Legitimizing Lies

Courtney M. Cox*

90 GEO. WASH. L. REV. (forthcoming 2022)

Lies are everywhere today. This scourge of misinformation raises difficult questions about how the law can and should respond to falsehoods. Legal discourse has traditionally focused on the law's choice between penalizing and tolerating lying. But this traditional framing vastly oversimplifies the law's actual and potential responses. Using trade secrets as a case study, this Article shows that the law sometimes accepts lies as a legitimate option for fulfilling legal requirements, and may even require lies in increasingly common circumstances.

Commonly supposed legal and moral commitments against lying do not undermine this reality. To the contrary, the Article reveals that the interplay between lying and the law is much more descriptively and normatively complex than the contemporary discourse generally acknowledges. And it provides support for the law remaining neutral with respect to the normative valence of lying at a time when the main argument favoring neutrality and against an anti-lying perspective—that the remedy for false speech is more speech—has been called into question.

Moreover, in legitimizing certain lies, the law takes lying seriously as a dual-use technology, one that can be put to good ends as well as bad. This raises important practical questions about how to lie, legally and morally, with implications in areas ranging from privacy to procedure to professional responsibility. Making this shift, from questions of justification—of when and whether lying is permitted—to questions of practicality, is increasingly urgent in the shadow of mass surveillance. This Article does not answer all questions raised by law's legitimation of lying, but by reframing the debate, it takes a critical step for clarifying the value of truth and the law's role in promoting it.

---

* Associate Professor of Law, Fordham Law School. D.Phil. in Philosophy, University of Oxford; J.D., University of Chicago Law School. For helpful comments and conversations, I thank Aditi Bagchi, Olivia Bailey, Pamela Bookman, Christopher Buccafusco, Michael Burstein, Anthony Casey, Bruce Cox, Nestor Davidson, Howard Erichson, Janet Freilich, Barbara Fried, Jeanne Fromer, Charles Tait Graves, Abner Greene, Daniel Hemel, Paul Hill, Lisa Larrimore Ouellette, Brian Leiter, Irina Manta, Jonathan Masur, Thomas Miles, Adam Mortara, Martha Nussbaum, Randall Picker, Alisa Philo, Jennifer Rothman, Bryson Santaguida, Sepehr Shahshahani, Stewart Sterk, Olivier Sylvain, Lior Strahilevitz, Murray Tipping, Maggie Wittlin, Felix Wu, Benjamin Zipursky, and any others I may have missed. I am grateful to audiences at the Harvard/Stanford/Yale Junior Faculty Forum, Intellectual Property Scholars Conference, NYU's Tri-State IP Workshop, GW Law IP Speaker Series, University of Chicago Law School, Fordham Law School, Cardozo Law School, Kelley School of Business, Baylor Law School, and LMU Loyola Law School. As always, I am greatly indebted to the Fordham Law Librarians, especially Kelly Leong. For excellent research assistance, I thank my full team of RAs, including Jocelyn Lee, Jordan Phelan, Juliann Petkov, M. Ryan Purdy, Amir Khedmati, and Edward Ernst; and especially Zach Huffman, Eleni Venetos, Benjamin Weissler, and Pamela White.

Legitimizing Lies

Courtney M. Cox

"Deception Is Security's Next Big Thing"
–HelpNet Security, Sept. 2020

INTRODUCTION

Lies are everywhere today. Their pervasiveness has amplified traditional debates about how the law can and should respond to lies. Within these debates, it is received, if contested, wisdom that the law and commonsense morality disfavor lying, with permissible lies forming an uneasily tolerated exception.[1] The doomscroll of lie-induced harms seems to reinforce this wisdom, underscoring the importance of ideals about truth.[2] But this largely unexamined reflex carries with it a danger: we risk blinding ourselves to the depth and breadth of the law's response to lying and the complexity of justice's commitment to truth.

Legal scholars have long focused on law either penalizing or permitting lies, but the law takes other approaches to deception as well. In this Article, I show that the law also accepts lies in express satisfaction of legal requirements and likely requires lying in increasingly common situations.[3] This phenomenon often passes without notice. Courts are discreet and may not call these acts lies.[4] But a lie by any other name is two. And in accepting these acts (and mislabeling them), the law legitimizes lies.

Using trade secrets as a case study, I show how law legitimizes lying. Trade secret law provides a remedy for theft of a company's confidential information—but only if a company has taken "reasonable precautions" to keep the information secret.[5] Enter the lie: decoys, mislabeled scripts, phishing simulations, honeypots, obfuscation, misinformation, the $1.5 billion industry in "deception technology," to name a few, are all deceptive precautions that straightforwardly satisfy this reasonable precaution requirement.[6] What is more, if deception is really the "next big thing" in information security—as

---

[1] *Infra* Part I.A; *see, e.g.*, Norman W. Spaulding, *The Artifice of Advocacy*, *in* LAW AND LIES: DECEPTION AND TRUTH-TELLING IN THE AMERICAN LEGAL SYSTEM 81, 96–106 (Austin Sarat ed., 2015) (describing the received wisdom).

[2] *See* 176 Cong. Rec. S14 (daily ed. Jan. 6, 2021) (statement of Sen. McConnell) ("Self-government, my colleagues, requires a shared commitment to the truth and a shared respect for the ground rules of our system."); *id.* at S21 (statement of Sen. Booker) ("The shame of this day is it is being aided and abetted by good Americans . . . who are surrendering to the passion of lies as opposed to standing up and speaking truth to power . . . ."); *id.* at S25–26 (daily ed. Jan. 6, 2021) (statement of Sen. Casey); *id.* (statement of Sen. Romney).

[3] *See infra* Part II.B.

[4] *See, e.g.*, SolarCity Corp. v. Pure Solar Co., No. 5:16-cv-01814, 2016 WL 11019989, at *1, , 9 (C.D. Cal. Dec. 27, 2016); *see infra* Part III.C.

[5] *See* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 180 (7th Cir. 1991); *see also* Defend Trade Secrets Act of 2016 (DTSA), 18 U.S.C. § 1836 *et seq*.

[6] *Infra* Part II.B.

trade publications and even the Wall Street Journal recently declared[7]—then trade secret law will increasingly require such precautions as "reasonable precautions."[8] Other areas of law similarly focused on avoiding harm, such as negligence, may follow.

All of these precautions are deceptive practices, and many undeniably involve lies.[9] They present falsehoods as true, in contexts where the audience is invited to rely on the representation made.[10] This fits squarely within current philosophical analyses of lying.[11] But these analyses have yet to gain recognition within the legal literature. Some scholarship—particularly commentary aimed at justifying stronger anti-lie prohibitions—focuses on a very narrow concept that excludes much of what the law counts as lies.[12] Other scholars include within the concept of a lie not merely the description of the action, but also the value judgment that lying is wrong—which then makes it very difficult to talk about what exactly is wrong (or not) with lying.[13] An important contribution of this Article is to bring recent philosophical work on lying to bear on the legal debate moving forward.[14]

In addition to denying that common deceptive precautions are lies, there are other ways of resisting my claim that trade secret law legitimizes lying, and exploring them proves fruitful. "Reasonable precautions" sets a floor, but not a ceiling, on the precautions that may be taken to protect a trade secret.[15] Equity, criminal law, torts, and other doctrines and substantive laws not considered may provide such limits and create legal risk. Such limits are not categorical, but they are complicated.[16] Far from undermining the analysis, such limitations raise further questions: If I am right, lawyers specializing in deceptive practices—deception specialists—will be needed,[17] raising

---

[7] Steve Preston, *MITRE Shield Shows Why Deception Is Security's Next Big Thing*, HelpNet Security (Sept. 30, 2020), https://www.helpnetsecurity.com/2020/09/30/mitre-shield-deception/; Heidi Mitchell, *In Battle Against Hackers, Companies Try to Deceive the Deceivers*, WALL ST. J. (Dec. 7, 2020), https://www.wsj.com/articles/in-battle-against-hackers-companies-try-to-deceive-the-deceivers-11607371200.

[8] *Infra* Part II.B.4.

[9] *Infra* Parts I.B, II.B.

[10] *Id.*

[11] *Infra* Part I.B.

[12] *Id.*

[13] *See e.g.*, Gregory Klass, *The Law of Deception: A Research Agenda*, 89 U. COLO. L. REV. 707 (2018).

[14] *E.g.,* JENNIFER MATHER SAUL, LYING, MISLEADING & WHAT IS SAID (2012); THOMAS L. CARSON, LYING AND DECEPTION: THEORY AND PRACTICE (2010).

[15] *See infra* Part II.C.

[16] *Id.*

[17] By "deception specialists," I do not mean cyberspecialists or technologists (though they will be needed too). I mean lawyers and academics who specialize in the law's treatment of lying. *Cf., e.g.*, Saul Levmore, *A Theory of Deception and then of Common Law Categories*, 85 TEX. L. REV. 1359 (2007); Saul Levmore, *Judging Deception*, 74 U. CHI. L. REV. 1779 (2007); Klass, *supra* note 13.

interesting tensions with the ethical rules that seem to preclude encouraging clients to lie.[18]

This is not a niche curiosity. Trade secret law protects key information assets: data and algorithms.[19] Meanwhile, digitization and remote work are eroding the effectiveness of facilities-based precautions, trends accelerated by the pandemic.[20] But corporate secrets are not the only thing at stake: that data includes *personal* data and those algorithms can be manipulated.[21] Trade secret decisions about "reasonable precautions" are harbingers of what is to come in other areas of the law, like negligence.

What are we to make, then, of the phenomenon of the law legitimizing lies? And particularly, what the phenomenon entails about the relationship between law and truth?

Some scholars and many practitioners believe that a corollary of the law's commitment to truth is a general disfavor or prohibition on lies and deception, since these are often thought to undermine truth.[22] This corollary is somewhat controversial[23] and perhaps unlawful,[24] but it (or at least its normative version) is experiencing a renaissance.[25] It comes down to defaults: Is the law's default setting to disfavor lies, and make exceptions by permitting certain ones? Or is the law generally neutral, despite its supposed commitment to truth, picking out certain lies and deceptions to police? Which is true as a descriptive matter, and which should be true as a normative one?

The trade secret case study presented here constitutes strong evidence that the neutral view provides the better descriptive picture, and that the neutral view may be *more* consistent with the commitment to truth than the anti-lie corollary. The case study also makes defending the corollary harder because ordinary morality cannot ground a legal objection to the law's legitimizing lies. The moral status of the lies at issue are contested (as a descriptive, not

---

[18] Daniel Markovits has begun upending common misconceptions about what these rules require. *See generally* DANIEL MARKOVITS, A MODERN LEGAL ETHICS (2008).

[19] *See infra* Part II.A.

[20] *See* Victoria A. Cundiff, *Reasonable Measures to Protect Trade Secrets in A Digital Environment*, 49 IDEA 359 (2009).

[21] *See* Courtney M. Cox, *Risky Standing: Deciding on Injury*, 8 NE. U. L.J. 75, 86 (2016) (discussing personal harms of data breach); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1355 (2018) (discussing the dangers of treating algorithmic trade secrets as privileged evidence in criminal proceedings).

[22] *Infra* Part III.A.

[23] *See e.g.*, Ariel Porat & Omri Yadlin, *A Welfarist Perspective on Lies*, 91 IND. L. J. 617, 624 (2016).

[24] *See* United States v. Alvarez, 567 U.S. 709, 718 (2012) (plurality) ("Absent from those few categories where the law allows content-based regulation of speech is any general exception to the First Amendment for false statement.").

[25] *See e.g.*, SEANA SHIFFRIN, SPEECH MATTERS: ON LYING, MORALITY, AND THE LAW (2014); JILL ELAINE HASDAY, INTIMATE LIES AND THE LAW (2019); Cathay Y.N. Smith, *Truth, Lies, and Copyright*, 20 Nev. L. J. 201, 227 (2019).

normative, matter), dooming any "Argument from Morality" that the law cannot work this way.

Challenging the Argument from Morality confirms the breadth of the claim—that law legitimizes lies—while providing a framework for further work. Trade secret law provides a natural starting point because a common exception to the rule against lying is for protective lies—lies that protect person or property by keeping a secret.[26] But interestingly, the exception for protective lies is not what defeats the Argument from Morality. And so my analysis's implications extend beyond trade secrets and protective lies, to areas ranging from privacy to procedure to professional responsibility, to name a few. Mapping this ethical terrain provides a framework for further work in these other areas of law.

These two strikes against the anti-lie corollary come at a time when rampant misinformation threatens the primary argument against the anti-lie corollary—that the best remedy for false speech is more speech.[27] But my case against the "Argument from Morality" is a descriptive one, about what ordinary morality holds and whether it can affect the law. We may still have normative concerns about whether, despite what ordinary morality suggests, the law *should* legitimize lying in this manner.[28] I do not minimize these concerns and I believe that those who do err.

But the law has a solution: it can lie. Unlike others, I entertain the possibility that the law's deception on this score is a feature, not a bug.[29] And so I do not believe that the ultimate question—whether law *should* legitimize lying—is the next or even most important question to ask.

The next questions instead concern *how* to lie as legally and ethically as possible, if possible. The case study illustrates that lying is not special. It is like other dual-use technologies—tools that can be used either responsibly or illicitly, for good ends or bad.[30] The important question for lying, as with all dual-use technologies, is how it is used, and whether such uses can be managed. Only then can we answer the ultimate question of whether and when the law *should* legitimize lies, and whether it should do so openly.

This Article thus represents a sharp break, on multiple dimensions, from trends in the growing body of literature on the law of lies and deception. That literature generally focuses on whether and how the law can (or should) penalize lying, or else permit it.[31] These questions have always been relevant

---

[26] *Infra* Part III.B.2.

[27] *See* Alvarez, 567 U.S. at 727 (Kennedy, J.) ("The remedy for speech that is false is speech that is true.").

[28] *Infra* Part III.C.

[29] *Id.*

[30] Herbert Lin, *Governance of Information Technology and Cyber Weapons*, *in* GOVERNANCE OF DUAL-USE TECHNOLOGIES: THEORY AND PRACTICE (Elisa D. Harris ed., 2016) (defining dual-use technology as "technology intended for beneficial purposes that can also be misused for harmful purposes").

[31] *See, e.g.*, Marc Jonathan Blitz, *Lies, Line Drawing, and (Deep) Fake News*, 71 OKLA. L. REV. 59 (2018); Cass R. Sunstein, *Falsehoods and the First Amendment*, 33 HARV. J.L. & TECH. 388, 390 (2020); SHIFFRIN, *supra* note 25; *see also* Part I.A.

in diverse areas from commercial law to procedural issues to criminal prosecution.[32] And these questions are of increasing importance and urgency as the problems of misinformation and fake news loom paramount.[33] But, as I argue here, there is another way to think about them, and it does not begin by assuming (or trying to justify the view) that lying is bad.

The Article proceeds as follows. Part I.A canvasses the literature's traditional framing of the law's response to lying, while Part I.B offers conceptual clarity about what a lie is, correcting common errors in the literature. Armed with this background, Part II turns to the Article's central case study, trade secrets. Part II shows how this increasingly important body of law accepts lies as a legitimate option for fulfilling its reasonable precaution requirement, and how it might require lying under increasingly common circumstances. Part III turns to various strategies for resisting this account, including the Argument from Morality and the objection that these are not really lies, among others. Finally, Part IV builds from the case study of Part II and analysis of Part III to explain the normative and ethical implications moving forward.

Developing a positive, pragmatic theory of lies and deception in the law is growing increasingly urgent. Recent events and the scourge of online misinformation demonstrate, palpably, lying's dangers and the difficulty of controlling deceptions.[34] Meanwhile, lying is fast becoming one of the best—and possibly only—ways to defend against cyber-threats[35] and to preserve autonomy in the shadow of mass surveillance.[36] This Article does not answer all of the questions these dilemmas raise, but it takes a critical step by showing the full breadth of what constitutes lying and exploring the breadth and depth of the law's response.

I. ON THE SUPPOSED PROHIBITION AGAINST LYING

There is much disagreement about lying, but most agree that lying is generally wrong even if most (regrettably) lie. The traditional legal debates over the relationship between the law and lying focus on the scope of that prohibition, and so on issues of punishment, tolerance, and justification.

There is also much disagreement about what lying is, though it often goes unstated. As a result, the legal literature has often missed developments in the philosophical literature that clarify the concept of lying in important ways.

To appreciate how the law's response to lying is both broader and deeper than typically assumed, we need to appreciate the focus of the existing debate about the law's response, and we need to get clear about what lying is—what

---

[32] *See infra* notes 46–60.

[33] *See* Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CAL. L. REV. 1753 (2019); Justin Hughes, *Gorgeous Photograph, Limited Copyright, in* ROUTLEDGE COMPANION TO COPYRIGHT AND CREATIVITY IN THE 21ST CENTURY (Bogre & Wolff, eds., forthcoming 2020).

[34] *Infra* Part III.A.

[35] *Infra* Part II.B.

[36] *Infra* Part IV.B.

actions, specifically, are we concerned with? In Part I.A, I describe the traditional debates. In Part I.B, I discuss the definition of lying and how it compares to deception.

A. The Law of Lying

There is general agreement within both ordinary and philosophical morality that lying is wrong, at least in a majority of central cases.[37] But there is much less agreement about why, and the circumstances where lying is permitted (if any).

Some situate the wrong of lying within a generally consequentialist (or utilitarian[38]) framework, focusing on the bad consequences that result.[39] These views are generally more permissive of lying, since the wrong of a lie is contingent on the harm that might result.[40]

Other theorists follow a nonconsequentialist approach, arguing, for example, that the wrong of a lie is that it is an affront to human autonomy, agency, or dignity.[41] These views are generally less permissive, though some define "lie" more narrowly so as to not count permissible lies as lies.[42] Immanuel Kant is probably the most famous for this approach, and many take his view to be that lying is wrong because it uses another person—and specifically, her reason—as mere means.[43]

Still others have attempted to reconcile these two approaches.[44] In addition, there is a sense in which all lying is necessarily an affront to the truth,

---

[37] *See* Spaulding, *supra* note 1, at 96–99. *See also* SHELLY KAGAN, NORMATIVE ETHICS 107 (2018).

[38] "Consequentialism" refers to moral theories that evaluate acts (or rules) based on the consequences. Consequentialism must be paired with a theory of the good—a theory about what consequences are good or bad. Within philosophical literature, "utilitarianism" refers to the combination of consequentialism with "welfarism," the view that an outcome's goodness depends solely on the well-being of individuals. The legal literature sometimes uses "utilitarianism" in the narrower, philosophical sense, but often uses the term interchangeably with "consequentialism," assuming them the same. *See* SHELLY KAGAN, NORMATIVE ETHICS 59–69 (2018).

[39] *E.g.*, HENRY SIDGWICK, THE METHODS OF ETHICS 485–92 (1981) (1907); JOHN STUART MILL, UTILITARIANISM 22-23 (2d ed. George Sher, ed. 1863); *see also* Alasdair MacIntyre, *Truthfulness, Lies, and Moral Philosophers: What Can We Learn from Mill and Kant?*, *in* THE TANNER LECTURES ON HUMAN VALUES 316 (1994) (describing competing traditions).

[40] *See, e.g.*, SIDGWICK, *supra* note 39, at 485–92.

[41] *E.g.*, Immanuel Kant, *On a Supposed Right to Lie from Philanthropy* (1797), *in* IMMANUEL KANT, PRACTICAL PHILOSOPHY 605 (Mary J. Gregor, trans. & ed., 1996); Christine M. Korsgaard, *The Right to Lie: Kant on Dealing with Evil*, 15 PHIL. & PUBLIC AFFAIRS 325, 325–27 (1986).

[42] *See* SISSELA BOK, LYING: MORAL CHOICE IN PUBLIC AND PRIVATE LIFE 14–15 (1999) (describing a narrow definition that excludes speaking "falsely to those with no right to your information").

[43] *See* Korsgaard, *supra* note 41.

[44] *See, e.g.*, MacIntyre, *supra* note 39.

because it breaks many of the linguistic rules that make conversation possible.[45] Common to all these accounts is a general anti-lying attitude, and any plausible account of lying will need to account for this discomfort with lying or else explain why such discomfort is misplaced.

Legal debates concerning lying generally fall into these same paradigms. Some, like Saul Levmore and Richard Posner, have advanced a cost-benefit view of the law's decision to penalize or permit lying, both as a general matter[46] and in specific contexts like contracts,[47] marketing,[48] and undercover reporting.[49] As with the philosophical debates, this broadly consequentialist approach is more permissive of lying than alternatives—and occasionally skeptical of a categorical prohibition. By contrast, others, like Aditi Bagchi, have offered nonconsequentialist accounts which draw narrow exceptions to the prohibition, often limited to cases where lying serves as a defense against wrongdoing or is justified by background injustice.[50] Still others walk the line between these approaches, seeking to articulate a more unified description of the varied moral norms animating the law's decision to penalize (or permit) lying and deception in given cases.[51]

More so than the philosophical debate, the legal debate tends to address specific contexts in which lying and deception occurs, rather than as a unified theory across different substantive areas.[52] This is perhaps not surprising, given the looming specter of the First Amendment and how its application

---

[45] *See id.* at 311–12 ("To assert is always and inescapably to assert as true . . . . [Some have] suggested that 'the utterance of a falsehood is really a breach of a semantic rule.'" (quoting Erik Stenius, *Mood and Language Games*, 17 SYNTHÈSE 269 (1967))).

[46] Levmore, *supra* note 17, at 1369 & n.41; *see also generally* Porat & Yadlin, *supra* note 23.

[47] Saul Levmore, *Securities and Secrets: Insider Trading and the Law of Contracts*, 68 VA. L. REV. 117, 137–42 (1982).

[48] David A. Hoffman, *The Best Puffery Article Ever*, 91 IOWA L. REV. 1395 (2006) (discussing marketing across areas of law).

[49] *See* Desnick v. Am. Broad. Cos., 44 F.3d 1345, 1351–52 (7th Cir. 1995); *see also* Levmore, *supra* note 17, at 1781–90.

[50] Aditi Bagchi, *Lying and Cheating, or Self-Help and Civil-Disobedience?*, 85 BROOK. L. REV. 355, 356 (2020).

[51] *See, e.g.*, STUART P. GREEN, LYING, CHEATING, AND STEALING: A MORAL THEORY OF WHITE-COLLAR CRIME (2006). Green describes himself as adopting a "primarily non-consequentialist, or deontological" approach to wrongfulness, *id.* at 39, but adopts harmfulness as a limiting principle for applying the moral norms governing lying and deception to criminal law. *Id.* at 44–45.

[52] *See generally, e.g.*, GREEN, *supra* note 51 (criminal law); Hoffman, *supra* note 48 (marketing); HASDAY, *supra* note 25 (family relationships); Anita L. Allen, *Lying to Protect Privacy*, 44 VILL. L. REV. 161 (1999) (sexual privacy); Irina D. Manta, *Tinder Lies*, 54 WAKE FOREST L. REV. 207 (2019) (sexual fraud); Mary Anne Franks, *Where the Law Lies*, *in* LAW AND LIES, *supra* note 1 (equal protection); Helen Norton, *Lies to Manipulate, Misappropriate, and Acquire Governmental Power*, *in* LAW AND LIES, *supra* note 1.

varies with context.[53] The most comprehensive treatment to date is that of Seana Shiffrin, who advances a "qualified [moral] absolutism about lying" in the nonconsequentialist tradition and argues for stronger legal regulation of lying than traditionally thought possible or prudent.[54]

Whatever the strengths or implications of these varying views, common to all of them is a generally prohibitive outlook that focuses on the line between lies that are prohibited (and so penalized) versus those that are permitted (and so not penalized). This is, perhaps, not surprising. The law is customarily viewed as embodying, or at least aspiring to, a commitment to truth.[55] Misrepresentations are barred by the rules of professional conduct and can provide the basis for civil liability;[56] criminal offenses involving fraud are the "most frequently charged" and "most widely and variously codified."[57] Even where the law might be said to "welcome[] deception," as with police interrogation tactics and other prosecutorial deception, it is often "not officially sanctioned" but condoned through "indifference"[58]—and perhaps uneasily so. And those lies that escape penalty are typically recast or reframed as something else, like "mere puffery."[59] In other words, permissive lies are generally treated as the exception rather than the rule, some as true exceptions (i.e., justified), some by definitional exclusion, and some escaping penalty because of the law's limitations (especially First Amendment limitations).[60]

Recent events suggest this seeming default is not without reason. Theranos, a startup with a purportedly "cutting-edge blood-testing system," catapulted to unicorn status (a startup valued at over $1 billion) by misrepresenting a key fact about its proprietary blood-testing technology—namely, that the technology did not exist.[61] Worse still, Theranos defended its deceptive practices by crying "trade secrets."[62] John Carreyrou's chronicle of Theranos's rise and fall reads like a case study of the numerous ways in which lies and deception cause harm:[63] There are the obvious direct and indirect harms from false beliefs in the reliability of Theranos' technology, not only to

---

[53] *E.g.*, Blitz, *supra* note 31; David A. Strauss, *Does the Constitution Mean What It Says?*, 129 HARV. L. REV. 2, 31–34 (2015).

[54] SHIFFRIN, *supra* note 25, at 2–4, 116–56, 182–223. Gregory Klass is also undertaking a project on the law of deception. *See* Klass, *supra* note 13

[55] *See* Porat & Yadlin, *supra* note 23, at 624 ("The concern over diluting the truth signal is a key factor in the almost general prohibition of lying, as well as its exceptions, under prevailing law.").

[56] *But see* MARKOVITS, *supra* note 18.

[57] GREEN, *supra* note 51, at 148–60.

[58] Julia Simon-Kerr, *Systemic Lying*, 56 WM. & MARY L. REV. 2175, 2181–82 (2015).

[59] *See* Hoffman, *supra* note 48, at 1396.

[60] *See* Porat & Yadlin, *supra* note 23, at 622; *see also* United States v. Alvarez, 567 U.S. 709, 720 (2012) (plurality) (Kennedy, J.).

[61] *See* JOHN CARREYROU, BAD BLOOD: SECRETS AND LIES IN A SILICON VALLEY STARTUP 1, 4, 178-181 (2018).

[62] *Id.* at 284.

[63] *See infra* Part III.

investors and business partners, but also (more devastatingly) to patients.[64] There is the blatant use of others as mere means. And there is the undermining of trust among employees. Carreyrou even suggests that the Theranos scandal arose from a culture that rewarded deceptions: though taken to extremes, Theranos followed Silicon Valley's "vaporware" playbook—the practice of securing investments for "already" developed software and hardware innovations that would "take years to materialize, if . . . at all."[65]

When one adds the pervasive and detrimental effects of fake news and misinformation on social media, from politicians, and within the news itself—and the new dangers presented by sophisticated deep fake technologies that enable every ill from involuntary porn to sophisticated forgeries—it is easy to fear the sky is falling.[66] Not surprisingly, much recent work argues for stronger prohibitions on lying.[67]

But all this attention to the line between penalizing and permitting, between wrong lies and exceptions, overlooks the breadth and depth of the law's potential responses. We will return to that question in Part II after getting some conceptual clarity about what a lie is.

B. What Is a Lie?

To see that law can legitimize lies, we first need to get clear about what lying is—what actions, specifically, are we concerned with? Although most everyone has a *general* understanding of what a lie is, philosophical and now legal consensus has been notoriously elusive about which actions, specifically, are included.[68] And as is probably obvious, which practices "count" will affect our understanding of the law's relationship to lies.

Some analyses limit the concept of "lies" or "misrepresentations" to intentionally false statements or assertions.[69] These analyses exclude omissions, merely misleading statements (i.e., true but misleading statements like half-truths), and conduct. There are various reasons for limiting the analysis in this way. For example, Jennifer Saul excludes omissions, merely misleading statements, and conduct because her project focuses on the lying-

---

[64] *See* CARREYROU, *supra* note 61, at 283–85; *see also, e.g.*, Michael Segal, *Does Theranos Mark the Peak of the Silicon Valley Bubble? John Carreyrou talks to Nautilus about the Lessons of a $1 Billion Fraud*, Nautilus (May 31, 2018), http://nautil.us/issue/60/searches/does-theranos-mark-the-peak-of-the-silicon-valley-bubble, https://perma.cc/JPN9-Z7DX. Former officers of Theranos, Elizabeth Holmes and Ramesh "Sunny" Balwani, have been charged with numerous counts of wire fraud, 18 U.S.C. § 1343, and conspiracy to commit wire fraud, 18 U.S.C. § 1349. *See generally* Third Superseding Indictment, United States v. Holmes, et al., No. 5:18-cr-00258-EJD (N.D. Cal. July 28, 2020), ECF No. 469. At the time of writing, the criminal proceedings remain ongoing as against both defendants.

[65] CARREYROU, *supra* note 61, at 296; *see also infra* Part III.C.

[66] *See* Chesney & Citron, *supra* note 33.

[67] *E.g.*, SHIFFRIN, *supra* note 25; Hoffman, *supra* note 48; HASDAY, *supra* note 25; Manta, *supra* note 52.

[68] *See, e.g.*, SAUL, *supra* note 14, at 1; KAGAN, *supra* note 38, at 113.

[69] *E.g.*, SAUL, *supra* note 14, at 1–20; SHIFFRIN, *supra* note 25, at 12 n.13.

misleading distinction in "what is said" and whether it matters morally.[70] And Shiffrin excludes conduct to avoid difficult questions about whether one may assert through conduct (as by making a face) and whether one may lie without making an assertion (as where sports players grimace as if in pain to get the opposing team penalized).[71]

By contrast, some theorists and practitioners adopt a broader view. For example, some expand the definition of lying to include omissions and statements that mislead (even if not strictly false). This is the approach taken by BLACK'S in defining the related term "misrepresentation":

> *Misrepresentation*. "[t]he act or an instance of making a false or misleading assertion about something, usu[ally] with the intent to deceive," including "not just written or spoken words but also any other conduct that amounts to a false assertion"[72]

These broader views have the advantage of capturing relevant conduct that those debating the regulation of lies care about. For example, consider President Clinton's infamous denial of his affair with Monica Lewinsky, stating "[t]here *is* no improper relationship" (omitting the qualifier "at present");[73] trademark law, which creates liability for the misleading use of marks and product appearance (trade dress);[74] and sumptuary laws, which once penalized people who "silently, but directly, l[ied]" about their class by "'dress[ing] above their station.'"[75] The broader view counts this behavior. Unfortunately, it does so by collapsing what many believe to be important distinctions between "direct lies" and "merely misleading."[76]

This Article carves something of a middle path and focuses on what I call "deceptive practices." Deceptive practices present or imply falsehoods. Unlike the limited view of "lies," deceptive practices include misleading assertions, omissions, and conduct. This focus is consistent with the broader view of "misrepresentation" generally taken by the law.[77] I will use the term

---

[70] *See* SAUL, *supra* note 14, at 1.

[71] *See* SHIFFRIN, *supra* note 25, at 12 n.13.

[72] *Misrepresentation*, BLACK'S LAW DICTIONARY (2019).

[73] SAUL, *supra* note 14, at vii.

[74] *See* Lanham Act, 15 U.S.C. §§ 1114, 1125(a); *see also* A&H Sportswear, Inc. v. Victoria's Secret Stores, Inc., 237 F.3d 198 (3d Cir. 2000).

[75] DAN ARIELY, THE (HONEST) TRUTH ABOUT DISHONESTY: HOW WE LIE TO EVERYONE—ESPECIALLY OURSELVES 120–21 (2013), *called into doubt on other grounds as described in, e.g.*, Tom Bartlett, *A Dishonest Study on Dishonesty Puts Prominent Researcher on the Hot Seat*, 68(2) CHRONICLE OF HIGHER EDUCATION (Sept. 17, 2021); *see also* Peter Goodrich, *Signs Taken for Wonders: Community, Identity, and a History of Sumptuary Law*, 23 LAW & SOC. INQUIRY 707, 717–19 (1998). In addition to penalizing such misrepresentations, sumptuary laws also sought to impose moral order of various sorts, from penalizing idolatry and excessive consumption to "institut[ing] an 'imagined social order'" that grounded such misrepresentations. Goodrich, *supra*, at 713–15, 722; *see also generally* ALAN HUNT, GOVERNANCE OF THE CONSUMING PASSIONS: A HISTORY OF SUMPTUARY LAW (1996).

[76] SAUL, *supra* note 14, at vii; *infra* Part III.B.5.

[77] *Misrepresentation*, BLACK'S LAW DICTIONARY (2019).

"affirmative misrepresentation" to refer to the narrow category of intentionally false statements or assertions. I will use "lie" in a more colloquial sense, where its meaning is clear and unlikely to cause confusion, for ease of exposition. Using these terms (1) sidesteps the debate about whether the broader category are also "lies" in a meaningful sense, (2) avoids confusion with the narrower understanding, and (3) allows us to make the distinction between lies and mere misleading that a broader definition of lies would otherwise collapse. In what follows, I describe these concepts in greater detail, and distinguish them from the related concept of deception.

1. Deceptive Practices, Deception, and Lies

The distinguishing feature of deceptive practices is how they operate: deceptive practices (or at least those with which we are concerned) present or imply falsehoods. "Falsehood" here has its standard meaning, of an untrue statement or proposition.[78] This broad definition of "deceptive practices" is consistent with the conduct described by *Black's* definition of "misrepresentation."[79]

A deceptive practice *deceives*—that is, the *deception* is "successful"—where it causes the target of that practice to have a false belief.[80] Lies present a clear example of deceptive practices: When Dave lies to Gina, he says something false but pretends that it is true. When Gina comes to believe what Dave says is true—when Gina comes to have a false belief—the deception succeeds.

Not all deceptive practices aim at deception, just as not all lies are intended to impart a false belief. A witness may lie on the stand to avoid repercussions from the mob boss; he might not intend to deceive, and may even hope that he does not.[81]

The deceptive practices to which we will turn in Part II all aim at preventing the target of the deceptive practice from learning the content of a trade secret.[82] That is, these practices seek to *deny* the target a true belief in the content of the trade secret. This means that there is an important distinction between a successful *deception*, just discussed, and a successful *deceptive practice*. A deception is successful when it causes the target to *believe* the intended falsehood. By contrast, a deceptive practice is successful when it achieves its goal of *denying* the relevant true belief. For example, information dumps—the "deliberate[] mixing [of] critical documents with masses of other documents to hide their existence or obscure their significance"—are a deceptive practice

---

[78] *Falsehood*, MERRIAM-WEBSTER (2020).

[79] *Misrepresentation*, BLACK'S LAW DICTIONARY (2019)

[80] *See, e.g.*, CARSON, *supra* note 14, at 46; SIDGWICK, *supra* note 39, at 317; *see also* SAUL, *supra* note 14, at 75–76. *See also infra* note 82.

[81] *See* CARSON, *supra* note 14, at 20.

[82] Many definitional accounts of "deception" include a success requirement, that a "deception" must successfully lead its target to believe a falsehood. *See, e.g.*, CARSON, *supra* note 14, at 3; SAUL, *supra* note 14, at 71. By contrast, common definitions of "lying" do not include a success requirement. "My dog ate my homework" is a lie, even if not believed.

whose success does not depend on the success of the deception.[83] Of course, the most interesting deceptive practices will be deceptive practices that make use of a successful deception, but, strictly speaking, a successful deception is not necessary for the deceptive practice to achieve its goal.[84]

Different deceptive practices have different types of "targets" (or audiences). The most common have direct intentional targets, as with the example of a lie told to a particular person. But there may be both direct and indirect intentional targets, as where a lie is told to Gina in the hopes that she will report it to Kei. And there may be collateral targets—targets who are not intended, but hear the lie anyways, as where a lie aimed at one person is broadcast to many listeners. There may also be unknown targets, as in the case of a mislabeled door, aimed at those who are looking for what is hidden behind the door (whoever those people turn out to be). Many deceptive precautions have multiple types of targets: the mislabeled door may have both known and unknown intentional targets (those who seek what is hidden) as well as known and unknown collateral targets (anyone else who passes by).

Finally, the concept of deceptive practices, as used here, does not include a moral (or legal) judgment about whether the practice is *wrong* or *improper*. Good philosophical practice usually requires identifying a practice before analyzing the question of whether all or only some instances of that practice (if any) are wrong or improper. This differs from the approach sometimes adopted in the legal literature, which then as a result struggles to articulate the distinction between lies that are *wrong* and those that might be permissible.[85]

2. A Word on Warranting and Other Requirements

Our definition roughly tracks contemporary analyses of lying, which have corrected various mistakes in traditional definitions.[86] Most of the standard definitions of lying, traditional and contemporary, include at least three requirements:

> (1) the liar states that P;
>
> (2) the liar believes P is false or is probably false; and
>
> (3) the liar takes themselves to be in a "warranting context"—a context in which the liar presents P as true (as opposed to, e.g., the theatre).[87]

---

[83] *See In re Sulfuric Acid Antitrust Litig.*, 231 F.R.D. 351, 363 (N.D. Ill. 2005) (noting procedural rules were amended to curb this practice). Information dumps succeed where the target does not form a true belief as to which document is critical, and do not depend on the target forming a false belief that a particular document is not critical.

[84] A successful deception is also not necessary for a deceptive practice to be morally wrong. *See* CARSON, *supra* note 14, at 21.

[85] *E.g.*, Klass, *supra* note 13, at 711, 731–36 (focusing on "deception," defined as "an act or omission that *wrongfully* causes a false belief in another" (emphasis added)).

[86] *See generally, e.g.*, SAUL, *supra* note 14; CARSON, *supra* note 14.

[87] *E.g.*, SAUL, *supra* note 14, at 3 (defining "lying" as "If the speaker is not the victim of linguistic error/malapropism or using metaphor, hyperbole, or irony, then

Our definition of "deceptive practices," as discussed *supra*, expands (1) to include not just statements, but other non-statement means of communicating P, like conduct. Our definition also takes as implicit (2), that the purveyor of the deceptive practice believes P is false or is probably false, to avoid complications about whose beliefs count for this purpose (when it is, e.g., a company undertaking the deceptive practice). Instead, our definition requires that P actually be false. In this way, our definition is perhaps overinclusive—for example, our definition includes "bullshit," where the speaker does not know or care whether P is true or false.[88] But in other ways, our definition might be underinclusive, as there are good reasons to think that a person lies even if they are mistaken about whether P is false.[89] The over-inclusiveness is consistent with the broader focus taken by the article—bullshit is certainly a *type* of deceptive practice even if it is not, strictly speaking, a lie.[90] The under-inclusiveness is also fine for our purposes: the main examples with which we are concerned include at least one falsehood.

The warranting requirement (3) merits further consideration. Our definition uses the phrase "presents." This is roughly correct, but it does not clearly exclude creative expression not normally counted as "lies" (e.g., theatre). Most philosophical analyses seek to exclude such fictional or figurative devices, and do so either by express exclusion[91] or through a warranting requirement.[92] For example, philosopher Thomas Carson describes "warranting" as an "invitation" to rely upon what is said—which actors arguably do not.[93]

I use the weaker "presents," for two reasons. First, something like theatre could be used as a deceptive precaution, and so it is appropriate for our purposes that it be counted or at least, ambiguously included. And second, although Carson emphasizes that the invitation is not a promise and need not be sincerely offered, it would be easy to confuse an invitation to rely with inducing reliance. But reliance is not part of the standard analytic definition of lying—a student lies when he says the dog ate his homework, even though he is not believed—even if reliance is an important element of certain lying-related legal causes of action (e.g., common-law deceit)[94] and even if reliance is central to one of lying's main harms.[95] To avoid this confusion, I offer the

---

they lie iff (1) they say that P; (2) they believe P to be false; (3) they take themself to be in a warranting context."); *see also, e.g.*, CARSON, *supra* note 14, at 30, 39; Andreas Stokke, *Lying and Asserting*, 110 J. PHIL. 33, 46–54 (2013).

[88] *See generally* HARRY FRANKFURT, ON BULLSHIT (2005).

[89] *See* SAUL, *supra* note 14, at 6.

[90] FRANKFURT, *supra* note 88; *see also* Lawrence M. Solan, *Lies, Deceit, and Bullshit*, 56 DUQ. L. REV. 73 (2018); David A. Graham, *What Trump Did in Osaka Was Worse Than Lying*, THE ATLANTIC (July 1, 2019) https://www.theatlantic.com/ideas/archive/2019/07/on-trumps-bullshit/593062/.

[91] *E.g.*, SAUL, *supra* note 14.

[92] *E.g.*, CARSON, *supra* note 14; Stokke, *supra* note 87, at 55.

[93] CARSON, supra note 14, at 3.

[94] *See* John C.P. Goldberg, Anthony J. Sebok & Benjamin C. Zipursky, *The Place of Reliance in Fraud*, 48 Ariz. L. Rev. 1001, 1004 (2006).

[95] *See, e.g.*, *id.* at 1011.

weaker "presents," with the consequence that my definition does not clearly rule out certain kinds of figurative speech.

The warranting requirement is really a modification of the intent requirement once believed "essential" to the definition of lying.[96] The intent requirement was usually conceived of as an intent to deceive, i.e., to impart a false belief to the listener.[97] Recent philosophical scholarship has shown the intent requirement is unnecessary as a conceptual matter,[98] though it may have moral significance.[99] But while intent to deceive may matter morally, that is a question of the line between permissible and impermissible lies, and not of the line between lies and not-lies.

3. A Right to Know

Finally, some theorists add the requirement that the target has the right to know P (or the truth value of P, or what P is meant to hide).[100] That is, these theorists maintain that, in addition to the three requirements identified above, a misrepresentation as to P is a lie if and only if the lie's target *has a right* to know P. By contrast, our definition does *not* include a requirement that the target has the right to know P (or the truth value of P, or what P is meant to hide). The Right-to-Know definitions are thus narrower than ours, because they exclude some practices that ours would capture.

Theorists who use the narrower definitions often advocate stringent—even absolute—prohibitions on lying.[101] A narrow definition makes this easier by excluding what others would call permissive lies. Rather than say such lies are permitted, the narrower definition denies that they are lies. But this begs the question, especially in our case where our focus is on lies that aim to protect information that others arguably do not have the right to know.

---

[96] *E.g.*, FRANKFURT, *supra* note 88, at 8; Arnold Isenberg, *Deontology and the Ethics of Lying*, *in* SELECTED ESSAYS OF ARNOLD ISENBERG 245, 249 (1973).

[97] Stokke, *supra* note 87, at 33.

[98] *Id.* (discussing literature). It is not entirely clear whether Shiffrin means to adopt this requirement. In place of (3), Shiffrin uses: "A intentionally presents P in a manner or context that objectively manifests A's intention that B is to take and treat P as an accurate representation of A's belief." SHIFFRIN, *supra* note 25, at 12. This suggests that "A[] intend[s] that B is to take and treat P as an accurate representation of A's belief," but that is exactly the sort of intent that Carson and others have shown to be unnecessary. *Id.*; Stokke, *supra* note 87, at 33.

[99] For example, intent to deceive has moral significance on deontological accounts that situate the wrong of a lie in the use of others as mere means. Shiffrin's account is somewhat confusing on this score: she does not situate the wrong of the lie in deception, believing these to be distinct wrongs, and so it would not seem necessary to her argument that lies require intent. Her later work appears to relax this requirement. *Cf.* Seana Shiffrin, *Learning about Deception from Lawyers*, 93 ARISTOTELIAN SOC. SUPP. 69 (2019) (arguing morally significant deception includes certain unintentional deceptions).

[100] *See* James Edwin Mahon, *The Definition of Lying and Deception, in* THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Edward N. Zalta ed., 2015), https://plato.stanford.edu/entries/lying-definition/.

[101] *See* CARSON, *supra* note 14, at 18–19.

II. HOW LAW LEGITIMIZES LIES: A CASE STUDY

With a clearer understanding of the nature of lies, we can turn to the relationship between deceptive practices and the law. Both law and commonsense morality have been characterized as exhibiting a general disfavor towards lying, with permissible lies forming the exception.[102] It is not surprising, then, that the literature has focused on the extent to which the law should penalize lying, and where the law might tolerate lying (by not penalizing it), whether for reasons of administrability, the First Amendment, or because such lies are not worthy of punishment.[103] Some have already argued or observed that, by declining to punish or tolerating lying, the law might incentivize lying.[104] But even this view simplifies the law's response to permitted lies.

The law goes further still. The law does not merely permit or penalize lies. The law also legitimizes lies: The law treats lies as a legitimate option for satisfying legal requirements and, in some cases, as the only option for satisfying those requirements.[105] While the literature focuses on the line between the first two responses, permit or penalize, this Article now turns to circumstances where law legitimates lying.

A natural starting point to understand the breadth of law's relationship with lying, and the depth of its permission, is with the law governing secrets: the law of trade secrets. As explained in Part II.A, trade secret law provides a remedy for misappropriation of confidential information, but only if a company took "reasonable precautions" to keep the information secret ("reasonable precaution requirement" or "RPR").

Part II.B shows how deceptive precautions straightforwardly satisfy this legal requirement. The use of such precautions has a long history and an even brighter future with the rapidly expanding market for "deception technology."[106] Litigants have begun relying on these precautions to satisfy the RPR, and courts have recognized the value of such precautions.[107] As these precautions become best practices, the law might even treat them as mandatory for securing legal relief—that is, the law might require lying.[108]

This is not to say that this legitimation lacks limits. As Part II.C explains, the RPR creates a floor, but not a ceiling. A tangled web of other substantive areas of law open a company to risk of sanctions or liability for harms caused

---

[102] The exception may swallow the rule. *E.g.*, Manta, *supra* note 52; *see also generally* United States v. Alvarez, 567 U.S. 709 (2012).

[103] *Supra* Part I.

[104] *See* Simon-Kerr, *supra* note 58, at 2181; *see also* Levmore, supra note 17, at 1780–81.

[105] The law also protects—as property—some lies. Courtney M. Cox, *The Power of Non-Words: Protecting Deception as Intellectual Property*, AALS Annual Meeting, Session on Intellectual Property and Culture cosponsored by the Section on Intellectual Property, the Section on Art Law, and the Section on Law and the Humanities (Jan. 7, 2021).

[106] *Infra* Part II.B.1–2.

[107] *Infra* Part II.B.3.

[108] *Infra* Part II.B.4.

by deception. But these limits are not categorical, and so do not undermine the fact that the law legitimizes lies.

At the outset, I emphasize that my claim is limited. I do not argue that *all* deceptive precautions satisfy the reasonable precaution requirement, but rather that a significant set of deceptive precautions could. Even so, as I explain in Part II.D, this limited conclusion is itself remarkable: what the trade secret case study reveals is not merely an instance of the law *condoning* or *tolerating* lying, but affirmatively and expressly treating lying as a legitimate option by providing legal relief *in virtue of* having taken such measures.[109]

A. Trade Secrets and the Reasonable Precaution Requirement

Trade secret law protects commercial secrets—like the recipe for Coca-Cola or Google's search algorithm—against misappropriation. As explained in Part II.A.1, trade secret law protects a broad range of commercially valuable information and is of increasing importance in the information economy.[110] Because it protects informational assets, but only against misappropriation (e.g., procurement by fraud), there are two dominant views of trade secret law: as intellectual property, and as the codification of commercial ethics.

But as explained in Part II.A.2, whichever view is correct, trade secret law only helps those who help themselves by keeping their confidential information secret. This requirement, known as the "reasonable precaution requirement" (RPR), provides the hook for our case study. It is common across all sources of trade secret law—state common law, the Uniform Trade Secrets Act (UTSA), and federal statutes.[111]

---

[109] *Cf.* Levmore, *supra* note 17, at 1362–74 (building theory of tolerated deception).

[110] *See* Deepa Varadarajan, *Trade Secret Precautions, Possession, and Notice*, 68 HASTINGS L.J. 357 (2017); Elizabeth A. Rowe, *Rats, Traps, and Trade Secrets*, 57 B.C. L. REV. 381, 381–82 (2016); David S. Almeling, *Seven Reasons Why Trade Secrets Are Increasingly Important*, 27 BERKELEY TECH. L.J. 1091, 1104–06 (2012).

[111] UTSA § 1(4)(ii); 18 U.S.C. § 1839(3)(A) (2018); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40(4) (1995); *see also* RESTATEMENT (FIRST) OF TORTS § 757, cmt. b (1939). Trade secret law developed as a common law doctrine until the late twentieth century, when states began adopting the UTSA. *See* Sharon K. Sandeen, *The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act*, 33 HAMLINE L. REV. 493, 498–502 (2010). Every state except New York has adopted it. Camilla A. Hrdy & Mark A. Lemley, *Abandoning Trade Secrets*, 73 STAN. L. REV. 1, 24 (2021). Congress created federal criminal liability for trade secret misappropriation with the Economic Espionage Act of 1996 ("EEA"), and recently created a federal civil cause of action in 2016's Defend Trade Secrets Act ("DTSA"). Economic Espionage Act ("EEA"), 18 U.S.C. § 1839(3), *amended by* Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 380 (2016). The RPR is generally interpreted consistently across both UTSA and non-UTSA jurisdictions. *See* Elizabeth A. Rowe, *Contributory Negligence, Technology & Trade Secrets*, 20 GEO. MASON L. REV. 1, 9 (2009). The DTSA closely follows the UTSA, and scholars anticipate that the DTSA will be construed consistent with existing trade secret law. *See* 1 ROBERT MERGES, PETER S. MENELL & MARK A. LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE: PERSPECTIVES, TRADE SECRETS, AND PATENTS 43–44, 48 (2017).

1. Trade Secrets

A trade secret is "confidential information which is not disclosed in the normal process of exploitation."[112] Virtually anything can be protected as a trade secret, provided it can be kept secret: recipes, code, algorithms, cell lines, client lists, business methods, manufacturing processes, sales numbers, and market research.[113] Trade secrecy is also recursive: the very precautions that protect trade secrets can constitute trade secrets.[114] Coca-Cola's recipe and Google's search algorithm are famous examples, as are some of the measures for protecting them.

Although the *subject matter* of trade secrets is virtually limitless, the requirement of confidentiality—of secrecy—is paramount. Such secrecy need not be absolute.[115] But information is not a trade secret if it is generally known within the relevant industry,[116] or if a company failed to take reasonable precautions to preserve its secrecy.[117]

Trade secret law, unlike other forms of intellectual property, only protects against misappropriation. "Misappropriation" means unauthorized *disclosure* of the secret;[118] unauthorized *use* of the secret;[119] or improper *acquisition* of the secret in violation of accepted norms of commercial ethics and corporate diligence (whatever and however undertheorized those norms may be).[120] By way of example, improper acquisition includes not only procurement by fraud,[121] but also extreme forms of corporate diligence, like aerial photography.[122] Trade secrets are not protected against reverse-engineering or independent development (unlike patents). And trade secrets are not protected against mere copying (unlike copyrighted works).

Trade secret law has long occupied an uneasy position in the pantheon of intellectual property and unfair competition law. Trade secret law, like other

---

112 Aronson v. Quick Point Pencil Co., 440 U.S. 257, 266 (1979) (citing RESTATEMENT (FIRST) OF TORTS § 757, cmt. b (1939)). Some jurisdictions also require that the information provide commercial advantage. *See* Gale R. Peterson, *Trade Secrets in an Information Age*, 32 HOUS. L. REV. 385, 390-91 (1995); *see also* Eric E. Johnson, *Trade Secret Subject Matter*, 33 HAMLINE L. REV. 545, 556–58 (2010).

113 MICHAEL A. EPSTEIN, EPSTEIN ON INTELLECTUAL PROPERTY, at 1-18 (5th ed. 2006).

114 *See, e.g.*, CrowdStrike, Inc. v. NSS Labs. Inc., No. 17–146, 2017 WL 588713, at *1, *4 (D. Del. Feb. 13, 2017) (holding that "methods of threat detection" in plaintiff's cybersecurity software "qualify as trade secrets").

115 Electro-Craft Corp. v. Controlled Motion Inc., 332 N.W.2d 890, 901 (Minn. 1983).

116 Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475 (1974).

117 *See infra* Part II.A.2.

118 *See* Kewanee, 416 U.S. at 475–76.

119 *See id.*; *see also* Am. Can Co. v. Mansukhani, 728 F.2d 818, 820 (7th Cir. 1982).

120 *See, e.g.*, E.I. DuPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1017 (5th Cir. 1970).

121 *See e.g.*, Phillips v. Frey, 20 F.3d 623, 630 (5th Cir. 1994) (finding improper acquisition where defendants feigned interest in buying plaintiffs' business).

122 *E.g.*, E.I. DuPont, 431 F.2d at 1017 (holding aerial photography of construction site constituted misappropriation).

forms of intellectual property, protects an information asset. But, unlike other forms of intellectual property, trade secret law only protects that asset against misappropriation. Accordingly, there are two dominant theories of trade secret law: one which characterizes trade secrets as intellectual property, and one which theorizes trade secret law as a form of unfair competition, and specifically, as the codification of commercial ethics.[123]

However these competing views are reconciled (or not), trade secret law is an increasingly important part of modern commercial law for two reasons: subject matter coverage and improved enforcement options.

First, trade secret subject matter is well-suited to twenty-first century needs. In addition to providing a cheaper and longer-lasting alternative to patents,[124] trade secret protection is available for a broader range of commercially valuable information.[125] This expansive subject matter is critical in the information economy: algorithms, data, source code, and business methods are not reliably covered by patents or copyright, and recent Supreme Court precedent has further eroded what protection had been available.[126] By contrast, trade secret law lacks substantive limits on protectable subject matter, and so can protect these information assets.

Second, two shifts in dispute resolution have made trade secrets easier to enforce. The Defend Trade Secrets Act ("DTSA"), enacted in 2016, created a federal civil cause of action with powerful remedies, including *ex parte* seizure of materials containing secrets (like hard drives or laptops).[127] And courts increasingly enforce arbitration agreements under the Federal Arbitration Act, ensuring access to a confidential forum (if desired).[128] Unsurprisingly, trade secret litigation has "explod[ed]" in recent years.[129]

2. The Reasonable Precaution Requirement

Trade secret law does not help those who fail to help themselves: "[o]ne who possesses a trade secret and wishes to protect it must act to preserve its secrecy."[130] This element of a trade secret claim is known as the "reasonable

---

123 *See* Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CALIF. L. REV. 241, 251–60, 260 n.90 (1998).

124 *See, e.g.*, Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 180 (7th Cir. 1991) (noting lack of registration and expiration).

125 *See* R. Mark Halligan, *Trade Secrets v. Patents: The New Calculus*, 2 ABA LANDSLIDE 1, 11–13 (July/August 2010).

126 *See id.*

127 Defend Trade Secrets Act of 2016 (DTSA), Pub. L. 114-153, 130 Stat. 376 (May 11, 2016), codified 18 U.S.C. § 1836 *et seq.*

128 Not all secret owners prefer arbitration; some use negative publicity against their adversaries. DARIN W. SNYDER & DAVID S. ALMELING, TRADE SECRET LAW AND CORPORATE STRATEGY, § 7.06(6).

129 David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 301 (2009); Personal experience; *see also* Varadarajan, *supra* note 110, at 358–59.

130 USM Corp. v. Marson Fastener Corp., 393 N.E.2d 895, 899 (Mass. 1979) (collecting cases).

precautions requirement" (RPR).[131] Common precautions include physical and technological limits on access; notifying employees and collaborators of the need to protect confidential information; and imposing contractual limits on employment and disclosure.[132]

Although putative secrets will not receive protection if disclosed unconditionally,[133] the RPR does not require absolute security or secrecy.[134] And with good reason: trade secret law aims, in part, at reducing overinvestment in security while encouraging limited disclosure that benefits innovation (e.g., joint ventures).[135] All that is required for trade secret protection is that a company make *reasonable* efforts.[136]

Like most tests for "reasonableness," whether a particular set of precautions satisfies the RPR is a case-by-case factual inquiry that, except "in . . . extreme case[s]," cannot be determined as a matter of law.[137] The dominant approach, articulated by Judge Posner in *Rockwell Graphic Systems, Inc. v. DEV Industries, Inc.*,[138] is a cost-benefit approach: Whether a particular set of precautions is reasonable "depends on a balancing of costs and benefits that will vary from case to case."[139] Such costs include both the direct cost of guns, guards, and gates—security's "sticker price"—and indirect costs, like "[in]convenience, employee cooperation, [and] disruption."[140] These costs must then be evaluated in light of the protection actually afforded (some

---

131 *See* DTSA, 18 U.S.C. § 1839(3); Uniform Trade Secrets Act, 14 U.L.A. 433; RESTATEMENT (FIRST) OF TORTS § 757, cmt. b (1939); *see also* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995) (important factor). The requirement is also called the "reasonable secrecy precaution" requirement or "RSP requirement," Robert G. Bone, *Trade Secrecy, Innovation, and the Requirement of Reasonable Secrecy Precautions*, *in* THE LAW AND THEORY OF TRADE SECRECY PRECAUTIONS (Rochelle C. Dreyfuss & Katherine J. Standburg eds., 2010), and the "reasonable efforts requirement," Rowe, *supra* note 111, at 2.

132 *See, e.g.*, Rockwell, 925 F.2d at 180; *see also Trade Secret Protection*, CORPORATE COUNSEL'S GUIDE TO PROTECTING TRADE SECRETS § 2.

133 Peterson, *supra* note 112, at 432–33 & nn.387–88 ("[T]he surest way to lose a trade secret is to generally disclose it without an express or implied obligation of confidentiality.") (collecting cases).

134 *See* USM Corp. v. Marson Fastener Corp., 393 N.E.2d 895, 900 (Mass. 1979) (collecting cases); E.I. DuPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1017 (5th Cir. 1970).

135 *See* Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 333–34 (2008) ("[O]verinvestment in secrecy is a real problem in the absence of trade secret protection.").

136 *See* E.I. DuPont, 431 F.2d at 1017; *see also* Rockwell, 925 F.2d at 178; USM Corp., 393 N.E.2d at 901.

137 Rockwell, 925 F.2d at 179–80; *accord*, Niemi v. NHK Spring Co., 543 F.3d 294, 301 (6th Cir. 2008) (citing Learning Curve Toys, Inc. v. PlayWood Toys, Inc., 342 F.3d 714, 725 (7th Cir. 2003) (quoting Rockwell, 925 F.2d at 173)).

138 925 F.2d 174 (7th Cir. 1991).

139 *Id.* at 179–80.

140 GUIDE TO PROTECTING TRADE SECRETS at §2:12.

secrets are easier to keep) and the secret's value. In short, there is no "bright line test for determining when an owner has made reasonable effort."[141]

Because whether precautions are reasonable "depends on the circumstances of each case,"[142] courts rarely find that a *particular* precaution was *required* and instead look to the totality of precautions taken. But there are exceptions. Non-disclosure agreements have become almost mandatory.[143] Similarly, failure to take either industry-standard precautions or basic precautions that are necessary under the circumstances will generally prove fatal to a trade secret claim.[144]

The role of the RPR has recently been the subject of some disagreement,[145] but Judge Posner's decision in *Rockwell* canvasses the territory well: The RPR serves two main purposes: evidentiary and remedial.[146] First, the RPR provides (a) evidence that the defendant took the secret by improper means (i.e., it did not merely leak), and (b) evidence of the secret's value (as a function of security costs).[147] Second, the RPR has "remedial significance": firms that failed to protect their secrets do not gain windfalls "merely because the defendant took the secret from [them], rather than from the public domain as it could have done with impunity."[148] Thus, the more that is spent on protecting a secret, "the more [the secret's owner] demonstrates that the secret has real value deserving of legal protection, that he really was hurt as a result of the misappropriation of it, and that there really *was* misappropriation."[149] To this picture should be added the recent contribution of Deepa Varadarajan, who has argued that the RPR also serves a role similar to possession for real or chattel property: providing notice of what is claimed.[150]

Whatever the merits of the various theoretical views, the RPR remains black letter law, with the DTSA following the UTSA in adopting the RPR as an independent requirement.[151] The predominant mode of analysis (for now)

---

141 David R. Ganfield II, *Protecting Trade Secrets: A Cost-Benefit Approach*, 80 ILL. B. J. 604, 606 (1992).

142 USM Corp. v. Marson Fastener Corp., 393 N.E.2d 895, 902 (Mass. 1979).

143 *E.g.*, Weins v. Sporleder, 569 N.W.2d 16, 23 (S.D. 1997); *see also* Peterson, *supra* note 112, at 432–33 & nn.387–88 (collecting cases).

144 *E.g.*, Defiance Button Mach. Co. v. C & C Metal Prods. Corp., 759 F.2d 1053, 1063–64 (2d Cir. 1985) (passwords); *see also* Rowe, *supra* note 111, at 26–27 ("[A] reexamination of what are reasonable measures to protect information based on current business norms is not only logical but is consistent with trade secret law.").

145 *See, e.g.*, Lemley, *supra* note 135, at 348–50 (arguing RPR should be demoted from a separate requirement to an evidentiary issue concerning secrecy); Peterson, *supra* note 112, at 390 & n.31 (cautioning against overemphasizing secrecy as RPR's critical function is showing lack of abandonment).

146 *See* Rockwell, 925 F.2d at 178.

147 *Id,* at 178–79.

148 *Id.* at 179 ("It would be like punishing a person for stealing property that he believes is owned by another but that actually is abandoned property.").

149 *Id.* at 179–80 (emphasis in original).

150 *See* Varadarajan, *supra* note 110, at 378–83.

151 18 U.S.C. § 1839(3)(A); UTSA § 1(4)(ii).

remains a *Rockwell*-ian cost-benefit analysis.[152] And this self-help requirement may be even more justified in a digital age, where legal remedies alone may be insufficient to address misappropriation.[153]

B. When Lies Secure Trade Secrets

Trade secret law requires companies to protect their secrets to be eligible for legal relief.[154] One common way of protecting secrets in ordinary life is relatively inexpensive: lie. Verbal decoys, like outright lies and misleading half-truths, can obscure a secret and even conceal its existence.[155] Is the same true for companies that need to protect commercial secrets? And if so, could the law recognize such efforts as "reasonable"?

The answer is yes. Deceptive precautions have both a longstanding history within intellectual property (Part II.B.1) and are emerging as an essential component of cybersecurity best practices (Part II.B.2). These deceptive precautions—many of which involve lies—satisfy the standard doctrinal test for the RPR. And though few courts have expressly addressed the issue, early harbinger cases suggest that courts will follow this standard doctrinal analysis, at least where the deceptive precautions are used as actual precautions and not to troll (Part II.B.3). Moreover, there may be an increasing number of situations where a company that fails to undertake such precautions will fail to satisfy the RPR (Part II.B.4). In other words, the law might not only legitimize certain lies; the law might require them.

This is not to claim that all such precautions could satisfy the RPR. As I explain in Part II.C, there are limits on "reasonable" precautions—on the lengths to which a company can go to protect its secrets. In so doing, I identify a gap in the literature and trade secret law itself, which largely focuses on the behavior of trade secret *defendants*.[156] But as relevant here, these limits do not *categorically* exclude lies, and so do not undermine the easy doctrinal case that lies can satisfy the law. To the contrary, they suggest that deception specialists may be needed.

1. A Tradition of Deceptive Precautions

Given the tensions described in Part I, *supra*, deceptive precautions might seem unusual—at least outside companies, like Theranos, engaged in widespread fraud. Many practitioners have expressed surprise at my thesis, that a plaintiff's own misrepresentations could satisfy an element of her legal claim, let alone be required by it. Unsurprisingly, it is infrequently litigated—at least not under these terms.

---

[152] *See* Rowe, *supra* note 111, at 9.

[153] *See id.* at 3.

[154] Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 180 (7th Cir. 1991); *see also* 18 U.S.C. § 1836 *et seq*.

[155] *Cf.* KIM LANE SCHEPPELE, LEGAL SECRETS: EQUALITY AND EFFICIENCY IN THE COMMON LAW 22–23 (1988) ("[T]he purpose in not telling the truth is often the attempt to keep a secret.").

[156] Discussion of plaintiff's behavior generally addresses litigation misuse. *E.g.*, Elizabeth A. Rowe, *Trade Secret Litigation and Free Speech: Is It Time to Restrain the Plaintiffs?*, 50 B.C. L. Rev. 1425 (2009).

But there is actually a long and venerated history of using deception to protect industrial secrets and information assets that continues to present day.[157] The examples make for good stories, like the fake town in the map that became a real one.[158]

Some deceptive precautions are used to conceal. Companies, including law firms, commonly use code names for sensitive matters.[159] Some mislabel facilities' doors[160] or directories[161] or scripts.[162] Others mask computer IP addresses to hide geographic locations.[163] The "long-awaited casting" of the mother in the hit sitcom *How I Met Your Mother* was "kept secret from the show's incredibly rabid followers" by, among other things, labeling the audition script "USC Student Thesis Film" because it was "[s]omething no one in Hollywood would ever actually read."[164]

Some conceal directly: The telephone booth that provided a direct line between Churchill and Roosevelt during World War II was kept in a room labeled as a bathroom.[165] Others through misdirection: A former car engineer recounted that, during road tests, her design team constructed fake car parts so that corporate spies—literally, photographers in trees—would focus on the decoy and not the actual innovations while the car drove past.[166] Sometimes, as in the road-test case, the deceptive precaution functions by imparting a false

---

[157] I use the term "information asset," instead of intellectual property, since such cases often involve assets for which it is unclear whether the assets are entitled to protection under our intellectual property laws and so unclear whether the assets are properly identified as intellectual *property*. *See, e.g.*, Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., Inc., 499 U.S. 340 (1991).

[158] *E.g.*, Sarah Zhang, *The Fake Places that Only Exist to Catch Copycat Mapmakers*, GIZMODO (Apr. 3, 2015), https://gizmodo.com/the-fake-places-that-only-exist-to-catch-copycat-cartog-1695414770; *see also, e.g.*, Nester's Map & Guide Corp. v. Hagstrom Map. Co., 796 F. Supp. 729, 731–32 (E.D.N.Y. 1992).

[159] Personal experience. *See, e.g.*, George N. Saliba, *Technology and Law Firms: Is Your Attorney up to Speed?,* MAGAZINE N.J. BUS. & INDUS. ASS'N, (Jan. 2008), https://media.gibbonslaw.com/files/publication/fea6255c-5e8c-4f95-9660-36bfc637943c/presentation/publicationattachment/5aba1b5f-c6b9-4002-9988-3c1a41712e43/nj%20business%20-%20technology%20&%20law%20firms.log.pdf.

[160] *Infra* note 165 and accompanying text.

[161] *E.g.*, Comp. ¶¶ 24, 60, BidPrime, LLC v. SmartProcure, Inc., No.18-cv-478, 2018 WL 5274202 (W.D. Tex. July 17, 2018).

[162] *See* Tanner Stransky, *'HIMYM' Unveils the Mother! The Creators Answer Your Burning Questions*, INSIDE TV (EW May 13, 2013), http://insidetv.ew.com/2013/05/13/how-i-met-your-mother-cristin-milioti; Adrienne Tyler, *Infinity War Directors Explain Need for Fake Scripts & Scenes*, SCREENRANT (Apr. 17, 2018), https://screenrant.com/avengers-infinity-war-fake-scripts/.

[163] Charles Tait Graves, personal communication.

[164] Stransky, *supra* note 162.

[165] The Churchill War Rooms, Clive Steps, King Charles Street, London, United Kingdom (visited January 2009); *The Ultimate Guide to Visiting the Churchill War Rooms*, STRAWBERRY TOURS, https://strawberrytours.com/london/museums/churchill-war-rooms (last visited Oct. 19, 2021).

[166] Anonymous, personal communication.

belief (however fleeting) about the object of inquiry. In others, it is enough that the false representations merely deny a true belief: the producers of *Game of Thrones* reportedly created many false endings to disguise which was real.[167]

In addition to concealing, some deceptive precautions are used to discourage would-be misappropriators. Major agricultural companies have been known to "lie" to each other about their "ability to determine [a seed's] parentage," "essentially . . . trick[ing] [another] into not misappropriating its trade secrets by leading it to believe it would get caught."[168]

Some deceptive precautions are used as second-level security precautions, testing and reinforcing the defenses that protect the underlying information asset. For example, Apple "[c]ompany lore" reportedly "holds that plainclothes Apple security agents lurk near the bar at [a local] BJ's," "and that employees have been fired for loose talk there."[169] As Adam Lashinksy reports, "It doesn't quite matter if the yarn is true or apocryphal. The fact that employees repeat it serves the purpose."[170] Interestingly, this precaution not only *works* regardless of whether it is true (as Lashinksy observes), but is also *deceptive* regardless of whether it is true: either the deceptive precaution is the undercover security, or the deceptive precaution is the rumor (causing employees to falsely believe that there are or might be undercover agents).

Some deceptions are similarly used as safeguards to identify and trace security breaches. False entries in everything from databases and client-lists[171] to phonebooks[172] and maps[173] trap the unwary who blindly copy material. This type of deceptive precaution—often called a "mountweazel" after a particularly colorful example[174]—is perhaps the most familiar within IP because it is the most frequently litigated: in addition to serving as a safeguard, such deceptive precautions also provide evidence.[175] This technique has been updated and expanded in the digital age, as discussed next.[176]

---

[167] *See* Callum Crumlish, *Game of Thrones Season 8 Spoilers: Daenerys Targaryen to Destroy Kings' Landing?*, THE DAILY EXPRESS (May 23, 2018), https://www.express.co.uk/showbiz/tv-radio/964012/game-of-thrones-season-8-spoilers-daenerys-targaryen-cersei-lannister-kings-landing-dragon. Producers of *Hunger Games* also reportedly used "screenplay variants for different recipients." Graeme McMillan, *The BBC Schools Hollywood on How to Respond to Leaked Scripts*, Wired (July 7, 2014), https://www.wired.com/2014/07/doctor-who-batman-superman-leaks/.

[168] Advanta USA, Inc. v. Pioneer Hi-Bred Int'l, Inc., No. 04-cv-238, 2004 WL 7346791, at *10 (W.D. Wis. Oct. 28, 2004).

[169] Adam Lashinksy, *Inside Apple: How America's Most Admired—and Secretive—Company Really Works* (Business Plus 2013).

[170] *Id.*

[171] *Infra* text accompanying notes 198 & 228.

[172] *See* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., Inc., 499 U.S. 340 (1991).

[173] *See* Andrew Clark, *Copying maps costs AA £20m*, THE GUARDIAN (Mar. 6, 2001), https://www.theguardian.com/uk/2001/mar/06/andrewclark.

[174] *Infra* Part III.B.3.

[175] *E.g.*, *Feist*, 499 U.S. at 344.; *see also, e.g.*, BidPrime, LLC v. SmartProcure, Inc. No. 1:18-cv-478, 2018 WL 6588574, at *4 (W.D. Tex. Nov. 13, 2018).

[176] *Infra* Part II.B.2.

Finally, some deceptive precautions are used *ex post*, to remedy security breaches that have occurred by obscuring the truth once it is out there. Some measures taken by Hollywood are now aimed at proactively providing for this inevitability: Warner Brothers reportedly "hired Kevin Smith to write a fake screenplay for the 2016 tentpole *Batman v Superman: Dawn of Justice*, with the express intent of leaking it online as a decoy to draw spoiler-hunters away from any legitimate news."[177] The latter category, unsurprisingly, are generally not litigated, but circulate as rumors; litigation would undermine the strategy.

Unless barred for some other reason, all these deceptive precautions would straightforwardly satisfy the doctrinal test for the reasonable precaution requirement, either on their own or as part of a general security package. All involve deceptive practices: presenting a falsehood as true. And many involve the narrower category of direct lies that we call affirmative misrepresentations:[178] an assertion that P (*e.g.*, this document is titled "USC student thesis"), where P is false, made in a context in which P is presented as true—that is, a context in which those who hear or read P are invited to rely on the representation as truthful.

2. Deceptive Precautions as "The Next Big Thing"

Deceptive precautions have taken on a new importance in the digital age. The trend has been growing since at least the turn of the millennium,[179] but has only recently received attention in the legal literature, mostly as a minor entry in the broader phenomenon of "active defense"—cybersecurity defenses that engage with the hacker rather than barring entry, and which range from observational honeypots and other deceptive technology to active and even aggressive means like counterstrikes or "hackbacks."[180]

One of the earlier recognized deceptive cyber-precautions is the honeypot. A honeypot is a decoy computer or network system designed to attract

---

[177] McMillan, *supra* note 167; B. Alan Orange, *Fake Batman v Superman Script Written and Leaked by Kevin Smith?*, MovieWeb (July 3, 2014), https://movieweb.com/fake-batman-v-superman-script-written-and-leaked-by-kevin-smith/.

[178] *Supra* Part I.B.

[179] *See, e.g.*, Ian Walden & Anne Flanagan, *Honeypots: A Sticky Legal Landscape*, 29 Rutgers Comp. & Tech. L.J. 317 (2003).

[180] *See, e.g.*, Rowe, *supra* note 110, at 416–17; Bruce P. Smith, *Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help*, 1 J. L. ECON. & POL'Y 171 (2005); Dorothy E. Denning & Bradley J. Strawser, *Active Cyber Defense: Applying Air Defense to the Cyber Domain, in* UNDERSTANDING CYBER CONFLICT: FOURTEEN ANALOGIES (George Perkovich and Ariel E. Levite, eds., 2017); *see also* Stephanie Balitzer, Note, *What Common Law and Common Sense Teach Us about Corporate Security*, 49 U. Mich. J. L. Reform 891, 896 (2016) ("Passive defense strategies generally encompass those strategies that block intruders from entering a network, whereas active defense strategies involve corporations proactively engaging hackers."). Confusion has resulted from grouping observational and investigative deceptive techniques together with counterstrikes and hackbacks as "active" defense, as many objections to the latter do not apply to the former.

hackers.[181] Its creators design the honeypot to look and act like a real system that is part of the network, but the honeypot is often separate, a mere decoy that is "isolated" (electronically or physically) from the main system and "closely monitored."[182] The honeypot can thus serve as a decoy, "deflect[ing] the hacker from breaking into the real system"[183] and buying time for an appropriate response.[184] The honeypot can also be used for research or investigative purposes, allowing the honeypot operators to gather information about the intruders, their methods, and the system weaknesses being exploited, and to "document evidence for criminal prosecution"[185] or other civil remedies.[186] Sometimes a given network will operate multiple honeypots ("honeynet") and there are also "centralized collection[s] of honeypots and analysis tools" used for broader study ("honeyfarm").[187]

Unlike other forms of "active defense," the honeypot is generally passive. Though the information generated could be used for counteroffensives, the decoy itself is not active and does not necessarily cause harm to the intruder's system (or to third-party systems used by hackers as shields). Accordingly, many of the criticisms levied against "active defense," and so much of the legal debate about active defense, does not apply to the more passive honeypot.[188] (For this reason, the grouping of honeypots and other passive detection and deception technologies with the more aggressive forms of active defense, like counterstrikes, has led to some analytic confusion.[189]) And it appears that honeypots can be designed to avoid pitfalls presented by various communications statutes, like the Computer Fraud and Abuse Act or the Electronic Communications Privacy Act.[190] Indeed, many of the legal concerns raised about honeypots apply primarily to their use in law enforcement because of entrapment issues that are raised;[191] these entrapment concerns do not apply to civil trade secret remedies.

"Deception technology" further develops—or at least, rebrands—the basic principles underlying the honeypot into its own "emerging category of

---

[181] Walden & Flanagan, *supra* note 179, at 318–19; Honeypot, SearchSecurity, https://searchsecurity.techtarget.com/definition/honey-pot (last visited Jan. 21, 2021) [https://perma.cc/7FZF-53AD].

[182] Honeypot, *supra* note 181.

[183] Walden & Flanagan, *supra* note 179, at 319.

[184] *E.g.*, Smith, *supra* note 180, at 177 (noting Symbiot's use of "Simulated Responses" that "'provid[e] "decoy" responses to service requests' that appear 'legitimate' but do not 'stress . . . critical servers'" (quoting Symbiot, Inc., Graduated Response™, http://symbiot.com/graduatedres.html#CYCLE)).

[185] Walden & Flanagan, *supra* note 179, at 319.

[186] *See* Sean L. Harrington, *Cyber Security Active Defense: Playing with Fire of Sound Risk Management*, 20 RICH. J.L. & TECH. 1, 18-19 (2014); *infra* Part II.B.3.

[187] Honeypot, *supra* note 181.

[188] *See* Walden & Flanagan, *supra* note 179, at 328-29.

[189] *See* Denning & Strawser, *supra* note 180, at 194-95 (attempting to distinguish between active and passive defenses).

[190] *See* Walden & Flanagan, *supra* note 179, at 345–47; Harrington, *supra* note 186 at 18-19. This is not to minimize the difficulty of design. *See Infra* Part II.C.

[191] *See* Harrington, *supra* note 186, at 18-19.

cyber security defence."[192] Like honeypots, deception technology "seeks to trick hackers into thinking they are getting close to critical data."[193] Unlike most honeypots,[194] deception technology includes decoys and traps hidden throughout the main system itself (rather than a walled-off system) and are used primarily to track, trace, and redirect a hacker that has already breached the outer perimeter.[195]

Some known uses of deception technology have been reactive, concealing trade secrets from and buying time against known intruders. When SmartProcure repeatedly attempted to hack BidPrime's system and scrape its trade secrets, "BidPrime security realized that [SmartProcure] was not going to stop" and that if SmartProcure realized "they had been detected, [they] would resort to even more subversive measures."[196] Accordingly, "[t]o protect its trade secrets," BidPrime "substitute[d] scrambled archive data for the data that would be displayed [in response to] searches performed under [one of SmartProcure's fake] account[s]."[197] As BidPrime explained in its complaint:

> [R]eal, but older, data was still displayed for searches performed under [SmartProcure's fake] account, and the data was mixed up. For example, a bid request result would display a real bid request title and a real bid request expiration date but, due to BidPrime's defensive scrambling, the expiration data may not have belonged with that particular bid title. In addition, to protect its trade secret bid source database, BidPrime dummied the bid source URLs that accompanied the scrambled bid requests.[198]

Increasingly, however, companies use deception technology proactively to identify and defend against unknown threats. For example, Illusive Networks capitalizes on the way authorized users inadvertently leave trails of information, including credentials, in places like their browsers' caches.[199] Hackers, once in a system, find and leverage this information to gain further access.[200] Illusive Networks plants fake credentials within this trail.[201] When hackers then use the fake credentials, "the system disorients them with deceptive data" and

---

[192] Jennifer O'Brien, *CSIRO's Data61 and Penten Hatch Cyber 'Deception' Tech*, CIO Magazine (Oct. 2, 2019), https://www.cio.com/article/3498936/csiro-s-data61-and-penten-hatch-cyber-security-deception-tech.html.

[193] Heidi Mitchell, *In Battle Against Hackers, Companies Try to Deceive the Deceivers*, THE WALL ST. J. (Dec. 7, 2020), https://www.wsj.com/articles/in-battle-against-hackers-companies-try-to-deceive-the-deceivers-11607371200.

[194] The meaning and use of these terms continues to evolve.

[195] Rowe, *supra* note 110, at 416-17.

[196] Comp. ¶ 60, BidPrime, LLC v. SmartProcure, Inc., No. 1:18-cv-478, 2018 WL 5274202 (W.D. Tex. July 17, 2018). "Web-scraping" is the automated downloading of "large amounts of data from websites." *Id.* at ¶ 42.

[197] *Id.* at ¶¶ 24, 60.

[198] *Id.* at ¶ 60.

[199] *Identify and Remove Attack Pathways*, ILLUSIVE, https://illusive.com/products-services/products/attack-surface-manager/.

[200] *Id.*

[201] *See id.*; Mitchell, *supra* note 193.

alerts the security team.[202] As Illusive's marketing explains: "[Illusive's] Attack Detection System plants deceptions on every endpoint that looks like the data attackers need to move towards critical assets. Immediate post-perimeter detection allows you to foil attacker reconnaissance and their lateral movement process."[203]

Deception technology is exploding. Sold as products, services, or both, by companies like Illusive, MITRE, TrapX, and Attivo Networks, the deception technology market was valued at $1.48 billion worldwide in 2018, a figure projected to reach $3.72 billion by 2026.[204] According to Illusive's chief executive, "the technology is more widespread than many assume, especially in highly regulated industries like banking, insurance and government."[205] Known users include national brands in diverse industries, from Land O'Lakes (agriculture) to Aflac (insurance) to Proctor & Gamble (consumer products).[206] In 2020, Illusive Networks completed a $24 million funding round, drawing interest from Spring Lake Equity Partners, Marker, NEA, Bessemer Venture Partners, Innovation Endeavors, Cisco, Microsoft, and Citi.[207]

Such deception technology is not the only use of deception that has become important. Misinformation—that ubiquitous topic du jour—also has a corporate security role to play. Trade secret law traditionally focused on former employees, partners, or corporate spies who misappropriate intellectual assets to compete.[208] But competition is no longer the only concern. Now, there is the risk that "hacktivists," disgruntled ex-employees, and other corporate enemies publish stolen secrets online.[209] Once the secret becomes widely available, it is no longer secret and trade secret protection disappears.[210]

---

[202] *See* Mitchell, *supra* note 193.

[203] *Deterministic Threat Detection*, ILLUSIVE, (last visited February 1, 2021), https://illusive.com/products-services/products/attack-detection-system/.

[204] *Deception Technology Market is Projected to Grow at USD 3.72 Billion by 2026 at a CAGR of 16.04%,* BIG NEWS NETWORK (Oct. 1, 2021) https://www.bignewsnetwork.com/news/271364084/deception-technology-market-is-projected-to-grow-at-usd-372-billion-by-2026-at-a-cagr-of-1604; *see also Deception Technology: Worldwide Market Opportunities through 2018-2023*, GLOBAL NEWSWIRE (December 20, 2018) (valuing deception technology market at $907.56 million in 2017, with forecasted growth to $1.84 billion by 2023). These valuations are consistent with earlier forecasts by Daniel Ives, a senior technology analyst at FBR Capital Markets. *Companies Look Beyond Firewalls in Cyber Battle with Hackers*, REUTERS (January 26, 2016), https://www.reuters.com/article/israel-tech-cyber-idCNL8N15A4HR (predicting "$3 billion market over the next three years").

[205] Mitchell, *supra* note 193 (explaining the perspective of Ofer Israeli, CEO of Illusive Networks).

[206] *Id; see also TrapX Security*, https://trapx.com (last visited February 1, 2021); *Case Study: Proctor & Gamble Transforms Its Cyber Resilience Program*, TRAPX (Nov. 20, 2020), https://www.trapx.com/wp-content/uploads/2021/01/TrapX_PG_Case_Study_072020.pdf.

[207] *Illusive Networks Secures $24 Million in Latest Funding Round*, PR NEWSWIRE (October 7, 2020).

[208] *See* Rowe, *supra* note 110, at 408–09.

[209] *See* Rowe, *supra* note 111, at 22–25 (collecting cases).

[210] Cundiff, *supra* note 20, at 399; Rowe, *supra* note 111, at 21 & n.158.

But the options for stopping the spread are limited: Takedowns are slow and unreliable.[211] And seeking one risks further publicity (the "Streisand effect").[212] Enter the lie: instead of an immediate takedown, bury the secret in an information flood.

There is speculation that Cisco did exactly this: when its source code appeared online, Cisco reportedly posted fake versions from fake usernames and IP addresses.[213] Doing so obscured whether any were authentic and (if so) which it was.[214] This technique has proven reasonably effective, as evidenced by a growing industry of public relations firms that publish rumors about their clients to bury or undermine negative or invasive press.[215] Early researchers and companies in this space identified "publicity disinformation, and other techniques of psychological operations" as aggressive, last resort measures,[216] suggesting broader and perhaps more dangerous uses than Cisco's.

Finally, deceptive precautions in cyberspace may be pedestrian. You, dear reader, have probably been on the receiving end. One of the biggest vulnerabilities in any network, computer or otherwise, remains the human one.[217] By now, most are aware of phishing: "[a] digital form of social engineering to deceive individuals into providing sensitive information."[218] But while most people are aware, at least nominally, of the risk, hackers have grown adept at mimicking legitimate communications.[219] And so, IT professionals increasingly recommend "phishing simulations" as part of best security practices: sending fake phishing emails to employees.[220] These simulations help IT identify employees who fail to report threats (a common

---

211 *See* Elizabeth A. Rowe, *Introducing a Takedown for Trade Secrets on the Internet*, 2007 WIS. L. REV. 1041, 1043 (2007).

212 Cundiff, *supra* note 20, 406-07 (discussing split regarding continued protection); Rowe, *supra* note 211, at 1086; *see e.g.*, DVD Copy Control Ass'n v. Bunner, 10 Cal. Rptr. 3d 185, 190, 196 (App. Ct. 2004) (reversing preliminary injunction in part because secret had spread online).

213 *See* Cundiff, *supra* note 20, 408 & n.220.

214 *Id.*

215 *See generally* FINN BRUNTON & HELEN NISSENBAUM, OBFUSCATION: A USER'S GUIDE FOR PRIVACY AND PROTEST (2015).

216 Smith, *supra* note 180, at 178 (quoting Paco Nathan & Mike Erwin, *On the Rules of Engagement for Information Warfare* 4-5 (Mar. 4, 2004), http://www.symbiot.com/pdf/iwROE.pdf).

217 *See generally, e.g.*, KEVIN MITNICK AND WILLIAM SIMON, THE ART OF DECEPTION: CONTROLLING THE HUMAN ELEMENT OF SECURITY (2002).

218 Gonzales III, Joaquin J., *Glossary of Cybersecurity Terms* (2019), *in* CYBERSECURITY: CURRENT WRITINGS ON THREATS AND PROTECTION (Joaquin Jay Gonzales III and Roger L. Kemp, eds. 2019).

219 *See* Kevin J. Ryan, *Phishing Is Getting More Sophisticated. Here's What to Look Out For*, INC. (Jan. 17, 2020), https://www.inc.com/kevin-j-ryan/cybersecurity-data-breaches-hacks-how-ceo-use-tech-survey.html.

220 Stu Sjouwerman, *Best Practices for Phishing Your Employees*, Forbes (May 18, 2020), https://www.forbes.com/sites/forbestechcouncil/2020/05/18/best-practices-for-phishing-your-employees/?sh=11d022552b63 ("Security awareness training should include an ongoing phishing program where you send fake phishing emails to your employees.").

problem) and those likely to fall for them, while simultaneously training employees on how to recognize threats and respond appropriately.[221] This deceptive precaution is increasingly recommended as a best practice,[222] but involves lying to the workforce.

3. Lies as a Legitimate Option

Given the trend towards the cost-benefit approach to the RPR suggested in *Rockwell* and *E.I. duPont*, most of the deceptive precautions described above easily count as a "reasonable precaution" for purposes of the RPR. And litigants have begun to treat them as such, citing their use of fake data as examples of precautions taken.[223] Where adopted, deceptive precautions provide evidence that (a) the trade secret owner treated the information as secret; (b) the defendant took the secret by improper means (i.e., it did not merely leak); and (c) that the secret had value (as a function of security costs).[224]

At least one court has recognized this possibility. In *SolarCity Corporation v. Pure Solar Company*,[225] SolarCity sued a competitor, Pure Solar; Pure Solar employees; and a former SolarCity employee who had leaked customer information to Pure Solar.[226] SolarCity learned of the problem when it began receiving complaints from customers about why Pure Solar had their contact information.[227] SolarCity developed a honeypot to investigate. As described in the complaint, once the software was implemented:

> any time a user exported customer data from SolarCity's customer database . . . the customer's actual phone number would be replaced with a different "decoy" phone number obtained by SolarCity through a third party vendor. SolarCity acquired multiple such decoy phone numbers to avoid duplication and detection. SolarCity then acquired a separate "honeypot" phone and had all calls to the decoy customer phone numbers routed to it. A SolarCity employee would answer the honeypot phone and obtain as much information as possible about the caller and the customer he or she was attempting to call. SolarCity analyzed the information obtained from these calls and information from call logs to the decoy phone numbers to determine whether the

---

[221] *Id.*

[222] *See id.*; *see also* Testimony of Daniel Castro, at *5 (2018) Preparing Small Businesses for Cybersecurity Success: Hearing before the Committee on Small Business and Entrepreneurship, United States Senate, One Hundred Fifteenth Congress, Second Session; Rukma Sen, *Why Integrated Phishing-Attack Training Is Reshaping Cybersecurity*, MICROSOFT SECURITY (Oct. 5, 2020), https://www.microsoft.com/security/blog/2020/10/05/why-integrated-phishing-attack-training-is-reshaping-cybersecurity-microsoft-security/.

[223] *E.g.*, Compl. at ¶¶ 19–22, SolarCity Corp. v. Pure Solar Co., No. 5:16-cv-01814 (C.D. Cal. Aug. 23, 2016) ECF No. 1.

[224] *See* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 178–80 (7th Cir. 1991).

[225] No. 5:16-cv-01814, 2016 WL 11019989, at *1 (C.D. Cal. Dec. 27, 2016).

[226] *Id.*

[227] *Id.*

> calls were to actual customers in SolarCity's database who had been assigned decoy numbers. If SolarCity was able to confirm that the call was to a customer in its database, SolarCity could then determine who exported the customer's information and when it had been exported.[228]

SolarCity alleged that the honeypot quickly "began receiving . . . calls from Pure Solar sales representatives."[229] SolarCity analyzed the decoy numbers and traced them to an employee whose "username was the only username that was consistently associated with exports of customer information where Pure Solar attempted to call a customer using the decoy phone number."[230]

SolarCity relied on its use of the honeypot, in conjunction with other security measures, to allege that it had satisfied the RPR under both the DTSA and California UTSA.[231] SolarCity also relied on honeypot evidence to support its other claims, including to establish a timeline for the application of the DTSA, to support allegations of ongoing activity for purposes of a RICO claim, and to show loss for its claim under the CFAA.[232]

In denying Defendants' motion to dismiss, the district court recognized the honeypot's evidentiary value. Although Defendants had not challenged SolarCity's satisfaction of the RPR, the court recognized the honeypot as evidence of both misappropriation and value. The court accepted allegations about the honeypot as "sufficient facts" to allege that "unlawful misappropriation" occurred after the DTSA's effective date.[233] And the court found that SolarCity "established 'loss' [under the CFAA] as it has alleged that Defendants' actions required it to undertake 'an investigation,' that included developing 'software applications that would detect the export of data from a search application accessing SolarCity's customer database,' acquire a honeypot, and analyze the information obtained from these honeypot calls," a loss worth at least $5,000.[234] The parties eventually settled.[235]

4. When Lying Is the Only Option

Trade secret law legitimates certain lies—like SolarCity's honeypot scheme—through the RPR. But could trade secret law mandate such precautions? If the court's approval of the honeypot precaution in *SolarCity* is

---

[228] Compl. at ¶¶ 19–22, SolarCity Corp. v. Pure Solar Co., No. 5:16-cv-01814 (C.D. Cal. Aug. 23, 2016) ECF No. 1.

[229] *Id.*

[230] *Id.*

[231] *Id.* at ¶¶ 42, 55 ("Plaintiff made reasonable effort and took reasonable steps in order to keep secret the information, including . . . by taking steps to determine whether breaches of the information contained in the database occurred and to address and take action to respond to actual or potential breaches"); *see also id.* at ¶¶ 19–22.

[232] *Id.*; Pl.'s Mem. Opp. Defs.' Mot. Dismiss 11, 15, SolarCity Corp. v. Pure Solar Co., No. 5:16-cv-01814 (C.D. Cal. Nov. 28, 2016), ECF No. 34.

[233] SolarCity, 2016 WL 11019989, at *4.

[234] *Id.* at *9 (citations omitted).

[235] Order, SolarCity Corp. v. Pure Solar Co., No. 16-cv-01814 (C.D. Cal. Aug. 27, 2018), ECF No. 70.

any indication, then the answer is: probably, especially as deception becomes more widely adopted as cybersecurity best practices.

While the RPR's case-by-case inquiry means that courts rarely fault the failure to take a *particular* precaution, some precautions are effectively treated as mandatory. Disclosing a trade secret without a non-disclosure agreement will generally bar a claim.[236] Older cases required that secrets be kept under "lock and key."[237] And, analogously, courts today increasingly recognize that failing to protect electronic passwords is a failure to take reasonable precautions.[238] These exceptions follow a pattern: they are basic, commonsense, and widely adopted. In short, they are best practices.

A review of cyber-security's history suggests that deceptive precautions are on that trajectory. Honeypots, developed in the early 1990s, grew increasingly commercialized around the turn of the millennium and have remained a standard investigative tool.[239] Phishing simulations are here to stay, and unlike fire alarms, cannot be pre-announced.[240] And today's "deception technology"—that $1.5 billion market aimed at identifying and mitigating internal threats—are already being touted as best practices.[241] If such

---

[236] *E.g.*, Weins v. Sporleder, 569 N.W.2d 16, 23 (S.D. 1997)); BidPrime, LLC v. SmartProcure, No. 18-cv-478, 2018 WL 8223430, at *2–3 (W.D. Tex. June 18, 2018) (finding lack of reasonable precautions where bid aggregator website's terms of service did not forbid users from copying and publishing data); *see also* Peterson, *supra* note 112, at 432–33 & nn.387–88 (collecting cases). A non-disclosure agreement alone, however, will not save a claim. *See* Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1334 (N.D. Ga. 2007).

[237] *E.g.*, McCann Const. Specialties Co. v. Bosman, 358 N.E.2d 1340, 1342 (Ill. Ct. App. 1977).

[238] *E.g.*, Defiance Button Mach. Co. v. C & C Metal Prods. Corp., 759 F.2d 1053, 1063-64 (2d Cir. 1985) (passwords).

[239] *See* Andrew Evans, Honeypots – Weighing up the Costs and Benefits (Oct. 28, 2002) (Global Information Assurance Certification Paper, SANS Institute), https://www.giac.org/paper/gsec/2300/honeypots-weighing-costs-benefits/103964.

[240] Testimony of Daniel Castro, at *5 (2018) Preparing Small Businesses for Cybersecurity Success: Hearing before the Committee on Small Business and Entrepreneurship, United States Senate, One Hundred Fifteenth Congress, Second Session; Rukma Sen, *Why Integrated Phishing-Attack Training Is Reshaping Cybersecurity*, MICROSOFT SECURITY (Oct. 5, 2020), https://www.microsoft.com/security/blog/2020/10/05/why-integrated-phishing-attack-training-is-reshaping-cybersecurity-microsoft-security/; MED TECH SOLUTIONS, PHISHING SIMULATION BEST PRACTICES: PROTECT YOUR PRACTICE AGAINST EMAIL ATTACKS 4 (2020), https://f.hubspotusercontent10.net/hubfs/4247816/MTS_Phishing%20_WP_010821.pdf.

[241] *See, e.g.*, Gilad David Maayan, *How Deception Technology Can Help You Detect Threats Early*, SECURITY TODAY (Aug. 12, 2019), https://securitytoday.com/Articles/2019/08/12/How-Deception-Technology-Can-Help-You-Detect-Threats-Early.aspx?Page=1; Dan Woods, *How Deception Technology Gives You The Upper Hand In Cybersecurity*, FORBES (June 22, 2018),

precautions would have caught a rogue employee or an external threat that breached the firewall, any litigator worth their salt will point to the failure to adopt such precautions as a failure to satisfy the RPR.

That such precautions will ultimately be required is consistent with expert views about what the RPR requires in the age of cybersecurity. The digital era presents "enhance[d] . . . risks of trade secret misappropriation through electronic means."[242] Accordingly, Elizabeth Rowe, for example, has argued that "what security measures are reasonable [under the circumstances]" now includes proactive risk assessment and mitigation of electronic threats.[243] Deception technology provides exactly that: risk assessment and mitigation—in real time and with minimal false positives.[244]

Will courts affirmatively require "deception" technology? A First Amendment defense might be raised, though its scope is unclear, and in any event, has not prevented courts from requiring basic notice and non-disclosures.[245] And courts might not be willing to do so under that name ("deception") given the tensions described in Part I and returned to in Part III.[246]

But both possibilities might escape notice: courts have been slow to pop the hood on technical precautions.[247] Litigants may discuss in general terms the precautions taken, using euphemisms like "honeypot," "decoy," and "obfuscation"; brand names of leading services; or certifications that confirm compliance with cybersecurity protocols without courts realizing that such compliance is satisfied through the use of deception technology.

C. Reasonable Limits

The cost-benefit approach in *Rockwell* and *E.I. duPont* establishes a floor of reasonableness: a company must take at least those precautions that are cost-effective.[248] But it does not establish a ceiling—a way to tell when a trade secret owner has gone too far. There must be limits to what is "reasonable," to the extent of self-help permitted trade secret owners. A company couldn't kill someone and seek relief on that basis, could it? Analogously, one might worry the RPR would go too far if it recognized lies as a legitimate option for satisfying a legal requirement—or worse, mandated them.

---

https://www.forbes.com/sites/danwoods/2018/06/22/how-deception-technology-gives-you-the-upper-hand-in-cybersecurity/?sh=5819c6af689e; *supra* note 204.

242 Rowe, *supra* note 111, at 14–26.

243 *Id.* at 26–27.

244 *Supra*, Part II.B.2; *see also* Maria Korolov, *Deception Technology Grows and Evolves*, CIO MAGAZINE (Aug. 29, 2016), https://perma.cc/T6CC-7ULE.

245 *See* Rebecca Wexler, *Warrant Canaries and Disclosure by Design: The Real Threat to National Security Letter Gag Orders*, 124 YALE L.J.F. 158, 169–73 (2014).

246 *See infra* Part III.C.

247 *See* Rowe, *supra* note 111.

248 *See* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 179–80 (7th Cir. 1991); E.I. DuPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1017 (5th Cir. 1970).

Any argument that deceptive precautions *do not* (as opposed to *should not*) satisfy the RPR presumes that there is some legal limit on what counts as "reasonable." The limits on a trade secret *plaintiff's* behavior, especially regarding precautions, remain undertheorized.[249] But it is clear that such limits do not *categorically* preclude deceptive practices from satisfying the RPR.

There are three broad categories from which such limits might be derived to the general case: equity, criminal law, and torts.

Equity. There is a principle of equity that might appear to foreclose legal recognition of deceptive precautions—namely, that "[n]o one shall be permitted to profit by his own *fraud*."[250] Lies often form the basis of unclean hands defenses,[251] including in trade secret cases.[252] While the unclean hands doctrine requires that the alleged misconduct be tightly related to the dispute before the court, deceptive precautions seem to fit that bill: the precautions taken by a trade secret owner are "at the heart of every trade secret misappropriation case and often determine[] the outcome."[253] Indeed, courts have declined to strike unclean hands defenses based on the use of honeypots—at least against copyright trolls who use honeypots to "seed[]" their work and "generate litigation."[254]

But this limitation is not a categorical one, and may in fact be quite limited. Where courts have accepted unclean hands based on the trade secret owner's lies, it is usually because the trade secret owner engaged in fraud-based misappropriation (including to gain the trade secret at issue).[255]

---

[249] *See supra* note 156.

[250] Riggs v. Palmer, 22 N.E. 188, 189–90 (N.Y. 1889); *see also* Campbell v. Thomas, 897 N.Y.S.2d 460, 469–70 (N.Y. App. Div. 2010) (collecting cases); Klass, *supra* note 13, at 725.

[251] *See, e.g.*, Gilead Sci., Inc. v. Merck & Co., No. 13-cv-04057, 2016 WL 3143943, at *29 (N.D. Cal. June 6, 2016) (finding unclean hands barred patent enforcement where, *inter alia*, plaintiff lied by omission about firewalling relevant personnel during joint venture and patents were based on trade secrets that had been misappropriated as a result); Thermech Eng'g Corp. v. Abbot Labs., No. G030381, 2003 WL 23018553, at *8–9 (Cal. Ct. App. 2003) (rejecting unclean hands defense based on, *inter alia*, plaintiff's alleged lie in which plaintiff failed to inform defendant that it used a different Teflon product than the one on the purchase order).

[252] *See* ACI Chem. Inc. v. Metaplex Inc., 615 So.2d 1192, 1195–97 (1993) (dicta) (citing 2 CALLMAN, UNFAIR COMPETITION, TRADEMARKS, AND MONOPOLIES § 14.24 (4th ed. 1982)).

[253] Rowe, *supra* 111, at 3; *see also* Scherer Design Grp., LLC v. Ahead Eng'g LLC, 764 F. App'x 147, 154 (3d Cir. 2019) (Ambro, J., dissenting).

[254] *See, e.g.*, Pl.'s Mot. to Strike at 3–4, 10, Malibu Media, LLC v. Schmidt, No. 19-cv-599 (W.D. Tex. May 4, 2020), ECF No. 21; Malibu Media, LLC v. Schmidt, No. 19-cv-599, 2020 WL 5351079, at *1–2 (W.D. Tex. Sept. 1, 2020) (denying in relevant part motion to strike) (case still pending); Malibu Media v. Doe, 2014 WL 2616902, at *3 (E.D. Mich. June 12, 2014) ("To the extent defendant's unclean hand defense relies on a seeding of Plaintiff's videos, the Plaintiff's motion to strike will be DENIED IN PART.").

[255] *See, e.g.*, ACI Chem., 615 So.2d at 1196–97; Cataphote Corp. v. Hudson, 422 F.2d 1290, 1295-96 (5th Cir. 1970); *see also* Comp. Assocs. v. Bryan, 784 F. Supp. 982,

Several courts have expressly rejected an unclean hands defense based on protective lies and deceptive precautions.[256] For example, in *Advanta USA, Inc. v. Pioneer Hi-Bred International, Inc.*, Advanta attempted to raise an unclean hands defense to trade secret misappropriation, arguing that Pioneer had lied when it told Advanta that it was "monitoring Advanta's commercial hybrids and that it had the ability to determine their parentage," even though "Pioneer's technology was not reliable for this purpose until" years later.[257] The court reasoned that "Advanta's argument—essentially that Pioneer tricked Advanta into not misappropriating its trade secrets by leading it to believe it would get caught—is unpersuasive."[258] And in *Scherer Design Group, LLC v. Ahead Engineering LLC*, the Third Circuit affirmed the rejection of an unclean hands defense even though Plaintiff had surreptitiously accessed Defendant's Facebook account to monitor suspected misappropriation.[259]

Deceptive precautions thus risk inviting an unclean hands defense, but unclean hands does not undermine the RPR's recognition or potential mandating of certain deceptive precautions, including lies. This risk simply underscores the need for legal counsel in designing deceptive precautions—which raises its own difficulties.[260]

---

998 (E.D.N.Y. 1992) (rejecting unclean hands based on plaintiff's subterfuge during investigation of misappropriation, noting that "the doctrine of unclean hands is only applicable when the conduct relied on is directly related to the subject matter in litigation—in this case meaning that it would have to be related to the creation or acquisition of the trade secrets themselves"). One might also expect courts to find unclean hands if a trade secret owner behaved as a troll and lied for the purpose of inducing misappropriation so as to generate a dispute. *Cf., e.g.*, *Malibu*, 2020 WL 5351079, at *1–2 (denying motion to strike unclean hands defense raised against copyright troll that used "a 'digital honeypot'—a scheme in which a copyright holder displays a work online in a way that lures users into downloading the work, only to then sue the users for copyright infringement").

[256] *E.g.*, Advanta USA, Inc. v. Pioneer Hi-Bred Int'l, Inc., No. 04-cv-238, 2004 WL 7346791, at *10 (W.D. Wisc. Oct. 28, 2004).

[257] *Id.*

[258] *Id.*

[259] Scherer Design Grp., LLC v. Ahead Eng'g LLC, 764 F. App'x 147, 148–50 (3d Cir. 2019) (unpublished) (explaining that Plaintiff accessed the account using cached password on Defendant's returned company laptop and "installed software that allowed [IT] to monitor [Defendant's] Facebook activity [after Defendant's termination] without detection"); *see also* Comp. Assoc. v. Bryan, 784 F. Supp. 982, 998 (E.D.N.Y. 1992) (rejecting unclean hands defense because use of "fictitious name" to license and sign agreements to procure defendant's allegedly infringing product, "although not condoned," "was taken not to copy the [software] for some competitive advantage but rather to resort to self-help to determine to what extent, if at all, [defendant] had copied and was using [plaintiff's] trade secrets").

[260] *See infra* Part IV.

Criminal Law. Many lies are criminalized.[261] More lies, in fact, than most are aware.[262] Federal offenses "include[d] 100 separate misrepresentation offenses" twenty years ago, and that number has almost certainly increased.[263] Such offenses, like our focus here, "criminalize not only lying but concealing or misleading as well" and are not limited to lies which are material.[264] There may be particular concern that various deceptive precautions in cybersecurity, especially if they continue to be lumped in with or characterized as "hackbacks," run afoul of criminal statutes like the Computer Fraud and Abuse Act ("CFAA").[265]

But common sense suggests that there is likely some daylight to be found. It would be odd to suggest that a "Beware of Guard Dog" sign (when there are none) is ill-advised merely because of the breadth of codes criminalizing lies. There is considerable prosecutorial discretion, and many commentators bemoan criminal law enforcement's inability or refusal to reach many pervasive and harmful lies.[266] Further, it is not clear that all such statutes would survive a First Amendment challenge.[267]

The potential for criminal liability for certain deceptive precautions creates risk. The real question that emerges is not *whether* one can lie to protect a trade secret in satisfaction of (or as required by) the RPR, but *how* to lie so as to avoid these particular and complicated constraints.[268]

Torts. Even if not illegal, the critic might insist that deceptive precautions—even those that appear innocuous—inevitably carry some risk that an innocent party will rely on the deception to their detriment, and so deceptive precautions should not satisfy the RPR.

This criticism is misplaced. Many reasonable precautions risk harm to others, and even open the firm to civil liability. Guard dogs and barbwire fences are generally considered reasonable precautions against trespassers,

---

[261] William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505, 517–18 (2001).

[262] *Id.*; *see, e.g.*, United States v. Wells, 519 U.S. 482, 502 (1997) (Stevens, J., dissenting) ("As now construed, § 1014 covers false explanations for arriving late at a meeting, false assurances that an applicant does not mind if the loan officer lights up a cigar, false expressions of enthusiasm about the results of a football game or an election, as well as false compliments about the subject of a family photograph. So long as the false statement is made 'for the purpose of influencing' a bank officer, it violates § 1014.").

[263] Stuntz, *supra* note 261, at 517 (citing Wells, 519 U.S. at 505 (Stevens, J., dissenting)).

[264] *Id.* at 517-18 (noting that over half the federal misrepresentation statutes lack materiality requirement (citing Wells, 519 U.S. at 505–06 & nn. 8–10 (Stevens, J., dissenting)).

[265] *See The Hackback Debate*, STEPTOE CYBERBLOG (Nov. 2, 2012), http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/.

[266] *See, e.g.*, Manta, *supra* note 52, at 210–12.

[267] *See, e.g.*, United States v. Alvarez, 567 U.S. 709, 729-30 (2012).

[268] *Infra* Part IV.

though they risk harm to non-trespassers for which a firm would be liable.[269] The mere possibility that a particular deceptive precaution involves these risks does *not* affect whether it can satisfy the RPR. Risks alone do not make a precaution unreasonable; the question is whether the risk is reasonable.[270]

A critic might counter that the risky-but-reasonable nondeceptive precautions identified involved small risks: well-trained dogs are unlikely to attack except when appropriate and children rarely need to hurdle a wall to escape greater danger.[271] But this assumes—incorrectly—that reasonable nondeceptive precautions always pose small risks, and that deceptive precautions always pose large ones. Guard dogs may be very risky: they may be vicious, or poorly trained and poorly secured. If they are—and if they cause harm—the firm faces liability. Yet these vicious guard dogs might still be a reasonable precaution, and the firm may not be liable if the dogs attack a wrongdoer.[272] Policing the care with which a firm undertakes its precautions is not within the purview of trade secret law; that is the purview of torts, when and if damages arise, and of regulations, for harms that must not be risked.

To be sure, some deceptions impose great risk. Were engineers to rely on information that had been obscured by deceptive precautions, the engineers could develop false beliefs about a device's parameters leading to devastating results. The risks posed might be unjustifiably great, perhaps providing ground for refusing to accept the deceptive precaution in satisfaction of the RPR. But it should not be assumed that because some deceptions pose an unreasonable risk that all do. And tort law and business regulations are almost certainly better suited than trade secret law for deterring such unjustifiably risky precautions. Moreover, a limitation on precautions that satisfy the RPR is unlikely to discourage a firm from taking such measures; if legal and cost-effective, companies will still take such precautions, even if they do not later cite them in court. The law needs to target the risk (and its consequences) directly. In sum, unless deception is somehow "special," mere risk of civil liability or individualized harm alone does not provide reason to find that deceptive precautions involving such risk cannot satisfy the RPR.

The Theranos case underscores this point, that nondeceptive precautions can be just as dangerous as deceptive ones. In addition to deceptive precautions, Theranos also used common nondeceptive precautions to protect its purported trade secrets: nondisclosure agreements, tinted windows, guards,

---

[269] *See* Rossi v. DelDuca, 181 N.E.2d 591, 592-94 (Mass. 1962) (holding dog owner liable for harm done to girls who came onto his property to escape danger); Woodbridge v. Marks, 45 N.Y.S. 156, 160 (N.Y. App. Div. 1897) (denying recovery where dog not "unusually or unnaturally vicious").

[270] *Cf.* Barbara Fried, FACING UP TO SCARCITY: THE LOGIC AND LIMITS OF NONCONSEQUENTIALISM (2020).

[271] *See, e.g.*, Rossi, 181 N.E.2d 591.

[272] For example, a court denied relief where the plaintiff strayed from the path. *See Woodbridge v. Marks*, 45 N.Y.S. 156, 159 (N.Y. App. Div. 1897). In distinguishing from spring guns, which are prohibited, the court observed that guard dogs are usually used to frighten off an intruder, which is permissible, despite the risk that they might "attack and bite any stranger who insisted upon forcing his way onto the locality [the dog] was set to guard." *Id.* at 160.

fingerprint scanners, and surveillance cameras.[273] But the precaution that contributed most directly to Theranos's fraudulent scheme was not a deceptive precaution. It was Theranos's aggressive enforcement of nondisclosure agreements—a precaution so commonly recognized as reasonable that it is one of the few required despite frequent abuse.[274]

D. Incentives and Expression, Depth and Breadth

I want to make a distinction here to clarify the nature of my claim. I have argued that trade secret law legitimizes lying. This is an argument about expressive force. But it is easy to confuse my claim with the view that the RPR *incentivizes* lying. Whether the law *incentivizes* lying is also concerning, but my claim is *not* about incentives.[275] My claim is about what the law *accepts*. This is one of the reasons that the trade secret case is so useful as a starting point for probing the depth of the law's response to permitted lies: it cuts directly to what the law approves.

I have assumed that the deceptive precautions at issue are cost-effective for the firm. Some subset of these are also already permitted.[276] If they are cost-effective, and permitted, companies (if they're smart) will use these precautions anyways, regardless of what trade secret law has to say about it. The incentive to use them comes from the precautions being cost effective for protecting valuable assets, not from the RPR's recognition thereof. This is true even for those limited precautions that the RPR requires: most are so basic—e.g., passwords—that if they are cost effective, we should expect companies to take them anyways.[277] Indeed, a common criticism of the RPR is that, if it is meant to induce precautions, it is either redundant or wasteful.[278]

---

[273] *See, e.g.*, CARREYROU, *supra* note 61, at 297.

[274] *See generally id.* at 296-97; *see also supra*, note 143. The abuse of nondisclosure agreements and trade secret law to silence whistleblowers had become so common that the DTSA created an express exception to trade secret liability for whistleblowers. *See* DTSA § 7, codified at 18 U.S.C. § 1833.

[275] *Cf.* William N. Eskridge, *Law and the Production of Deceit*, *in* LAW AND LIES, *supra* note 1. Eskridge discusses the law's encouragement of lies, largely through the lens of regulations in the LGBTQ and immigration contexts that leave those regulated little choice but to lie to the government about who they are. Many of the lies he identifies are "required" in the sense of having no alternative to evade the law's consequences, even if the lies themselves are maintaining a legal fiction. This differs from the sense of "required" used here, in which the law requires a lie to someone else. But he raises an interesting question about whether "Don't Ask, Don't Tell" comes very close to being a *policy* of lying that would raise similar expressive concerns.

[276] *See supra* Part II.C.

[277] *See supra* Part II.B.4; *see also supra* Part II.A.2 (explaining that the RPR is a fact-intensive inquiry that, with few exceptions, does not require *particular* precautions be taken). One might think that the moral valence of lies would give companies pause, such that such precautions would not be taken unless required; the explosive growth of deception technology and the prevalence of phishing simulations provides empirical evidence to the contrary. *Supra* Part II.B.2. In any event, the full scope of required deceptive precautions remains for future work.

[278] *See, e.g.*, Douglas Lichtman, *How the Law Responds to Self-Help*, 1 J.L. ECON. & POL'Y 215, 228 (2005).

And if the point is to induce innovation, the RPR's effect likely remains minimal: in most cases, the main issue is whether cost-effective precautions are available (innovate), not whether the law will recognize them.[280]

The situations in which the RPR *would* incentivize deceptive precautions is quite limited. There may be an effect if a less expensive deceptive option and a slightly more expensive non-deceptive option are incompatible, or using both would be superfluous. If the RPR only recognizes the non-deceptive option, the company may choose the non-deceptive option to preserve its ability to litigate. But if the RPR recognizes both, the company will choose the deceptive option. In that sense, the RPR may, at the margin, incentivize lying (and free up capital for innovation).[281]

But if the non-deceptive precaution is insufficiently protective or the deceptive precaution is extremely effective (e.g., deception technology), the company will *still* adopt the deceptive precaution to preserve its information asset, regardless of what the law says.

Interestingly, the RPR's main incentive effect is not on the choice about whether to use cost-effective deceptive precautions, but about what additional *non-deceptive* security measures to take. If the law accepts the deceptive precaution in satisfaction of the RPR, then the company will adopt only the deceptive precaution and not the non-deceptive precaution. But if the law does not accept the deceptive precaution in satisfaction of the RPR, then the company will adopt *both* the deceptive and non-deceptive precautions (or forego litigation). That is, if the RPR does not recognize deceptive precautions, some companies will spend *more* on security than they otherwise would.[282]

Permitting deceptive precautions is thus consistent with a primary goal of trade secret law, of minimizing overinvestment in security.[283] And, given the difficulty of sustaining a ruse over the long term, the reliance on deceptive precautions may ultimately contribute to the leakiness of secrets, something that is cited as another advantage of the trade secret regime.[284] The behavior that is *incentivized*—avoiding wasteful expenditure—is (arguably) good; to get there, the law must *recognize* lying as a legitimate option.

Although most focus on the law's incentives, the expressive force in this realm is more stunning: It reveals the depth of law's treatment of permitted lies. And it is of particular concern for theoretical reasons. We turn to these issues in Part III.

III. RESISTING LIES

The claim that law legitimates lying may elicit a strong reaction that the law cannot be this way. Although some scholars have argued that the law, *de facto*,

---

[280] *See id.* at 227–29.

[281] In this sense, there is an incentive story to tell. But it is about innovation, and not about incentives to lie.

[282] *See* Lichtman, *supra* note 278, at 230.

[283] *See id.* at 230-31.

[284] *See* Lemley, *supra* note 135, at 332–37 ("[T]rade secret law actually encourages broader disclosure and use of information, not secrecy.").

incentivizes lying by placing people in impossible situations[285] or by permitting lies where efficient or difficult to stop (rightly or wrongly),[286] my claim takes it a step further. My claim is that the law *de jure* recognizes lying by accepting certain lies in satisfaction of a legal requirement. It is not, or at least not merely, about incentives.[287]

Skepticism about the law's ability to legitimize lies tends to take one of several forms. The first move is to deny that these deceptive practices are in fact lies. This strategy fails: the case study's examples present or imply falsehoods in warranting contexts, and so are lies on almost any definition, including BLACK'S.[288] But even if the strategy succeeds, it does so only in a trivial way: I will still have shown that the law de jure accepts *the fact that deception was used* as fulfilling a legal requirement.

The other skepticisms are more theoretical. One proceeds by suggesting the law's legitimization of lies conflicts with the law's commitment to truth. Yet another appeals to a natural-law style Argument from Morality. Finally, an entirely different sort of skeptic, about the import of my claim, might wonder why anyone would find the claim anything but obvious, or at least, anything but an incremental contribution to the efficiency story about permitted lies.

This Part challenges the bases for these theoretical skepticisms. Exploring their limits shows that the case study is not a niche curiosity. The phenomenon, of law legitimizing lies, has much broader implications about the law's response to lying, including why it may be good that so many resist recognizing certain examples as lies.

A. The Law's Commitment to Truth

A belief in the law's commitment to truth is almost universal, at least as an ideal of what the American legal system is or aspires to be (the "commitment").[289] This commitment has often been invoked in the wake of the capitol riots, highlighting its importance, actual or perceived.[290] But what should we think about this commitment, if the law sometimes legitimizes lies?

The most immediate question is what the phenomenon—of law legitimizing lies—can tell us about what the commitment means for theorizing

---

[285] *Cf.* Eskridge, *supra* note 275, at 254, 256.

[286] *See, e.g.*, Levmore, *supra* notes 17, 46, at 1369; Simon-Kerr, *supra* note 58 at 2175.

[287] *Supra* Part II.D.

[288] *Supra* Parts I.B, II.B. The objection that some of the examples do not invite reliance confuses warranting contexts with the existence of reliance interests. *Infra* Part III.B.

[289] *E.g.*, United States v. Havens, 446 U.S. 620, 626 (1980) ("There is no gainsaying that arriving at the truth is a fundamental goal of our legal system."); Susan Haack, *Of Truth, In Science and Law*, 73 BROOK. L. REV. 985, 986 (2008) ("Nevertheless, truth is surely *relevant* to legal proceedings, for we want, not simply resolutions, but *just* resolutions; and substantial justice requires factual truth."); *see also* Hon. Sandra L. Lynch, *Constitutional Integrity: Lessons from the Shadows*, 92 N.Y.U. L. Rev. 623, 636 (2017).

[290] *E.g.*, Timothy Snyder, *The American Abyss*, N.Y. TIMES (Jan. 9, 2021), https://www.nytimes.com/2021/01/09/magazine/trump-coup.html.

the law's response to lying. Because lies and deception often undermine the truth, a commonly assumed corollary of the law's commitment is that the law generally disfavors lies and deception, making exceptions only for reasons of administrability, immateriality, or the First Amendment (the "anti-lie corollary").[291] This anti-lie corollary is somewhat controversial[292] and perhaps unlawful,[293] but the trend favors the corollary.[294] It comes down to defaults: Is law's default setting to disfavor lies, and make exceptions by permitting certain ones? Or is the law generally neutral, despite its supposed commitment to truth, picking out certain lies and deceptions to police? And which default *should* the law adopt given the commitment to truth?

The anti-lie corollary has strong intuitive appeal as a descriptive and normative matter.[295] Criminal prohibitions of deception are staggeringly plentiful.[296] Most jurisdictions recognize a common law tort for misrepresentation.[297] Civil causes of action for various types of deception abound, whether about people (e.g., defamation) or products (e.g., false advertising).[298] Deception satisfies the "improper conduct" elements for some torts, including trade secret misappropriation.[299] The law often deprives deceivers of advantages gained through deception: Fiction is copyrightable, but fiction presented as facts is often not.[300] And fraud vitiates consent, consent which would otherwise be available as a defense to torts like battery or trespass.[301]

There are, of course, exceptions. The tort of misrepresentation was originally very narrow, and courts have been slow to extend it, especially in

---

[291] *See* Spaulding, *supra* note 1, at 96 ("If deception is not condemned, it is denied, and when it can't be denied it is framed either as a necessary evil or a deviant practice of bad lawyers."); MacIntyre, *supra* note 39, at 311–12; Porat & Yadlin, *supra* note 23, at 624.

[292] *See e.g.*, Porat & Yadlin, *supra* note 23, at 624.

[293] *See* United States v. Alvarez, 567 U.S. 709, 718 (2012) ("Absent from those few categories where the law allows content-based regulation of speech is any general exception to the First Amendment for false statement.").

[294] *See, e.g.*, SHIFFRIN, *supra* note 25, at 123; HASDAY, *supra* note 25, at 20; Manta, *supra* note 52, at 216; Smith, *supra* note 25, at 214; *cf.* Genevieve Lakier, The Invention of Low-Value Speech, 128 HARV. L. REV. 2166, 2216 (2015).

[295] *E.g.*, Porat & Yadlin, *supra* note 23, at 624 (observing the "almost-general prohibition of lying").

[296] *See* Stuntz, *supra* note 261, at 517–18.

[297] RESTATEMENT (FIRST) OF TORTS § 525 (1938).

[298] *See, e.g.*, Knafel v. Chicago Sun-Times, Inc., 413 F.3d 637, 640 (7th Cir. 2005) (defamation); Merck Eprova AG v. Gnosis S.p.A., 760 F.3d 247, 255-56 (2d Cir. 2014) (false advertising).

[299] *See* UNIFORM TRADE SECRETS ACT § 1(1)–(2) (misappropriation includes procurement by fraud).

[300] *See generally* Smith, *supra* note 25.

[301] *See* Desnick v. Am. Broad. Cos., 44 F.3d 1345, 1351–52 (7th Cir. 1995) (collecting cases); *see also* Barbara A. v. John G., 193 Cal. Rptr. 422, 431 (Ct. App. 1983) (collecting cases).

non-commercial settings.[302] Some courts declined—at least for a time—to find liability for misrepresentations concerning HIV-status [303] or birth control.[304] Similarly, the law sometimes "give[s] effect to consent procured by fraud,"[305] as where seduction is "effected by false promises of love" (not battery)[306] or where "testers" document "evidence of housing discrimination" by "pos[ing] as prospective home buyers" (not trespass).[307] Patent law, which long excluded deceptive inventions, now accepts them, [308] and patents themselves are often deceptive, with some permissibly claiming inventions that do not yet exist.[309]

What makes the difference? A few themes make for plausible exceptions. One might argue that courts make exceptions and permit deception, including affirmative misrepresentations, where necessary for socially valuable enterprises, like testers and investigative reporting.[310] Alternatively, maybe courts permit deception where the truth-teller and the deceiver look alike, like busybodies posing as prospective buyers at open houses.[311] The law also narrowly construes lies so as to excuse deception where some amount of gamesmanship is inevitable (e.g., perjury).[312]

Legitimizing lies creates an uneasy tension with this picture. Most of the above examples merely tolerate lies. They are true exceptions—excepting permitted lies from punitive consequences that would otherwise apply. Not so, with the trade secret case study. It shows that the law can and does go beyond merely permitting. The lies at issue in the case study were already permitted; trade secret law takes the further step of legitimizing and possibly requiring them.[313]

---

[302] *See* Laura Barke, Note, *When What You Don't Know Can Hurt You: Third Party Liability for Fraudulent Misrepresentation in Non-Commercial Settings after* Doe v. Dilling, 34 S. ILL. U. L. J. 201, 202–04 (2009); *see also* United States v. Neudstadt, 366 U.S. 696, n.26 (1961) (citing Prosser, *Remedies for Misrepresentation*, TORTS § 85, at 702–03 (1941)).

[303] *See* Doe v. Dilling, 888 N.E.2d 24, 40 (Ill. 2008).

[304] *See, e.g.*, Stephen K. v. Roni L., 164 Cal. Rptr. 618, 621 (Ct. App. 1980); Welzenbach v. Powers, 660 A.2d 1133, 1136 (N.H. 1995); *see also* Barke, *supra* note 302, at 209–10 & n.63 (collecting cases).

[305] Desnick v. Am. Broad. Cos., 44 F.3d 1345, 1351–52 (7th Cir. 1995) (collecting cases).

[306] *Id.* at 1352 (citing Pletnikoff v. State, 719 P.2d 1039, 1043 (Alaska Ct. App. 1986)).

[307] *Id.* at 1353 (citing Northside Realty Assocs., Inc. v. United States, 605 F.2d 1348, 1355 (5th Cir. 1979)).

[308] *See* Juicy Whip Inc. v. Orange Bang Inc., 185 F.3d 1364, 1366-68 (Fed. Cir. 1999).

[309] *See generally* Janet Freilich, *Prophetic Patents*, 53 U.C. DAVIS L. REV. 663 (2019); Janet Freilich and Lisa Larrimore Ouellette, *Science Fiction: Fictitious Experiments in Patents*, 364 SCIENCE 1036 (2019).

[310] *See, e.g.*, Desnick, 44 F.3d at 1353-54.

[311] *See id.* at 1351, 1353

[312] *See* Stuntz, *supra* note 261, at 517–18.

[313] *But see supra* Part II.C.

I mentioned that there is an alternative way to view these cases, and the phenomenon of legitimizing lies counts in its favor. Rather than beginning with the assumption that the law generally disfavors (or should disfavor) deception and asking why the law makes certain exceptions, one might begin with the opposite assumption: the law takes no principled stance on deception (the "neutral view"). Proponents of the neutral view believe that the anti-lie corollary gets the defaults wrong, as a descriptive or normative matter.[314]

The neutral view has an appealing simplicity. Under the neutral view, when the law penalizes lying or deception, it is because the law has picked out that channel of communication to protect. Some protected channels are those where lies produce direct harms: lying about STDs harms more than the target.[315] Other channels involve social practices that depend, for their effectiveness, on truthfulness (e.g., perjury). Finally, misinformation in some circumstances generates waste. Many commercial deceptions do not add value, but merely transfer value from one party to another while increasing costs (parties must pay to defend against deception).[316] And deceptive advertising not only harms deceived consumers, but also decreases the quality of goods available.[317]

In all other situations, the law remains neutral about lying. As a normative matter, this reflects a judgment that other measures are better suited to protect against the harms of lies. Such justifications have a strong pedigree and are repeatedly cited: "[T]he remedy to be applied is more speech, not enforced silence."[318] "[T]he best test of truth is the power of the thought to get itself accepted in the competition of the market."[319] They are also practical: "a healthy skepticism is a better protection against being fooled . . . than the costly remedies of the law."[320]

But if these are the only justifications for the neutral view, the only real value-add is its simplicity: the anti-lie corollary arguably permits roughly the same lies, by making exceptions for similar reasons. And some of these justifications for the neutral view—that more speech is the cure, that the marketplace of ideas will prevail—seem discredited by the infodemic and other misinformation online.[321]

The trade secret case study presented here counts strongly in favor of the neutral view. Unlike the anti-lie corollary, the neutral view readily accommodates other responses to lying beyond the traditional dichotomy of

---

[314] *See e.g.*, Levmore, *supra* note 17; *see also* Desnick, 44 F.3d 1345 (Posner, J.).

[315] *Cf.* Mussivand v. David, 544 N.E.2d 265 (Ohio 1989).

[316] *Cf.* Rockwell, 925 F.2d at 178 (characterizing trade secret law as deterring "efforts that have as their sole purpose and effect the redistribution of wealth from one firm to another"); Lemley, *supra* note 135, at 333–34.

[317] *See* Klass, *supra* note 13, at 725–26.

[318] Alvarez, 567 U.S. at 728 (Kennedy, J.) (quoting Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring)).

[319] *Id.* (quoting Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting).

[320] Desnick, 44 F.3d at 1354.

[321] *See, e.g.*, Matteo Cinelli, Walter Quattrociocchi, Alessandro Galeazzi, et al., *The COVID-19 Social Media Infodemic.* 10 SCI. REP. 16598 (2020).

penalizing and permitting. The neutral view is neutral, and so if it serves one of law's aims to legitimize certain lies as "reasonable," no tension is created if the law does so.

The trade secret case study provides a nice example of how, under the neutral view, the law can treat lying as a mere tool—i.e., a tool without any moral valence. Recall that one of the law's aims is thought to be avoiding waste—avoiding transfers that impose costs without adding value.[322] Both the neutral view and the anti-lie corollary can accommodate the law's penalizing lies where they lead to waste, and permitting lies where they do not.[323] And so both are consistent with the lies from the case study being permitted: lying to an employee about a codename or using fake data to stimy hackers does not—in the central case—cause a reliance that would lead to "mere transfer" of resources from the respective targets to those using deceptive precautions; that is neither the purpose nor the effect of any deception.

But these lies also help *prevent* waste. Avoiding such transfers is their precise aim. On the neutral view, the law can legitimize this use, and in so doing, strengthen the anti-waste measures: as discussed earlier, recognizing deceptive precautions as satisfying the RPR prevents wasteful overinvestment in security.[324] The anti-lie corollary, by contrast, seems inconsistent with the express recognition.

Another example: Many of the deceptive precautions do not undermine channels of communication that the law has picked out as requiring protection. To the contrary, many of the deceptive precautions, like deception technology, proactively *defend* such channels by, e.g., securing the network and identifying bad actors. These practices *sacrifice* the reliability of some channels to promote the reliability of others. The neutral view can readily promote and reinforce this. The anti-lie corollary cannot, absent some further explanation.

The case study thus counts in favor of the neutral view, as a descriptive matter: it provides a data point best explained by the neutral view, and it demonstrates that the neutral view can be consistent with the commitment to truth—perhaps more so than the anti-lie corollary. The latter might also provide a reason to favor the neutral view as a normative matter, insofar as the commitment to truth is a real value. Two, maybe three, strikes against the corollary, at a time when the main argument against the corollary—that the remedy for false speech is more speech—appears under attack.

B. Against the Argument from Morality

Some skeptics of the claim that law legitimizes lying may resist the conclusion through an appeal to commonsense morality (call this the "Argument from Morality"). The Argument from Morality fails, but evaluating why the argument fails demonstrates the potential breadth of the phenomenon—because it would fail against more than just protective lies like the case study—and provides some benchmarks for a theory moving forward.

---

322 *See supra* notes 316–317 and accompanying text.

323 *See id.*

324 *Supra* Parts II.A & II.D.

The Argument from Morality is really a collection of arguments that, roughly, the law cannot legitimize lies because of lying's moral status. It has the flavor of a broadly equitable objection.[325] In its simplest form, the Argument from Morality contends that lies are immoral and therefore cannot constitute legitimate options for satisfying legal requirements. This version depends on two assumptions: (1) What is immoral cannot be *legitimized* by law (even if it might be permitted). And (2) All lies are immoral. Obviously, this is a strawman. No one seriously contends that the law does not legitimize immoral actions. And very few seriously contend that *all* lies are immoral.[326] Still, the strawman version illustrates the general structure that arguments from morality will take.

The strawman Argument from Morality can be strengthened in various ways. The first premise, about what the law can and cannot legitimize, may be weakened. It could say that, *in certain contexts*, the law cannot legitimize what ordinary morality generally prohibits. Trade secret law makes for a good case study, because trade secret law would have at least as strong a claim as any to being such a context. Though part of intellectual property,[327] trade secret law is really a species of "unfair competition"[328] and there is a long tradition of treating trade secret law as a codification of commercial good faith.[329]

The strawman argument could also be strengthened by weakening the second premise. We could reject the extreme view that *all* lies are immoral, relying instead on *ordinary* morality's *general* prohibition against lying.

But even so strengthened, the Argument from Morality still fails. The problem is that a general prohibition admits of exceptions or gray areas, and the trade secret case study offers numerous examples that fall within them. At minimum, the moral status of such precautions is open to question. And while the law might prohibit that which morality generally prohibits, the law is and generally should be cautious about importing specific applications of purely moral principles, particularly where the moral status of a principle or its applications is disputed.

In evaluating the Argument from Morality, the moral question is thus more limited than the larger debate over whether lying and deception are generally wrong. Rather, the question is: whatever the general moral status of lying or deception, what is the moral status of the particular deceptive practices at issue? Specifically: in these cases, is it permissible for the agent to cause, or take steps that will in part cause, the target (a) not to form a true belief (i.e., deny the target a relevant true belief); or (b) to have or form a false belief ?

The project of this section is largely descriptive, not normative. The question is still: *Can* the law legitimize lying despite the Argument from

---

[325] As contrasted with narrow equitable grounds, which do not foreclose the phenomenon. *See supra* Part II.C.

[326] There is a cottage industry criticizing Kant on these grounds, else trying to save him from the absolutist view. Kant, *supra* note 41, at 605, 607; Korsgaard, *supra* note 41, at 325–27.

[327] *See, e.g.*, Lemley, *supra* note 135, at 312–14.

[328] *See* Hrdy and Lemley, *supra* note 111, at 15-17.

[329] *See* RESTATEMENT (FIRST) OF TORTS § 757 (1939).

Morality? That is, could the Argument from Morality ground any kind of broadly equitable objection that the law's legitimization of lies is somehow legally invalid or that the decisions in the case study were wrongly decided? This is a descriptive question, even if it turns on normative questions about the moral status of lying. This section does *not* address the questions: *Should* the law legitimize lying? Or *should* trade secret law be this way? Those "should" questions are normative—about whether such laws would be good ones. We begin turning to the normative in Part III.C.

1. Methodology

There are two general approaches to determining whether a specific lie or deceptive practice is (morally) permissible. The first considers what generally makes deceptive practices wrong, and evaluates whether those features ("wrongmakers") are present in particular cases. This approach does *not* assume there to be a general moral prohibition against lies or deceptive practices, even though (1) it may be the case that many if not most such practices are morally impermissible and even though (2) it may also be the case that it would be better for individuals to *believe* there to be such a general prohibition (even if there is not).[330] The second approach takes deception to be generally prohibited, considers what features justify exceptions (if any), and evaluates whether particular practices fall within those exceptions.[331]

This Article follows the first approach.[332] However, before turning to that analysis, I address why the exception for "protective lies" does not straightforwardly apply to the case study.

2. The Exception for Protective Lies

At the outset, I set aside a notable and generally agreed[333] exception to the prohibition against lying: the exception for protective lies.[334] I address it first both because deceptive precautions are protective lies of sorts, and because even stricter moral theories often recognize the exception. If the exception applies to a significant number of deceptive precautions, then the Argument

---

330 *See, e.g.*, SIDGWICK, *supra* note 39, at 488-89.

331 *See, e.g.*, BOK, *supra* note 42, at 13-14, 18. The Kantian approach might be viewed under either lens, but falls more naturally under the second. *E.g.*, Korsgaard, *supra* note 41; *see, e.g.*, *id.* at 341–48 (suggesting a double-level theory may forbid lying under ideal conditions but permit lying under non-ideal ones). Shiffrin recently developed a similar Kantian framework, but appears to make an exception for the sorts of lies at issue here (but denies that they are lies). *See* SHIFFRIN, *supra* note 25, at 153.

332 *Cf.* United States v. Alvarez, 567 U.S. 709, 719 (2012) (Kennedy, J.) (rejecting categorical approach to false speech).

333 The existence of the exception is generally agreed, though its scope is not.

334 *See e.g.,* Allen, *supra* note 52, 162 & n.2 (discussing "the widespread moral belief and religious doctrine that lying sometimes is a morally justifiable response to others seeking information to which they have no right"); SHIFFRIN, *supra* note 25, at 153 (suggesting some claims made for privacy do not count as lies, but without further explanation); Shiffrin, *supra* note 99, at *16 (similar).

from Morality almost certainly fails. But as will be discussed, the exception does not apply.

A defense of protective lies traditionally begins with the murderer at the door: A murderer at the door asks whether his intended victim "has taken refuge in our house" (they have) and we "cannot evade an answer of 'yes' or 'no.'"[335] May we lie to protect the intended victim?[336] Kant infamously argued that, even under such extreme circumstances, the answer is still no: one is not permitted to lie.[337] But this is an obviously inhumane result. The example is so compelling that Kant's critics argue the result undermines his entire theory, while Kant's defenders argue Kant made a mistake, that his theory is not in fact committed to such an extreme position.[338]

The example has several features thought to warrant an exception.[339] The murderer at the door is an evil-doer. The information sought would be used to seriously harm another. Lying is necessary to conceal that information and so is necessary to protect the other person from serious harm.[340] The murderer seeks to use the would-be liar as a tool for furthering the evil scheme, and lying is the only way to avoid becoming complicit.[341] These features are important on most views for explaining why lying under such circumstances is permissible and possibly required. But these features are *critical* for justifying the exception on stricter, nonconsequentialist views.

For example, Korsgaard explains how even Kant's otherwise unyielding theory can accommodate this example: Kant's Formula of Universal Law requires that a person act only on maxims they could will to be universal law.[342] Many commentators had thought this doomed Kant, because they could not will a maxim of lying to a murderer at the door to be universal—the lie would no longer be effective.[343] But as Korsgaard explains, the murderer would not reveal his motives. Rather, the murderer "must suppose that you do not know who he is and what he has in mind," otherwise you would not help him.[344]

---

335 Kant, *supra* note 41, at 611.

336 *Id.*

337 Or, at least, has commonly been taken to argue. *See* Helga Varden, *Kant and Lying to the Murderer at the Door… One More Time: Kant's Legal Philosophy and Lies to Murderers and Nazis*, 41 J. SOC. PHIL. 403, 406 (2010) (arguing that this "traditional interpretation" is "mistaken").

338 *See* Korsgaard, *supra* note 41, at 326–28; *see also* Varden, *supra* note 337, at 405.

339 *See also infra* Part III.B.4.a.

340 Korsgaard, *supra* note 41, at 340; *see also* BOK, *supra* note 42, at 107-09; SHIFFRIN, *supra* note 25, at 35–36.

341 Korsgaard, *supra* note 41, at 340 (identifying self-respect as a second reason to lie to the murderer).

342 *Id.* at 328–330.

343 *Id.*

344 *Id.* at 329. Korsgaard fights the hypothetical. *See id.* at 330. As even she acknowledges, if "the murderer does, contrary to [her] supposition, announce his real intentions[,] [t]hen [her] arguments . . . do not apply." *Id.* at n.4 ("In this case, I believe your only recourse is refusal to answer (whether or not the victim is in your house, or you know his whereabouts)."). This does not affect our interest in the case, which is that the murderer's bad actor status is *critical* to the existence of the exception.

Because of this, your lie will work, even if anyone would lie under such circumstances: "the murderer supposes you do not know what circumstances you are in—[] that you do not know you are addressing a murderer—and so does not conclude from the fact that people in those circumstances always lie that *you* will lie."[345] She concludes that, under the Formula of Universal Law, "[i]t is permissible to lie to deceivers in order to counteract the intended results of their deceptions, for the maxim of lying to a deceiver is universalizable."[346] But critically, this is because the murderer "has . . . placed himself in a morally unprotected position by his own deception."[347]

Korsgaard similarly reconciles the murderer at the door with Kant's Formula of Humanity—the imperative that one treat others only as an end, never as *mere means*. On her telling, the Formula of Humanity best explains why Kant found lying "so horrifying"—"it is a direct violation of autonomy."[348] One can never assent to lying: either one does not know of the lie (e.g., a false promise to repay) and so cannot assent, or else does know, and so assents to what the liar seeks (a handout), not what the liar proposes (a loan).[349] But for the same reason, the Formula of Humanity provides terms that can be used to "give an account . . . of what vindicates lying to a liar."[350] Specifically, "[t]he liar tries to use your reason as a means—your honesty as tool."[351] And "[y]ou do not have to passively submit to being used as a means."[352] But again, critically, lying to the murderer at the door is a departure from the ideal because of the murderer's own deception. In such circumstances, "but only then," does ideal theory yield.[353]

The difficulty is that trade secret law does not assume deceptive, or even bad, actors. Reasonable precautions must be taken to shield the trade secret from *all* actors. Fake source code is published to the world; false endings to a series to anyone who might look; car disguises to anyone who is passing by. These methods protect the secret as against illegitimate and legitimate corporate diligence alike. The exception for protective lies—for lying to a liar—does not straightforwardly apply and so does not provide an easy answer to our question about the moral status of these precautions. We are better looking elsewhere.

3. Against Global Wrongmakers

We turn to what makes lying wrong without assuming a more general prohibition against lying. One plausible explanation is that lies cause harm. Such harms fall into two categories: The first are harms caused by imparting

345 *Id.* at 329–330 (emphasis in original).
346 *Id.* at 330.
347 *Id.*
348 *Id.* at 334.
349 *Id.* at 332.
350 *Id.* at 338.
351 *Id.*
352 *Id.*
353 *Id.* at 349.

false beliefs. The second are harms to trust.[354] Each can affect more than the deception's target: false beliefs may be shared, and societal trust undermined. Whether a deceptive practice is wrong depends, at least in part, on whether it would lead to these harms, individually or in aggregate.[355]

Another plausible explanation is the Kantian one, that lying and deception use others as mere means. This explanation has force and may be a reason why the law *should not* legitimize lying.[356] But this type of explanation generally does not support the Argument from Morality. The law is generally not so strict—it is not Kantian—and importing non-harm-based moral reasons is generally cabined to those areas of the law that directly involve dignitary harms (and even then, is regrettably controversial).[357]

Before addressing particular deceptive practices, and whether they present these wrongmakers,[358] it is worth sketching briefly why we should not assume that deceptive practices (or, more particularly, lying) always generate these harms,[359] or have an aggregate effect that warrants a *rule* against such acts.[360] I do not aim to prove why there is not a general prohibition against lying; I have assumed that there is not. But these arguments are common enough that it may be helpful to the reader to gesture at common mistakes underlying them before turning to why wrongmakers are not present or might be mitigated with respect to particular deceptive precautions (Part III.B.4).

a. Harms from False Beliefs

A false belief will not always harm a target, unless false beliefs are always bad.[361] But it is not clear that all false beliefs have such disvalue; that would,

---

354 *See* SIDGWICK, *supra* note 39, at 485. There is a third potential harm, namely, that the target might take offense (i.e., "feel bad") if they discover that they were deceived or duped. But, for better or worse, the law generally does not protect against purely emotional harms.

355 This manner of reasoning, based on the effects of a particular action, is generally considered consequentialist. But considering harms is also central to many other styles of ethical reasoning. *See generally, e.g.*, TIMOTHY SCANLON, WHAT WE OWE TO EACH OTHER (2000); DEREK PARFIT, ON WHAT MATTERS (2011). For an illuminating discussion of the limits to nonconsequentialist approaches, see Barbara H. Fried, *The Limits of a Nonconsequentialist Approach to Torts*, 18 LEG. THEORY 231 (2012).

356 *Infra* Part III.C.

357 *See* Austin Sarat, Haley Cambra, Sarah Smith, & Olivia Truax, *Law and Lies*, *in* LAW AND LIES, *supra* note 1, at 1, 2; Kenneth S. Abraham & G. Edward White, *The Puzzle of Dignitary Torts*, 104 CORNELL L. REV. 317 (2019). *But compare* Ernest J. Weinrib, *Understanding Tort Law*, 23 VAL. U. L. REV. 485 (1989) (developing deontological theory of torts), *with* Robert L. Rabin, *Law for Law's Sake*, 105 Yale L.J. 2261, 2269–83 (1996) (book review) (attacking Kantian foundations of Weinrib's view).

358 *Infra* Part III.B.4.

359 KAGAN, *supra* note 38, at 107; SIDGWICK, *supra* note 39.

360 *See* MILL, *supra* note 39, at 22–23.

361 Roughly, something that is "intrinsically" good is something that is valued for its own sake. *See* MILL, *supra* note 39 at 28–29. By contrast, something is

in part, depend on true beliefs being intrinsically good. Although knowledge is often recognized as an end-in-itself, this does not mean that all knowledge is valuable. Some true beliefs are trivial, like the knowledge that Miley Cyrus's favorite color is purple.[362] For most people, such knowledge is morally irrelevant, unless instrumental to some further end, like the pleasure of celebrity gossip. Indeed, the internet makes painfully clear that not all knowledge is valuable.

The more plausible claim is that false beliefs are *instrumentally* bad because an individual acting on false beliefs makes worse decisions. But this claim is also false: some false beliefs are instrumentally good, like beliefs in false deadlines (for spurring writing) or in lucky charms (for instilling courage). Other false beliefs are instrumentally neutral. And some true beliefs are instrumentally bad, as where a patient's recovery could be jeopardized by learning the truth about their situation.[363]

Whether a false belief harms the target, then, is contingent. It depends on the moral significance of the belief's content; any emotional reaction to the belief; and the number and significance of the decisions to which the belief is relevant (what the law calls "materiality").

But potential harm is not limited to the initial target. False beliefs spread. And poor decisions based on false beliefs can similarly cause harm. These harms must also be evaluated. Although similar considerations apply, the analysis is harder as it involves, e.g., determining whether, how, and to whom the misinformation will spread.[364] Even so, harm remains contingent. There are some false beliefs—like about Miley Cyrus's favorite color—that are unlikely to be harmful.

One difficulty remains: even if harm is contingent, it is frequently objected that would-be liars are not well positioned to evaluate whether their lies are likely to produce harm, and, worse, may overestimate their predictive capacity.[365] But the cost and likelihood of error is also contingent. And the question remains whether measures could be taken to reduce the cost and

---

"instrumentally" good when it "contribute[s] to producing other goods (or eliminating various bads)." *Id.* Although some things may be both intrinsically and instrumentally good, others may only have moral value insofar as they are instrumentally valuable. *Id.*

362 *What is Miley Cyrus's Favourite Colour?*, ANSWERS (2013), wiki.answers.com/Q/What_is_Miley_Cyrus's_favourite_colour (visited Sept. 28, 2013). If you think this knowledge has value, you should fact check. The author did not consider it important to confirm.

363 This type of example has motivated the other major exception to a general prohibition, the exception for benevolent lies. *See* SAUL, *supra* note 14 at 69-71; *see also generally* Thomas E. Hill, 18 J. VALUE INQUIRY 251 (1984).

364 The manner of spreading ("how") may matter because misinformation forwarded in "warranting contexts" is likely more harmful than if spread through "non-warranting contexts" like rumor mills.

365 *See* William H. Simon, *Virtuous Lying: A Critique of Quasi-Categorical Moralism*, 12 GEO. J. LEGAL ETHICS 433, 437-38 (1999); Helen Norton, *Lies and the Constitution*, 2012 SUP. CT. REV. 161, 186-87 (2013).

likelihood of error, as tort law arguably does for other (non-deceptive) precautions.[366]

b. Harm to Trust

Another commonly suggested reason why deception is generally morally problematic is that it undermines the trust needed for society to function. Recent events notwithstanding,[367] there is reason to be skeptical of this claim.

First, empirical evidence about the actual pervasiveness of lying seems to count against this.[368] If recent events suggest there is a breaking point, it has been a long time coming. And the trade secret case study provided many examples of lies that secure the reliability of channels—examples of lies that are trust-enhancing.[370]

Second, it is also not necessarily a social bad for individuals to be wary of being deceived. As Sidgwick points out, sometimes it is the desired result:[371] wariness is good where it deters would-be thieves. Similarly, in legitimately secretive enterprises, it might be better for individuals to be aware that information they receive may be incomplete or contain minor inaccuracies. Deception will only be effective where identifying the deceptions is difficult.[372] But deceptive precautions, including lies, need not deceive to be effective,[373] and where they do, such deception may be temporary.[374] A general awareness that deceptive practices may be used could go a long way towards allowing individuals to protect themselves by tempering the reliance they place on information in making decisions.

4. Mitigated Wrongmakers

Having identified the primary wrongmakers—harms from false belief and harms from trust—and having gestured at why such wrongmakers are not present in all cases, we turn to whether there is a core set of legitimized lies that are likely morally unproblematic—or, at the least, whose impermissibility is sufficiently disputed. The goal is not to show that *any* legitimized lie is permissible. Rather, I argue that a core set is unlikely to lead to these harms,

---

366 *See* Stanley Ingber, *Rethinking Intangible Injuries: A Focus on Remedy*, 73 CALIF. L. REV. 772, 793-94 (1985); *supra* Part II.C.

367 It is difficult to summarize the current zeitgeist in a footnote. For the benefit of future readers, this Article was completed in the aftermath of the 2020 U.S. presidential election in which President Joseph Biden was elected, then-President Donald J. Trump maintained that there was electoral fraud despite repeated debunking of these claims, and a mob of Trump supporters overran the U.S. Capitol in an unsuccessful attempt to overturn the election by force. *Cf.* Jeremy Waldron, *Damned Lies*, NYU School of Law, Public Law Research Paper No. 21-11 (March 3, 2021), https://ssrn.com/abstract=3797216.

368 *See* MacIntyre, *supra* note 39, at 318–22 (collecting statistics); *see also* BERNARD WILLIAMS, TRUTH AND TRUTHFULNESS 85 (2002); SIDGWICK, *supra* note 39, at 318.

370 *See supra* Part II.

371 SIDGWICK, *supra* note 39, at 318.

372 *See id.* at 318-19 (explaining how deceit is "necessarily self-limiting").

373 *See supra* Parts I.B, II.B.

374 *See supra* Part II.B.1.

such that they are likely morally permitted or, at least, are not clearly impermissible. Neither judgment justifies treating the legitimized lies differently from other, nondeceptive practices that may play on another's reason or otherwise risk harm. If enough such examples exist, then the gray area of deceptive practices is significant enough that the moral status of such acts cannot support the Argument from Morality against legitimizing them.

Our discussion uses examples from the trade secret case study, but provides a framework that is generalizable moving forward. These examples share several features that affect whether a particular deceptive practice is likely morally permissible or at least within this gray zone: where the deceptive practice exhibits an *entrapment structure*; where the content of the deceptive practice is *not material*; where trust in a given context is *inappropriate*; where the target lacks a *reliance interest* in what is said or implied; and where *signaling* mitigates risk of harm. A deceptive practice need not have all these features to be permissible. Similarly, some deceptive practices may have all these features, but still be impermissible. My goal is only to show that a sufficient number of deceptive practices are arguably permissible such that the Argument from Morality fails. (This is different from the all-things-considered questions of whether the law *should* legitimize lies and whether trade secret law *should* function this way, questions to which we return, briefly, in Part III.C.)

a. Entrapment Structure

Begin with a common example: fake entries designed to catch copycats and moles. Sometimes called "Mountweazels"—after Lillian Virginia Mountweazel, a fictional photographer in THE NEW COLUMBIA ENCYCLOPEDIA—this method of IP self-help enjoys a long history that continues today.[375] Recent examples include "esquivalience," which caught Dictionary.com's copying of THE NEW OXFORD AMERICAN DICTIONARY (2001 ed.), and "hiybbprqag," which caught Bing's copying of Google search results.[376] Variants on this precaution are increasingly common in computer security, including honeypots, honeynets, and increasingly sophisticated forms of deceptive technology.[377]

Different variants have different targets: Some, like Mountweazels, are released to the world at large, and others, like fake authentication data, only to users on a company network. So let's begin with a narrower, stylized version,

---

[375] *Mountweazel, Lillian Virginia*, THE NEW COLUMBIA ENCYCLOPEDIA (William H. Harris and Judith S. Levey, eds. 1975); Eleanor Williams, *Unclear Definitions: Investigating Dictionaries' Fictitious Entries through Creative and Critical Writing* 15, 20 (April 16, 2016) (unpublished manuscript), https://pure.royalholloway.ac.uk/portal/en/publications/unclear-definitions-investigating-dictionaries-fictitious-entries-through-creative-and-critical-writing(56281366-fd07-4ec9-adf5-d254d81be9cd).html.

[376] Williams, *supra* note 375, at 16–18.

[377] *Id.*; *supra* Part II.B.

targeting particular individuals through the use of fake codenames—a type of precaution sometimes called a "Canary Trap."[378]

Suppose that Yosef starts work on a top-secret project, for which Yosef (and only Yosef) is given the fake codename "Canary." Other employees, who work separately from each other and Yosef, are each given their own codename (*e.g.*, "Hummingbird," "BlueJay"). If anyone leaks, the manager will know there was a leak—and its source. To avoid complications about whether mislabeling is a direct lie or merely misleading, we can consider two versions: one where a manager *tells* Yosef that "the product's codename is 'Canary,'" and one where no one *tells* Yosef the code name, but he reasonably infers it based on labels and actions (e.g., he is given files labeled "Canary"; his manager asks about "Canary's status"). Call the first case, with a direct lie, "Canary," and the second, "Canary*."

The *Canary* cases exhibit an *entrapment structure*: they have been designed so that the only risk of harm from the false belief is *to* a bad actor *through* that bad actor's own actions. Assuming that Yosef does not share that he is working on "Canary," he is unlikely to be harmed by his false belief about the codename. Yosef's false belief is only harmful if Yosef improperly communicates that false belief beyond his manager. And so any harm caused—unemployment, liability for breach and misappropriation—would be warranted by his actions; they would not be wrongful had management used nondeceptive means.

Because of the entrapment structure, ordinary morality and similar harm-based views will have difficulty defending the view that *Canary* is wrong. To the extent the false belief generated by *Canary* causes harm, it only causes harm to bad actors. And any harm caused is justified by the bad actor's bad actions. As discussed *supra*, the exception for lies to bad actors does not apply because many *Canary* cases' targets are not bad actors. Indeed, the *purpose* of the deceptive practice is to distinguish good from bad targets. But the essence of that protective lies exception—that the *wrong* of lying be limited to bad actors in virtue of their bad acts—reinforces the permissibility of such a use. While a nonconsequentialist account of the wrong of lying that does not situate the wrong of a lie in the harm it causes might still conclude the practice is wrong because it involves or could involve lies to innocent targets, non-harm-based views are sufficiently disputed that whatever wrongness there may be does not support the Argument from Morality.[379]

b. Non-Materiality

The entrapment structure is not the only reason that *Canary* and similar precautions are unlikely to cause harm. *Canary* also has a low risk of harm

---

[378] *See* Roger A. Grimes, *Beyond Honeypots: It Takes a Honeytoken to Catch a Thief*, CSO Magazine (Apr. 16, 2013), https://www.csoonline.com/article/2614310/beyond-honeypots--it-takes-a-honeytoken-to-catch-a-thief.html.

[379] *Cf.* Benoit v. Saint-Gobain Performances Plastics Corp., 959 F.3d 491, 498 (2d Cir. 2020) (strict liability and negligence require damages); GREEN, *supra* note 51, at 44–45 (endorsing harm principle in criminalization of fraud).

because the false belief is *not material*—Yosef's false belief about the codename is irrelevant to decisions beyond his decision to leak. If management had lied about something relevant to Yosef's other decisions—like engineering parameters—then a resulting false belief could cause harm to others, and may even be very likely to do so. Such a deceptive practice would involve imparting a false belief that is *material*, and so is unlikely to be morally permitted.

Other intuitively permissible examples also exhibit non-materiality. For example, recall the rumor that Apple monitors for leaks using undercover security agents posing as bar patrons.[380] That deceptive precaution operated on multiple levels: either the deception is the plainclothes security or the deception is the rumor. *Neither* false belief is material to collateral decisions, other than whether to share information.[381] The false belief is unlikely to lead to harm, and so the deceptive precaution is likely morally permissible.

This principle appears generalizable: when the number and significance of collateral decisions to which a false belief is relevant are minimal, the false belief is less likely to cause harm, and vice-versa—the greater the number or significance of collateral decisions to which a false belief might be relevant, the more *material* any resulting deception and so the greater the likelihood of harm.[382] Most intuitively benign deceptive precautions fit this bill. Coincidentally, or perhaps not so coincidentally, the law recognizes a similar materiality limitation on actionable falsehoods,[383] though perhaps not as broadly as commonly assumed.[384]

c. Trust and Secrecy

Entrapment and non-materiality minimize harms from false beliefs, but what of harms to trust? Harms to trust can undermine reliable channels of communications and degrade working environments. But such harms do not necessarily undermine the permissibility of a lie, and when put in context, do not support the Argument from Morality.

First, precautions that lower workplace morale or degrade working environments are not necessarily morally impermissible. Many nondeceptive precautions reduce worker happiness, from windowless labs and fences to standard nondeceptive monitoring. Unless taken to extremes, such precautions do not categorically raise moral problems. The same is true for

---

380 Lashinksy, *supra* note 169.

381 The case also exhibits an entrapment structure: those most likely to be harmed are precisely those who (wrongfully) share their secrets. If the ploy is a ruse, the target similarly cannot complain that they were harmed because they did not share information out of fear that their comrades were plainclothes security—they were prohibited from sharing the information in the first place.

382 "Relevant" is used in a loose sense, meaning something on which the listener is likely to rely in making the decision. Beliefs can affect decisions without being (rationally) relevant (as, e.g., the law of evidence recognizes).

383 *See, e.g.*, Flegles, Inc. v. TruServ Corp., 289 S.W.3d 544, 550 (Ky. 2009) ("[T]rade talk or 'puffing' . . . is not actionable as fraud."); *see also* RESTATEMENT (SECOND) OF CONTRACTS § 168, § 168 cmts. b & c.

384 *See* Stuntz, *supra* note 261, at 517–18; *e.g.*, United States v. Wells, 519 U.S. 482 (1997).

deceptive precautions. There are always line-drawing problems. But some reduction in workplace quality is permitted, and that is all that is needed to defeat the Argument from Morality, which is categorical in nature.

Second, not all harms to trust are impermissible, as the Apple rumor illustrates. Employees *should* be wary of trusting that fellow bar patrons are who they say. They should be particularly wary if they intend to discuss confidential information, but also about inconsequential details, which hackers leverage to defeat security.[385]

Critically, the harms to trust from these cases are not global. For example, even were Yosef to learn about the lie, his mistrust is unlikely to extend beyond his manager. Companies should consider these costs, but such costs do not necessarily constitute a wrong.

d. Reliance Interests and Channels

Entrapment structure and immateriality are explanatorily powerful for many seemingly permissible precautions. But these features do not fully explain others that are intuitively unproblematic.

Recall how a former car engineer and her team would put fake car parts on road-test vehicles to keep new features secret from competitors' photographers.[386] The fake car parts served as decoys—not just mere covers—so that the photographers would focus on the decoy and not the actual innovation. In this way, the "Car Costumes" were not merely designed to deny a true belief about the innovation, but to instill a false—if fleeting—belief about what to photograph.

This deception is intuitively permissible—so much so that some have called this example "uninteresting." But it is difficult to explain why (which makes it, philosophically, very interesting).

The deception lacks an entrapment structure: The target photographer is not a bad actor. She does not breach any duty owed the manufacturer. She does not trespass. And the car is driven in public, without expectation of privacy from passers-by. If the team did not use a decoy, the photographer would not be liable for misappropriation—trade secret law protects only against illicit takings, not competitive research or reverse-engineering.[387]

And the deception is material: the photographer is misled about how to focus when the car is in frame.

A commonly offered explanation is that the photographer does not have a *right* to the information. But this does not explain the intuition about this case: that someone lacks a right to some piece of information does not justify any means of withholding it from them. The public arguably did not have a right to know about President Clinton's relationship with Monica Lewinsky, but that would not justify lying under oath.[388]

---

385 *See generally, e.g.*, MITNICK AND SIMON, *supra* note 217.

386 *Supra* Part II.B.1.

387 *Supra* Part II.A.

388 For a nuanced discussion of this case, see generally SAUL, *supra* note 14, at 118–26.

Other intuitively permissible precautions exhibit similar features as Car Costumes: posting fake source code following a breach to obscure which, if any, was real ("Fake Code"); and using multiple endings and mislabeled scripts to keep secret a series' finale ("Fake Finale").[389] Both lack an entrapment structure. The misrepresentations in Fake Code may be material to, e.g., coders making decisions about their own work or who might waste time on dead-ends based on the putative source code. The misrepresentations in Fake Finale are material to many of its targets, including reporters, employees, and possibly even fans.[390]

Note an interesting feature of these cases: the deception only harms the target if she *relies* on the misrepresentation. There are two ways to avoid this harm: either the engineering team (or studio, or Cisco) does not use the deceptive precaution, or the targets do not rely on the deceptive precaution. A common assumption among those who advocate a strong prohibition on lying is that the interest in relying is, in some sense, primary: the default is that one is entitled to rely.[391] But it appears ordinary morality does not make this same assumption.[392]

A trade-off must be made between the value of using the deceptive practice and the value of the respective targets' interest in relying. In particular, the value of being able to shield information with falsehood must be weighed against the value of being able to rely on representations made in various contexts—on different "channels," to borrow Shiffrin's term.[393] Where the balance tips in favor of reliance, there is a *reliance interest*. Where it does not, there is none; one relies on that channel at her own peril.

In the trade secret context, the value of the precaution can be great: it has value both for the trade secret owner, and also for society, assuming trade secret law picks out information the secrecy of which it is socially valuable to protect. The precaution may also prevent wasteful expenditure on additional precautions and, if effective, stop a race to the bottom.[394]

In some of these cases, there would not seem to be a strong reliance interest on the other side. In Car Costumes, the balance tips against the photographer's interest in relying on appearances on the street.[395] And in Fake

---

389 *Supra* Part II.B.

390 A false belief about the series finale may be very material to fans: They may have wagered a large sum based on it.

391 *Cf.* SHIFFRIN, *supra* note 25.

392 *Cf.* SIDGWICK, *supra* note 39, at 317-18.

393 SHIFFRIN, *supra* note 25, at 2-3.

394 *Supra* Part II.D.

395 The visual aspect seemingly renders this obvious: "Appearances can be deceiving," the saying goes, suggesting you rely on appearances at your peril. But photography's seeming accuracy has made many forget the conventional wisdom. Deciding which visual channels to protect, and how, is increasingly important. *See generally* Jennifer L. Mnookin, *The Image of Truth: Photographic Evidence and the Power of Analogy*, 10 YALE J.L. & Human. 1; Joshua Rothman, *In the Age of A.I., Is Seeing Still Believing?*, THE NEW YORKER (Nov. 5, 2018), https://www.newyorker.com/magazine/2018/11/12/in-the-age-of-ai-is-seeing-still-believing.

Code, it is hard to argue that there is a strong reliance interest in the veracity of random message board postings. Of course, there could be complications where a deceptive practice has multiple targets with different reliance interests (Fake Finale, *infra*) or where a precaution, like Fake Code, excessively pollutes a channel with misinformation. These are important problems for future work about which channels to protect and how.[396] But all that is needed for our purposes is that some plausible number of such precautions could be designed to avoid those complications, and it appears they can.

e. Channels and Signaling

Some precautions that might not otherwise be permissible could become permissible if done correctly. Fake Finale illustrates this complexity because the deceptive practices (filming multiple endings, mislabeled scripts) have diffuse targets who differ in morally significant ways. There are media outlets seeking a scoop; employees (production teams, actors, staff); and fans.

Spying media outlets do not raise problems: If they are bad actors who, e.g., seek information in violation of non-disclosure agreements, then the precaution has an entrapment structure. Or, if they merely observe public filming, there is no reliance interest as in Car Costumes.

Fans are similar: their reliance interest on reports about the series' finale are at best weak. Complaints about fake news in tabloids and entertainment circulars usually focuses on the harm to the subjects of that news, not its audience.[397] If one believes everything in US Weekly, one has only oneself to blame.

But employees present a difficulty. Although some might be bad actors who would leak, others are not. A false belief about the finale is likely very material: employees have collateral decisions about career opportunities, to which the false belief is relevant (e.g., do they love the script?). And their reliance interest is strong, as employees cannot avoid such decisions or basing them, in part, on representations the studio makes. If there is no way to differentiate between these targets, the potential harm to employees would seem to count against the practice's permissibility.

The moral difficulty is that the employees have a strong reliance interest, and so deceiving them—imparting a false belief—is likely wrong. But morality does not require the studio to disclose the truth, or even completely refrain from risking some harm. And the studio could mitigate the risk of harm, by reducing the risk of imparting a false belief or by weakening the reliance interest. If the studio sufficiently mitigates this risk, the deceptive practice is likely permissible.

How might such mitigation be achieved? By signaling to employees that communications and appearances relating to the finale (or other important plot developments) may not be reliable. Such signaling could be achieved

---

396 *Infra* Part IV.

397 *See, e.g.*, Ashley Cullins, *Kim Kardashian Sues Website Over Claims She Faked Paris Robbery*, THE HOLLYWOOD REPORTER (Oct. 11, 2016), https://www.hollywoodreporter.com/thr-esq/kim-kardashian-sues-website-claims-937240.

through formal warnings in contract or employee guidelines, and informally through creative jokes. By signaling that certain communications may be unreliable, the studio does not deceive its employees as to the credibility of inferences they might make about certain subjects—about which channels of communications between them and the studio are reliable. If employees rely on such communications anyways, they do so at their own peril; but critically, they realize (or should realize) that it is at their own peril.[398]

This signaling approach may not be appropriate in all circumstances. But that is not my claim. My claim is only that it is appropriate in this case, where the studio was already presumed to be excused from imparting true beliefs.

Something similar likely applies in other cases. Several deceptive precautions, like Mountweazels, use signaling to mitigate risk of harm from false beliefs by cautioning innocent targets against reliance, thereby creating or reinforcing an entrapment structure. Although hidden so as to trap wrongdoers, the signals become clear upon closer examination: Ms. Mountweazel's work, titled "*Flags Up!*", suggests caution. Further examination shows she was born in "Bangs, Ohio," and died with pleasing symmetry "in an explosion while on assignment for *Combustibles* magazine."[399] These are "too neat a coincidence"; "Pop! goes the weasel, indeed."[400] There are more and less ethical ways to lie.

5. Direct Lies and Merely Misleading

There might remain a concern that even if the deceptions involved are not problematic, deceptive precautions that require the use of a direct lie—affirmative, direct statements that are intentionally false—are prohibited. If that is so, then to the extent that one of the above deceptions depends on the use of direct lie, the deceptive precaution should not be permitted even if the deception itself—the imparting of a false belief—would have been morally permissible. This might be troubling for two reasons: first, many of the precautions that are seemingly innocuous, such as phishing simulations and IP masking, seem to require a "direct lie" of sorts (taking the emission of an IP address to constitute a "statement"); and second, it may not always be clear how to draw the line between mere misleading and direct lies (is IP masking correctly characterized as a direct lie?).[401]

This concern ought be dismissed. As several philosophers have argued, the mechanism of deception—whether a direct lie or merely misleading—is generally *not* morally significant to whether the conduct is permissible.[402]

---

[398] *See* GREEN, *supra* note 51, at 78–79. Reportedly, some actors prefer to be lied to in this manner: it relieves pressure of keeping the truth secret. *See* Tyler, *supra* note 162.

[399] E. Williams, *supra* note 375, at 20–25.

[400] *Id.*

[401] For how existing philosophical theories about "what is said" are inadequate for distinguishing between direct lies and merely misleading, see SAUL, *supra* note 14.

[402] *See, e.g.*, SAUL, *supra* note 14, at 69–99; WILLIAMS, *supra* note 368, at 108; SIDGWICK, *supra* note 39, at 317. *But see generally* SHIFFRIN, *supra* note 25.

The most convincing argument for this position is a highly technical one in the philosophy of language.[403] I will not repeat it here, except to suggest in broad strokes why the reader should not find the claim shocking (as many do).

The problem has to do with communications, and with what the listener is entitled to believe based on what is said. Some have suggested that there is a difference between what is said and what is implied: listeners "are entitled to simply believe what is *said* . . . but if something is not said but merely communicated, we have no such entitlement."[404] Various reasons have been suggested for this principle of "caveat auditor" or listener beware:[405] the speaker does not say what they merely imply, and so cannot be responsible for the listener's inferences; the listener makes the inference and so is the one responsible; or the listener could question or clarify what is implied and so fails to do so at his peril (unlike direct lies which permit of no questioning).[406] But the difficulty is that for communications to succeed, listeners must assume that their interlocutors are playing by the same language rules, not only in what they assert but also in what they imply, and infer meaning accordingly.[407] Merely misleading plays on the fact that the listener must make these inferences for communications to succeed.[408] Bernard Williams explains this simply:

> If the circumstances are those of "normal trust" . . . the hearer will take for granted as much what I imply as what I assert; if he has reasons to be suspicious, he is as free to apply his suspicions to what I assert as to what I imply.[409]

Because lying is not morally worse than deception, where deceptions are permitted, so too might direct lies. That a deceptive practice involves direct lies does not necessarily render it impermissible. This is enough to defeat the Argument from Morality, though there may still be normative significance to the distinction, as I discuss next.

C. Lying about Legitimizing

A residual unease might remain: Even if lying is permissible, it is better if people do not *believe* that lying is permissible.[410] If that is so, then it is alarming that the law treats deception as a legitimate option for fulfilling legal requirements because, in legitimizing lies, the law legitimizes a principle that should be not be widely known or accepted.[411] This charge has more force than the more permissive or neutral accounts usually give it credit, in part because the law's toleration or even incentivizing of permissive lies does not

---

403 *See generally* SAUL, *supra* note 14.

404 *Id.* at 77 (describing view).

405 *See* GREEN, *supra* note 51, at 78–79 (coining term).

406 *See* SAUL, *supra* note 14 at 73–86 (collecting views).

407 *See id.* at 72, 82.

408 *See id.* at 80.

409 WILLIAMS, *supra* note 368, at 108.

410 *See* SIDGWICK, *supra* note 39, at 485.

411 *See generally, e.g.*, Cass R. Sunstein, *Social Norms and Social Rules*, 96 COLUM. L. REV. 903, 964 (1996). *But see generally* Matthew D. Adler, *Expressive Theories of Law: A Skeptical Overview*, 148 U. PA. L. REV. 1363 (2000).

raise the charge quite so squarely as does law's legitimization of lies. Responding to it will reveal something further about the complex nature of law's commitment to truth.

The charge has force because it is important that people are *disposed* to be sincere, even if they often fail to be truthful.[412] Even Sidgwick, a consequentialist who doubted the prohibition on lying, agreed that "[N]o one doubts that it is, *generally speaking*, conducive to the common happiness that men should be veracious."[413] A failure to take this seriously is, perhaps, one of the strongest objections against traditions that do not prohibit lying, or that collapse the distinction between lying and mere misleading.[414]

It is sometimes thought that the reason this disposition matters has to do with the difficulty of cabining lying to those cases where it is warranted. This disposition is already precarious, as evidenced by the ease with which people resort to lies.[415] The disposition might be destroyed if it were widely believed that deception is not only legally permissible, but often sanctioned by law. This seems to be the lesson of Silicon Valley vaporware and Theranos, and maybe modern politics: Lying begets lies.[416]

But that is not the only, or even the most valuable, part of the disposition. The important insight of Kant (or at least, the view ascribed to him) is that the choice to lie reveals something fundamental about our attitudes towards others. Attempts at deception are attempts at using another's reason—their ability to make autonomous, rational choices—as a mere tool, a lever to be pushed or pulled.[417] In a word, lying is manipulative.

For this reason, on many readings of Kant, coercion and deception are regarded as "the most fundamental forms of wrongdoing to others—the roots of all evil."[418] Even if it were permissible to lie in some situations, believing this to be so—thinking of it as allowed—speaks volumes about how we view each other or think we should view each other. It's not just our disposition toward sincerity that might save us from lying in the wrong circumstances. It's really our disposition towards each other that honesty about lying puts at risk.

The law's legitimizing lying is thus a real concern, not easily dismissed, and concerning in a way that the law's toleration of lies is not. Toleration does not have the same expressive force as legitimizing—as treating lying as a legitimate option, the best option, the only option.[419] These concerns are why those who

---

412 For interesting discussions, see WILLIAMS, *supra* note 368, at 84–122; MARKOVITS, *supra* note 18.

413 SIDGWICK, *supra* note 39, at 485.

414 *See* SAUL, *supra* note 14, at 86; *see generally also* Lynch, *supra* note 289.

415 *See* Allen, *supra* note 52, at 165–67. Nearly half of survey respondents said they lied to commercial websites. Shriti Sannon et al., *Understanding People's Decisions to Tell Privacy-Protecting Lies in Multiple Online Contexts*, https://www.ftc.gov/system/files/documents/public_comments/2017/11/00051-141907.pdf (collecting literature).

416 *See* BOK, *supra* note 42.

417 Korsgaard, *supra* note 41, at 331–33 ("The question whether another can assent to your way of acting can serve as a criterion for judging whether you are treating her as a mere means.").

418 *Id.* at 333.

419 *Supra* Part II.D.

might dismiss my claim as obvious, adding only incrementally to the story that law and economics has already told, are mistaken.

So what to do? There are two options. One might conclude that the law should not be this way, that it should not legitimize lies. Or one might conclude that the law should legitimize lies, but it would be better if no one believed that it did.

If it would be better that no one believed the law legitimizes lying, this project might seem doomed. Indeed, some philosophers think that moral theories that recommend they ought not be believed[420] cannot be correct moral theories.[421] But the law differs from morality in important ways and this may be one.

For now, I observe only that the law already demonstrates it has a solution: the law lies about the problem. "Puffery," "deflection," "bluffing," "legal fictions"—these are all terms that the law and legal theorists have used to suggest that permissible lies are somehow not lies.[422] And in so doing, the law may walk a line between maintaining a belief in a general prohibition and applying a more flexible, and possibly better, rule.

If this is a good solution—work for another time—then we have learned something else about the relationship between law and lying. Contrary to what others have argued,[423] the law's deception and apparent inconsistency is a feature, not a bug.

But if that's the case, why unearth this feature? As we turn to next, there is something useful and urgent, for scholars at least, about not indulging this particular deception.

IV. TOWARDS AN ETHICS OF DECEPTION

Once you see the phenomenon—that the law treats lying as a legitimate option and maybe sometimes the only option—you begin to see it everywhere. It appears in security debates about whether the government can require companies to leave up their FISA warrant canaries once the canaries become untrue,[424] in jury instructions that insist juries adhere to the law when they

---

420 *See e.g.*, SIDGWICK, *supra* note 39, at 485–92.

421 *See* PARFIT, *supra* note 355, at 40–43 (discussing Williams).

422 *See, e.g.*, Hoffman, *supra* note 48, at 1400–01 (puffery); SHIFFRIN, *supra* note 25, at 153 (deflection); ROBERT A. WENKE, THE ART OF NEGOTIATION FOR LAWYERS 33 (1985) (bluffing); L. L. Fuller, *Legal Fictions*, 25 ILL. L. REV. 363, 366–68 (1930) (defining legal fictions). Whether this amounts to "legal hyprocrisy," *see* Ekow N. Yankah, *Legal Hypocrisy*, 32 RATIO JURIS 2, 5 (2019), depends on the law's supposed commitment to truth and the anti-lie corollary, and is work for another time.

423 *Cf., e.g.*, Hoffman, *supra* note 48, at 1427 (complaining of ambiguity in regulating misleading commercial speech); Levmore, *supra* note 17 (arguing that unified theory might be useful); Klass, *supra* note 13 (arguing for unified research agenda).

424 *See* In re Grand Jury Subpoena to Facebook, No. 16-MC-1300, 2016 WL 9274455, at *5 n.10 (E.D.N.Y. May 12, 2016); Wendy Everette, Comment, *The FBI Has Not Been Here*, 23 GEO. MASON L. REV. 377, 387 (2016); Naomi Gilens, Note,

could nullify it,[425] in privacy debates about criminal record expungement,[426] in fiduciary duties[427] and ethical duties at the bargaining table.[428] And then there are questions about how far these conclusions reach once the door is opened: Could the failure to engage in certain protective lies open up criminal or tort liability under theories of aiding and abetting? If you refuse to lie to the terrorist at the door, have you offered him material assistance? Could an attorney really—ethically—advise their client to lie?

What might seem a niche question of trade secret law—an area of law itself no longer niche—is not so limited. Correcting our understanding of the relevant practices reveals the breadth of the law's permission of lies, and the case study shows its depth.[429] And that the law legitimizes lies has significant implications for understanding the law's relationship to truth.[430]

Is this reality a good thing? *Should* the law legitimize lies? I'm not convinced that the right question to ask. As argued in Part III.C, the law has resources for mitigating that harm: unlike an ethical theory, the law can lie. This means that the critical question is not about justification, but about practicality. Part IV.A turns to what that practicality involves. Part IV.B concludes by reflecting on its urgency.

A. Lying as Dual-Use Technology

This Article's trade secret law case study offers an important insight about deceptive practices: they are just another tool in the security arsenal. Some deceptive practices are excluded, as exceeding the bounds of permissible conduct, much as some extreme security precautions (e.g., murder) would also not be recognized. But there are many precautions that clearly satisfy a requirement of trade secret law, though they risk harm. Like guns, guards, and NDAs, deceptive practices can be used responsibly or illicitly. There is nothing special about them—to the law, lies are simply a dual-use technology.

The natural next question, then, is a practical one: How ought one to lie? What risks do different deceptive precautions create and how can the law mitigate them? How do we measure their costs, both internal to the company and external? And how do we minimize them?

The NSA Has Not Been Here, 28 HARV. J. L. & TECH. 525, 537 (2015); Wexler, *supra* note 245.

425 *See* Eleanor Tavris, *The Law of an Unwritten Law: A Common Sense View of Jury Nullification*, 11 W. ST. U. L. REV. 97, 104–111 (1983).

426 *See* Marc A. Franklin & Diane Johnsen, *Expunging Criminal Records: Concealment and Dishonesty in an Open Society*, 9 HOFSTRA L. REV. 733, 750–54 (1981).

427 *See* Andrew S. Gold, *The New Concept of Loyalty in Corporate Law*, 43 U.C. DAVIS L. REV. 457, 477–79, 488–94 (2009); *see also* Basic Inc. v. Levinson, 485 U.S. 224, 234–35 (1988) (questioning whether corporate officers might justifiably conceal information from shareholders to maximize shareholder value).

428 *See* Robert S. Adler & Elliot M. Silverstein, *When David Meets Goliath: Dealing with Power Differentials in Negotiations*, 5 HARV. NEGOT. L. REV. 1, 36–39 (2000); *see also* RESTATEMENT (SECOND) OF AGENCY § 348 cmt. d.

429 *Supra* Parts I.B, II, III.A.

430 *Supra* Part III.

I argued tort law is better positioned than trade secret law to address these questions.[431] The normative upshot is we should spend time thinking about whether tort law is up to the task, and if not, how to fix it. These are also issues for business and professional ethics to take up, to fill gaps the law cannot reach.

To this end, we need a better theory of *how* to lie—legally and ethically. The existing legal landscape is quite complicated, as Part II.C above explained. The limits on lying are significant and the penalties potentially steep. Not all such limits would be enforced,[432] and not all are enforceable under the First Amendment.[433] Civil liability, both for taking or failing to take, certain deceptive measures, are potentially large. And in some instances, the technology and cyberlaw governing it are quite complicated. I may disagree with those who have advocated for a unified theory of the law's approach to deception.[434] But I very much agree that deception is worthy as a discipline.[435] As a practical matter, if nothing else, deception specialists are needed.

We made some progress on the ethical front in Part III.B.4, identifying features that make deceptive practices more or less acceptable. These features include entrapment, materiality, and the absence of relevant reliance interests.[436] And we identified one method—signaling—for further reducing harm where reliance interests exist and materiality cannot be further minimized.[437] This ethical analysis provides tools for practitioners: levers to pull as they design deceptive practices. For example, just because most phishing simulations are innocuous ("Your package has arrived!") doesn't mean that all would be ("Click for information about COVID-19").[438] The question is not whether to use this technology, but how to properly design it.

Changing the framing leads to these important practical questions. Recognizing that the law legitimizes certain lies brings us to a more neutral position. It snaps us out of the old debate of looking to justify a prohibition against lies or exceptions to it, out of arguing about whether the exceptions would undermine the rule, out of debating whether what someone did was in fact a lie and therefore wrong. At least momentarily, it snaps us out of panicking over deep fakes and misinformation on the internet, and the urge to shore up what feels like a crumbling commitment to the truth. It focuses us on the question of *how* to use the tools at hand.

This is not to say we can't make use of the old debates. One of the advantages of calling a lie a lie—at least in the scholarly hallways, but perhaps

---

431 *See supra* Part II.C.

432 *See* Stuntz, *supra* note 261.

433 *See generally* United States v. Alvarez, 567 U.S. 709 (2012) (plurality).

434 *Supra* Part III.C.

435 *See* Levmore, *supra* note 17.

436 *Supra* Part III.B.4.

437 *Id.*

438 *See* Bradley Barth, *'Insensitive' Phishing Test Stirs Debate Over Ethics of Security Training*, SC MEDIA (Sept. 29, 2020), https://perma.cc/7EYV-77T2 (discussing ethics of actual simulation that promised employees bonus payments and of potential simulations regarding COVID-19).

also back in chambers—is the wealth of resources that become obviously relevant. When lies are dismissed as mere "puffery," for example, this can lend itself to an "I know it when I see it" approach.[439] But puffery is not different because it is somehow a different category that can be seen; it comes down to, or should come down to, the harms at stake and whether the particular speech act creates them.[440] Getting better at that analysis of harms is necessary for mitigating risks.

There is another advantage to recognizing lies as dual-use technology, instead of pretending deceptive precautions are somehow different in kind from their more nefarious counterparts: there is a whole literature on managing dual-use technologies, a concept here borrowed from security studies.[441] You gain the resources for dealing with such dual-use practices. And some of the more sophisticated existing accounts of the practicalities of deception are in the context of war.[442] It is time to bring them to bear in a civilian context.

B. The Surveillance Monster at the Door

Lies will also become increasingly important. Return for a moment to one of the trade-secret study's examples: posting fabricated computer code online and misrepresenting its source, so as to obscure which (if any) versions are authentic.[443] While the Cisco example was *ex post*, coming after the misappropriation had already occurred, there is a question about whether such precautions should be taken preemptively. This question has been raised in the context of data privacy—about the protections companies should take to protect consumer data for consumers' sake.[444] Indeed, negligence law does not wait for custom to catch up.[445]

This misinformation practice would reduce the reliability of information communication channels that seek to trade in such information, which consequentialists and nonconsequentialists alike identify as a problem with lying.[446] But is it? Must the reliability of all communication channels be maintained? Perhaps, it's time to consider the practical wisdom of the law's channeling function to different tiers of communication or types of communications.

The case study allows us to address these issues without the complications of individual privacy rights or personal relationships.[447] But deceptive practices are of increasing importance in these and other spheres as well.

---

439 *Cf.* Hoffman, *supra* note 48, at 1416.

440 *See generally id.*

441 *E.g.*, Elisa D. Harris, ed., *Governance of Dual-Use Technologies: Theory and Practice* (Am. Acad. Arts & Sci. 2016).

442 For example, philosopher Cecil Fabre has a forthcoming book on the ethics of foreign espionage and counterintelligence.

443 *Supra* Part II.B.2.

444 Sarah Cortes, *IP and Data Breaches: An Empirical Study of Darknet IP Crime and Its Implications for Legal Remedies*, IPSC (Aug. 2018).

445 *See* The T.J. Hooper, 60 F.2d 737, 740 (2d Cir. 1932) (Hand, J.).

446 *See* Porat & Yadlin, *supra* note 23, at 624, 631–33; SHIFFRIN, *supra* note 25, at 1, 136–38.

447 *Cf., e.g.*, HASDAY, *supra* note 25.

The age of big data has already shown that companies do not need to lie to manipulate you—to present accurate information in a way to which you will predictably respond, using your reason as mere means, or to bypass your reason entirely.[448] If you do not take the extreme measure of opting out of connected society altogether (even assuming you could), you will have no choice but to disclose or to obfuscate. Many have already chosen the latter.[449] And if lies are to be used as tools, we would do well to think carefully about how to use them, and how to regulate them, without fully curbing their use. We need a theory of how to lie.

CONCLUSION

This Article's conclusion, that the law legitimizes lying, challenges commonly held assumptions about how the law addresses the truth. In shifting the conversation, problems with the traditional focus on prohibitions, exceptions, and justifications of lies becomes clear: the traditional focus obscures important *practical* questions that appear when one takes lying seriously as a protective tool, as the law of trade secrets does.

These practical questions—about *how* to lie ethically and legally—are of increasing urgency as society finds itself caught between online misinformation and pervasive surveillance. Deceptive precautions are already a standard part of cybersecurity and there is a nearly $2-billion-dollar-and-growing market for "deception technology." The need for deception specialists is clear.

Raising these questions is an important first step. Answering them fully is the work of future scholarship. But this Article lays the foundation for doing so. Rebutting the Argument from Morality, in particular, foregrounds several features that mitigate the risks posed by lying: where the deception exhibits an *entrapment structure*, where the content of the deception is *not material*, where trust in a given context is *dangerous*, where the deception's target lacks a *reliance interest* in suggestions made or implied by the deceiver, and where the deceiver *signals* that its representations are less than reliable. These and other features need to be more fully developed. But moving away from the justification question and towards practical questions about managing what is, in fact, a dual-use security technology, is a good and necessary start.

---

[448] *Cf.* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATION CAPITALISM (2019).

[449] *See* notes 424–428 *supra* and accompanying text.