ways to gain access to secrets that are too hard to reverse engineer, independently discover, or access as part of a departing employee's general knowledge and skill.[157] That is, it might be sensible to, say, tolerate certain third-party hacking of businesses' secrets.[158] A concern with this approach, though, is that it is hard to pin down just what these broadened proper means would be that would not also offend the commercial ethics—such as employees' duties to their employers and competitors' obligations not to trespass on another business's property to obtain secret information—trade secret law wants to promote.[159] Another possibility is to require more of businesses with data and computing secrets in terms of what they must do to undertake reasonable efforts to keep their information secret and thereby qualify for legal protection. Like the possibility of investing more in absolute secrecy in the absence of legal protection, this path would require businesses to spend more money on secrecy protection that might otherwise be spent on innovation.

While these proposals to change trade secret law have something to offer, they also have costs that might exceed their benefits. To the extent they do, another possibility is to maintain trade secret law as is and invoke other laws more actively to diminish trade secrecy's flaws for the software and computing industry. In particular, antitrust law might become more attentive to anticompetitive effects stemming

---

156 *Cf.* Jacob Victor, *Reconceptualizing Compulsory Copyright Licenses*, 72 STAN. L. REV. (forthcoming 2020) (exploring how compulsory licensing in copyright law ought to work to strike a similar balance between incentives and access).

157 *Cf.* Simpson, *supra* note 153, at 1157 (suggesting the creation of an affirmative defense to trade secret theft or misappropriation action if the defendant can make out the following three elements: "First, the defendant must prove the trade secret is extremely difficult to discover independently and reverse engineer; next, the defendant must show that the trade secret in question would perform a *valuable benefit to the health and wellbeing of society*; and finally, that the company was suppressing its discovery").

158 Tolerating certain forms of hacking might be seen as a form of civil disobedience that is socially beneficial. *Cf.* EDUARDO MOISÉS PEÑALVER & SONIA K. KATYAL, PROPERTY OUTLAWS: HOW SQUATTERS, PIRATES, AND PROTESTERS IMPROVE THE LAW OF OWNERSHIP (2010) (positing that civil disobedience with regard to intellectual property law can lead to improved laws).

159 *See supra* Section I.A.

from excessive secrecy and might consider anticompetitive misuse of secrecy to be an antitrust violation.[160] Additionally, it might be worth revisiting whether patent or copyright law—perhaps in a somewhat revised form—might be a better fit for the aspects of software and computing studied in this Article.[161] If so, it might divert some information out of secrecy and into patent or copyright protection, to the benefit of follow-on innovation and competition.

To the extent any changes are made within or atop trade secret law, it is critical that they be targeted with care only at the contemporary forms of information described in this Article that are now subject to excessive secrecy in the software and computing industry. Not only can there otherwise be unintended consequences with regard to other secret information, but it is quite possible that this situation will ultimately resolve itself in the marketplace. That is, the computing industry might change enough down the road in ways that diminish the current state of excessive secrecy that is harming follow-on innovation and competition. Such change already happened once earlier in the computing industry: Whereas the early computing industry relied heavily on trade secrecy for the software that was bundled with the hardware it sold,[162] it then principally deemphasized trade secrecy once it started selling software separately.[163] If the industry changes enough again so that excessive secrecy diminishes, trade secret law might no longer need drastic changes.

One development worth following in this context is the artificial intelligence development tools that Amazon, Google, and Microsoft have recently made available to the public via application program interfaces.[164] These application program interfaces allow third-party developers to use sophisticated vision, knowledge, language, and

---

[160] *Cf.* Jeanne C. Fromer, *The Unregulated Certification Mark(et)*, 69 STAN. L. REV. 121, 196–98 (2017) (suggesting that antitrust scrutiny can be used as a supplement to trademark law to police anticompetitive behavior with regard to certification marks beyond what trademark law already allows).

[161] *Cf.* Jeanne C. Fromer, *A Psychology of Intellectual Property*, 104 NW. U. L. REV. 1441, 1501–08 (2010) (suggesting that patent law is a better fit for computer source code than copyright law); Katyal, *supra* note 66 (reflecting on how software has never fit consistently or neatly into a form of intellectual property protection); Pamela Samuelson, *Strategies for Discerning the Boundaries of Copyright and Patent Protections*, 92 NOTRE DAME L. REV. 1493, 1495 (2017) (arguing for nuance in discerning the "proper boundaries of copyright and utility patent protection").

[162] *See supra* note 59.

[163] *See supra* text accompanying notes 59–64.

[164] *Artificial Intelligence on AWS*, AMAZON WEB SERVS., https://aws.amazon.com/machine-learning/ai-lex-polly-rekognition (last visited Apr. 5, 2019); *Cloud AI Products*, GOOGLE CLOUD, https://cloud.google.com/products/ai (last visited Apr. 5, 2019); *Cognitive Services*, MICROSOFT AZURE, https://azure.microsoft.com/en-us/services/cognitive-services (last visited Apr. 5, 2019).

speech software platforms built on the extensive data that these mega-companies have each collected to train these software platforms. In this way, there are a limited number of sources selling, or making available, the results of cloud-based software and data to competitors in an industry. There could be two important implications of this development. First, rather than one competitor keeping data or automation tools for itself, all competitors might gain access to important innovation tools, thereby leveling the playing field. Second, the limited number of sources providing such data or automation devices might have the ability to gather information from their various purchasers about possibilities for improvement or future uses as input to follow-on innovation that redounds to the benefit of all purchasing competitors. Such an outcome might blunt worries about excessive secrecy on one front by allowing easier entry into a competitive space and a level playing field.[165]

In sum, computing machines filled with software and fed with data have become today's Oompa-Loompas. They have become great secret-keepers due to industry developments: the growth of cloud computing, the elevation of data and growing use of machine learning, and automation. With these developments, trade secrecy protection has become excessive because the changes allow business to circumvent trade secret law's central limitations allowing independent discovery, reverse engineering, and use of a departing employee's general knowledge and skill. To fix the ensuing problem of excessive secrecy, the law will have to remain vigilant about increasing reliance on trade secrecy in the software and computing industry and consequent effects on follow-on innovation and competition. It ought to prepare to step in and modify or supplement trade secret law to free today's Oompa-Loompas for society's benefit.

---

[165] Yet by keeping secret their extensive data and ensuing software tools, the power given to companies like Amazon, Google, and Microsoft makes it harder for others to compete with them (let alone explore the robustness of their data and software tools).