The Privacy Hierarchy: Trade Secret and Fourth Amendment Expectations

Matthew B. Kugler[*] *& Thomas H. Rousse*[**]

ABSTRACT: This Article examines public expectations of privacy in trade secret and the Fourth Amendment. Using an original, nationally representative survey of over a thousand respondents, we identify two privacy hierarchies. The first hierarchy is between domains: The public believes that surveillance conducted by commercial entities for competitive advantage is a greater violation of privacy than the same surveillance conducted by law enforcement without a warrant for criminal investigations. The second hierarchy involves types of surveillance: The same searches are rated as large (or small) privacy violations regardless of whether they are performed by law enforcement or a private company.

From these empirical findings and an analysis of prior doctrine, we argue that Fourth Amendment restrictions on police surveillance should be viewed as a "floor" for trade secret restrictions on commercial surveillance. This approach reverses the relationship between public and private surveillance recently advocated by several prominent scholars and by Justice Gorsuch in his dissent in Carpenter v. United States*, yet is consistent with longstanding trade secret doctrine. We argue further that this position provides practical benefits and is normatively justifiable given the differing objectives of trade secret and the Fourth Amendment. Practically, our framework provides guidance to courts that wish to draw upon the larger and more thorough case law of the Fourth Amendment when addressing issues that are novel to trade secret. Normatively, there is less public interest in*

[*] Assistant Professor, Northwestern University Pritzker School of Law.

[**] Law and Science Fellow, J.D./Ph.D. Candidate, Northwestern University Pritzker School of Law.

The authors thank Michael Birnhack, Erin Delaney, Shari Diamond, Ahmed Ghappour, Laura Pedraza-Fariña, Janice Nadler, David Schwartz, Nadav Shoked, Matthew Spitzer, Lior Strahilevitz, Rory Van Loo, Rebecca Wexler, and participants of the Tel Aviv University Law and Technology Workshop, the Intellectual Property Scholars Conference, the Chicago IP Colloquium, the Privacy Law Scholars Conference, and Northwestern University's Pritzker School of Law's J.D./Ph.D. seminar for comments on earlier drafts, as well as Myriam Bloom, Eva Derzic, Alexander Ogren, and Conor Tucker for helpful research assistance.

exposing the trade secrets of companies than there is in investigating crimes. As a result, we believe there should be greater privacy protection in trade secret.

I. INTRODUCTION

Common to both trade secret law and the Fourth Amendment are questions of what is and is not private. Is trash private when left in a dumpster behind an office building, or is it abandoned—free for the first taker? There is a fairly clear answer if you are a law enforcement officer: You are free to put on your rubber gloves and start digging.[1] But what about private investigators,

1. *See infra* Section IV.A.3.

corporate spies or competitive intelligence professionals?[2] Companies often have commercially sensible, if morally debatable, reasons to check up on their competitors. Where is the line for them?

This question hits on a fundamental tension in American privacy law. "Suspicion of the state has always stood at the foundation of American privacy thinking, and American scholarly writing and court doctrine continue to take it for granted that the state is the prime enemy of our privacy."[3] One would think, given this widely shared sentiment, that the state is uniquely constrained in its ability to surveil. Yet, as our trash-searching government agent would be quick to point out, this is rarely the case. Quite often, the government can conduct searches that would be forbidden to private parties.[4]

So, can corporate investigators search the trash like the government, or are the rules different for them? This brings us to trade secret law. Trade secret allows for a cause of action when one person or company obtains secret and valuable commercial information from another by "improper means."[5] The critical question, then, is whether a particular means is proper. Some means of investigation are obviously improper because they violate other legal rules. For example, physical trespasses and conversion give rise to simple torts,[6] and wiretaps and computer hacks violate state and federal statutes.[7]

Not all cases are that clear, however. The comments to the Uniform Trade Secret Act ("UTSA")[8] tell us that "[i]mproper means could include otherwise lawful conduct which is improper under the circumstances" and that "[a] complete catalogue of improper means is not possible."[9] So there is a set of forbidden techniques that cannot be readily deduced by consulting other laws, and there is no definitive list of those techniques. This creates a

2. The organization of Strategic and Competitive Intelligence Professionals differentiates "competitive intelligence" from "corporate spying" by pointing out that the latter sounds illegal. *Code of Ethics*, SCIP, http://web.archive.org/web/20171016065453/https://www.scip.org/page/CodeofEthics (last visited Jan. 2, 2019) ("Competitive intelligence is the process of legally and ethically gathering and analyzing information . . . . Corporate spying often implies illegal activities . . . .").

3. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1211 (2004).

4. *See infra* Part IV.

5. *See infra* Section II.A.

6. *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 158 (AM. LAW INST. 1965) (describing liability for intentional intrusions on land); *id.* §§ 221–242 (describing, defining, and clarifying conversion of chattels).

7. *See, e.g.*, 18 U.S.C. § 1030 (2012) (defining "[f]raud and related activity in connection with computers"); Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2512 (describing prohibitions against electronic interception of communication); *see also* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1615 (2003) (describing the prevalence of computer misuse legislation).

8. *See* UNIF. TRADE SECRETS ACT § 1 cmt. (UNIF. LAW COMM'N 1985).

9. *Id.* § 1 cmt. at 5–6; *see also* RESTATEMENT (FIRST) OF TORTS § 757 (AM. LAW INST. 1939) (detailing improper means of discovery for another party's trade secret).

puzzle for inquisitive corporations looking to push the limits of competitive advantage.

Making matters even murkier, courts deciding whether a given means is improper have often looked to their impressions of corporate morality. As the Supreme Court remarked in the 1974 *Kewanee Oil v. Bicron* case, "[t]he maintenance of standards of commercial ethics and the encouragement of invention are the broadly stated policies behind trade secret law."[10] This invitation to moral evaluation tends to lead to conclusory statements in judicial opinions. For example, one court derided otherwise-legal aerial surveillance photos as "a school boy's trick" and condemned it as improper because "our ethos has never given moral sanction to piracy."[11] While this may not be an unreasonable conclusion, it does not provide a clear method for determining whether other searches are improper. As the court there observed, "'[i]mproper' will always be a word of many nuances, determined by time, place, and circumstances."[12] Similarly, the Supreme Court of Pennsylvania has observed that trade secret law depends in part on the amorphous "standards of the business community."[13]

This uncertainty brings us to the focus of this Article: using privacy hierarchies to analogize between different domains of privacy law. We know quite a lot about the rules for searches by government agents—criminal prosecutions produce much case law—but we know less about the rules for commercial surveillance. This raises the question of how one domain should relate to the other. The Fourth Amendment concerns government surveillance, whereas trade secret concerns private surveillance. Is the Fourth Amendment more protective of privacy, or is trade secret? Or do cross-cutting policy concerns result in a mix, where neither regime is consistently more protective than the other?

Several scholars have argued that positive law, such as trade secret and trespass, should be used to inform Fourth Amendment standards.[14] They believe that the Fourth Amendment should be read to restrict the government from performing searches without warrants if those searches would be prohibited to private actors. Others have gone further, arguing that that positive law should set a "floor" for the Fourth Amendment analysis so that the Fourth Amendment would prohibit more than does positive law.[15] Justice Gorsuch cited this work favorably in his dissent in *Carpenter v. United States*, inviting future Fourth Amendment litigants to make positive law arguments.[16]

---

10. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 481 (1974).
11. E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1016–17 (5th Cir. 1970).
12. *Id.* at 1017.
13. Coll. Watercolor Grp., Inc. v. William H. Newbauer, Inc., 360 A.2d 200, 205 (Pa. 1976).
14. *See infra* Section II.C.
15. *See infra* Section II.C.
16. Carpenter v. United States, 138 S. Ct. 2206, 2268–72 (2018) (Gorsuch, J., dissenting).

Despite the congruence between these newly-salient theories of the Fourth Amendment and the themes of American privacy law articulated by Whitman and others before him, we are skeptical of their reasoning in the context of trade secret. From a standpoint of economic efficiency, the law wants companies to be able to keep trade secrets from each other. If an invention can be kept secret, a company can benefit from its creation even if it is not eligible for other intellectual property protections. Because of the value in allowing this type of secrecy, the law further seeks to make secrecy cheap by allowing companies to rely on a strong trade secret regime rather than investing in costly and wasteful physical precautions. Thus, the law restricts the surveillance capabilities of one company to give greater freedom to another.

The criminal procedure context is different. Society does not benefit by allowing corporations to hide criminal activity or evade government regulation. It therefore makes sense for competitors turning to spycraft for commercial advantage to labor under greater restrictions than government investigators working, in theory, for the public good. Having stronger protection under trade secret is also consistent with historical understandings of trade secret as promoting corporate morality, not corporate privacy. American trade secret law is not value-neutral in this sense.

In Part II of our Article, we examine the doctrinal foundations of trade secret law and the regulation of government investigators under the Fourth Amendment. We then lay out the normative basis for a Fourth Amendment floor to trade secret and explain our disagreement with previous attempts to link public and private privacy law.

By the close of Part II it will be clear that analogizing between the Fourth Amendment and trade secret—under our theory or any other—depends on two empirical propositions. First, the perceived invasiveness of searches must be consistent regardless of whether the searcher is a commercial competitor or the government, with the same searches being viewed as more or less of a violation of privacy in each context.[17] A consistent hierarchy allows us to fulfill our primary goal in this project: to determine where a search ranks in one domain based on where it ranks in the other. If one thinks about the relative volume of case law in trade secret and the Fourth Amendment, one can see the value of being able to do that. Second, the domain that receives more privacy protection must be constant.

It is only on the second of these propositions that we differ from previous theorists. If we are correct about the relative value of privacy across contexts, the public should be less concerned when the government conducts a particular search as part of a criminal investigation than when a private

17. This is not an ordinal prediction—we are not strictly interested in rank order but instead degree. This is why our later test of this hierarchy is a correlation between mean scenario scores rather than scenario rank orders.

company does so for commercial advantage. If prior theorists are correct, then fear of government investigators should trump concerns about commercial surveillance.

In Part III, we test both of these empirical propositions by means of an original and nationally representative survey study. In doing so, we draw on a literature from Fourth Amendment law that defines the "reasonable expectations of privacy" protected by the Constitution by empirically measuring the privacy expectations of ordinary citizens.[18] We expand on this literature by presenting data on people's *commercial* privacy expectations and comparing these to their privacy expectations regarding government searches.

No one has previously sought to do this kind of work in trade secret, but there is a rich tradition of looking to the surveys of moral intuitions to gain scientific understanding of public norms in other contexts. This is particularly common in torts, where there is a focus on whether acts are morally blameworthy and what level of culpability is implied by a given level of knowledge or intent.[19] Survey methods have also been used by scholars trying to quantify the subjective value lost in takings cases, looking at whether people take proposed use into account when assigning valuations,[20] and examining whether people really feel free to decline police requests to search their persons and property.[21]

Here, we surveyed a sample of adult Americans that was nationally representative in age, sex, race and ethnicity, geographic region, and educational attainment. Participants rated whether ten different surveillance scenarios violated an expectation of privacy and whether the law should

---

18. *See, e.g.*, Bernard Chao, Catherine Durso, Ian Farrell & Christopher Robinson, *Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology*, 106 CALIF. L. REV. 263, 270 n.25 (2018); Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205, 248–51 [hereinafter Kugler & Strahilevitz, *Actual Expectations*]; Matthew B. Kugler & Lior Jacob Strahilevitz, *The Myth of Fourth Amendment Circularity*, 84 U. CHI. L. REV. 1747, 1749 (2017) [hereinafter Kugler & Strahilevitz, *Fourth Amendment Circularity*]; Christine S. Scott-Hayward, Henry F. Fradella, & Ryan G. Fischer, *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19, 24–26 (2015); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727, 729, 733–34 (1993).

19. Pam A. Mueller, Lawrence M. Solan, & John M. Darley, *When Does Knowledge Become Intent? Perceiving the Minds of Wrongdoers*, 9 J. EMPIRICAL LEGAL STUD. 859, 871–73 (2012); Joseph Sanders, Matthew B. Kugler, Lawrence M. Solan, & John M. Darley, *Must Torts Be Wrongs? An Empirical Perspective*, 49 WAKE FOREST L. REV. 1, 24–25 (2014).

20. Janice Nadler & Shari Seidman Diamond, *Eminent Domain and the Psychology of Property Rights: Proposed Use, Subjective Attachment, and Taker Identity*, 5 J. EMPIRICAL LEGAL STUD. 713, 723–26 (2008).

21. *See, e.g.*, Janice Nadler & J.D. Trout, *The Language of Consent in Police Encounters*, *in* THE OXFORD HANDBOOK OF LANGUAGE AND LAW 326, 328–31 (Lawrence M. Solan & Peter M. Tiersma eds., 2012); *see also* Matthew B. Kugler & Lior Jacob Strahilevitz, *Assessing the Empirical Upside of Personalized Criminal Procedure*, 86 U. CHI. L. REV. (forthcoming 2019) (manuscript at 9–13) (on file with authors).

permit a commercial competitor to gather information using each technique. People generally condemned searches that violated other legal rules, such as trespass or wiretapping. This supports the "independent legal wrong" approach to improper means. People also condemned many other searches, however, including dumpster diving, use of aerial drones, and video surveillance of public places. On the whole, our findings reflect a sensible hierarchy of privacy expectations that is broadly consistent with existing doctrine and that suggests a general skepticism of new technologically-enabled surveillance.

Turning to our dual hierarchies, we also explored whether public expectations differed in government and corporate surveillance contexts. We constructed parallel stories in which the government, rather than a competitor, conducted surveillance using the same techniques without a warrant. Our data provide support for both the empirical propositions mentioned above. First, the results show the hypothesized consistency in search hierarchy; the privacy expectations score given to a search conducted by one searcher strongly predict the score received with the other searcher. Second, the data also show that people want and expect the government to have *more* freedom to surveil than commercial parties, rather than the reverse, and that this is consistent across all searches. This supports the normative theory we develop in Part II and is directly counter to theories previously advanced by other scholars.

In Part IV, we review how trade secret law relates to the particular means of information gathering examined in Part III and attempt to establish where ethical lines are drawn. We demonstrate that a Fourth Amendment floor for trade secret is consistent with current case outcomes; no technique plainly barred under the Fourth Amendment is permitted under trade secret.

In summary, we have three independent sources of support for our theory of the Fourth Amendment floor: first, our normative argument based on the purpose of trade secret law; second, the beliefs and expectations of ordinary citizens; and, third, the doctrinal conclusions of the courts. We conclude by discussing the implications of these results for trade secret doctrine.

II. PRIVACY IN THE TRADE SECRET AND FOURTH AMENDMENT CONTEXTS

Some means of commercial investigation are plainly proper and non-invasive. Much can be learned from a review of a company's public quarterly financial reports, for example, or by tracking mentions of it in the media.[22] One competitive intelligence firm suggests looking at local newspapers, press

22. *See, e.g.*, *Competitive Intelligence: The CEO Dared Us to Research His Company.* We Did., COMPETITIVE FUTURES, https://www.competitivefutures.com/our-work/competitive-intelligence (last visited Jan. 2, 2019) (describing how Competitive Futures used publicly available documents and employee interviews to investigate Guitar Center, a major player in the music industry that was, contrary to its public line, on the verge of bankruptcy).

accounts, public court and permit filings, annual reports, and trade show documents when performing an initial assessment of a company.[23] Though these forms of information gathering consider only public information and do not raise concerns under either trade secret or the Fourth Amendment, other methods are more problematic. Before we review the most controversial issues in trade secret misappropriation, we are going to lay out the background principles of trade secret and Fourth Amendment law to explain how each one approaches the concept of privacy.

Prior scholars have argued that the Fourth Amendment should be read to prohibit governmental searches if private citizens would not be allowed to conduct those same searches. This perspective has recently attracted the attention of Justice Gorsuch in two major Fourth Amendment cases in the 2018–2019 Term.[24] We believe that this ordering is exactly backwards in the trade secret context. Trade secret should treat any set of actions that would amount to a Fourth Amendment search as improper means, but some things that are improper under trade secret may not be violations of the Fourth Amendment. At the end of the section we will explain our normative perspective the relationship between two areas of law—the Fourth Amendment floor for trade secret—and why we disagree with prior scholars on this issue.

A. TRADE SECRET LAW AND THE AMBIGUITY OF "IMPROPER MEANS"

Although its secret nature can conceal its importance from the public eye, trade secret law is a vital and valuable part of the intellectual property regime. It protects key information such as the secret formula for Coca-Cola and the proprietary search algorithms at the heart of Google's success. In surveys, companies large and small rate trade secrets as "very important" more often than they do any other type of intellectual property.[25] While the exact value of trade secrets is difficult to measure, estimates of the total value of trade secrets held within the United States are in the trillions of dollars.[26] By

23. FULD + CO, CODE OF ETHICS: A LEGAL AND ETHICAL COMPETITIVE INTELLIGENCE GUIDE FOR CLIENTS 4 (2014). Fuld + Co is a competitive intelligence firm in Boston.

24. *See* Will Baude, *Thoughts on Property and Positive Law After the* Carpenter *Oral Argument*, WASH. POST (Nov. 30, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/11/30/thoughts-on-property-and-positive-law-after-the-carpenter-oral-argument (contextualizing Justice Gorsuch's questioning during oral argument with recent scholarship on the use of positive law); Orin Kerr, *Three Reactions to the Oral Argument in Byrd v. United States*, REASON (Jan. 12, 2018, 4:20 PM), http://reason.com/volokh/2018/01/12/reactions-to-the-oral-argument-in-byrd-v (highlighting issues with Justice Gorsuch's deployment of Baude's positive law approach to the Fourth Amendment).

25. Katherine Linton, *The Importance of Trade Secrets: New Directions in International Trade Policy Making and Empirical Research*, J. INT'L COM. & ECON., Sept. 2016, at 1, 6–7 (describing several different surveys).

26. *See* Elizabeth A. Rowe, *Contributory Negligence, Technology, and Trade Secrets*, 17 GEO. MASON L. REV. 1, 5 (2009) ("United States publicly traded companies own an estimated five trillion dollars in trade secret information.").

both reducing expenditures on protecting secret information and reducing the risk of sharing trade secrets with other firms, trade secrets enhance innovation.[27]

Though protection of techniques and specialized knowledge by individual artisans and guilds is an age-old practice,[28] the roots of trade secret law took hold only in the late nineteenth century.[29] Early trade secret cases relied on a pervasive rhetoric "of honor, trust, and the moral value of work" to treat workplace knowledge as an asset of the firm rather than the property of an individual employee.[30] By 1868, U.S. courts recognized "[t]he duty of employees to protect trade secrets" from dissemination as an express element of contracts and, by the turn of the century, as "an implied term in *all* employment."[31] This shift helped transform trade secrets from a specific feature of certain employment agreements to a widespread element of commerce. Beyond changing the relationship between employers and employees, however, the doctrine of trade secret law also set boundaries for permissible behavior of third parties seeking to uncover valuable trade secrets by defining improper means.

There are two main sources for modern trade secret law: the Restatement of Torts and the UTSA. Versions of the UTSA have been adopted in 47 states, and courts in many jurisdictions—including some that use the UTSA—have applied prior precedent interpreting the Restatement to interpretations of the UTSA or recognize the Restatement where the UTSA does not control.[32] These sources of law address two related issues. First, what counts as a trade secret? Second, what are permissible and impermissible means of obtaining such a secret? The answers from each source are largely consistent, and we will draw on both to briefly outline the fundamental principles of trade secret

27. *See* Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 329–38 (2008) (listing the benefits of incentives to innovate and disclose trade secrets provided by protection).

28. For a fascinating discussion of the role of European guilds and apprenticeships in the dissemination and regulation of specialized knowledge, see generally David de la Croix, Matthias Doepke & Joel Mokyr, *Clans, Guilds, and Markets: Apprenticeship Institutions and Growth in the Pre-Industrial Economy*, 133 Q.J. ECON. 1 (2018).

29. Catherine L. Fisk, *Working Knowledge: Trade Secrets, Restrictive Covenants in Employment, and the Rise of Corporate Intellectual Property, 1800–1920*, 52 HASTINGS L.J. 441, 446 (2001).

30. *Id.*

31. *Id.* at 483, 494.

32. *See, e.g.*, AT&T Commc'ns of Cal., Inc. v. Pac. Bell, Nos. 99-15668, 99-15736, 2000 WL 1277937, at *2 (9th Cir. Sept. 8, 2000) (citing Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984)) (interpreting the Restatement of Torts on the nature of a trade secret as a property right); Householder Grp. v. Fuss, No. C07-573 SI, 2008 WL 2891052, at *5 (N.D. Cal. July 22, 2008) (applying the Restatement where Arizona's version of the UTSA was silent).

law. The new federal Defend Trade Secrets Act[33] largely mirrors the UTSA on these questions with a small exception that is noted below.[34]

Sections 757 through 759 of the Restatement (First) of Torts influenced the application of trade secret doctrine in courts for more than a half century.[35] The definition of a trade secret provided by the Restatement is quite broad: "A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."[36] Among the factors to be considered in determining whether something is a trade secret are the number of others outside the business who know the information, "the extent of measures" the owner takes to guard it, and "the ease . . . with which" a competitor could properly acquire it.[37]

Section 757 of the Restatement describes the basic elements of trade secret misappropriation. Note the use of "improper means," the focus of our survey:

> "One who discloses or uses another's trade secret, without a privilege to do so, is liable to the other if[:]
>
> (a) he discovered the secret by improper means,
>
> (b) or his disclosure or use constitutes a breach of confidence reposed in him by the other in disclosing the secret to him[.]"[38]

So, a trade secret cannot be legally obtained through a breach of confidence or by improper means. But what are improper means? Like many vital legal concepts, a comprehensive definition has eluded legislators, courts, and scholars. Comment *f* of Section 757 simply states, "A complete catalogue of improper means is not possible."[39]

The UTSA, drafted in the mid-1960s and first adopted by the predecessor to the Uniform Law Commission in 1979, provides the basis for state trade secret law in every state except New York and arguably North Carolina.[40] The

33. 18 U.S.C. § 1836 (2012).

34. SEYFARTH SHAW, THE DEFEND TRADE SECRETS ACT: WHAT EMPLOYERS SHOULD KNOW NOW 4 (2016), http://www.seyfarth.com/uploads/siteFiles/practices/163502DefendTrade SecretsActGuideM1.pdf. Unlike the UTSA, the Defend Trade Secrets Act appears to exclude from the category of improper means "any other lawful means of acquisition." 18 U.S.C. § 1839(6); *see infra* notes 52–55 and accompanying text.

35. ELIZABETH A. ROWE & SHARON K. SANDEEN, CASES AND MATERIALS ON TRADE SECRET LAW 27 (2013).

36. RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. LAW INST. 1939).

37. *Id.*

38. *Id.* § 757.

39. *Id.* § 757 cmt. f.

40. *See Trade Secrets Law in New York*, DIGITAL MEDIA L. PROJECT, http://www.dmlp.org/legal-guide/new-york/trade-secrets-law-new-york (last visited on Jan. 10, 2019) ("New York does not have a statute governing trade secrets law. Instead, it is based solely on the common law."); Christopher A. Moore, *Redefining Trade Secrets in North Carolina*, 40 CAMPBELL L. REV. 643, 652–59 (2018) (noting that North Carolina's trade secret legislation was derived from the UTSA but reverted to a prior common law understanding in 1997).

UTSA closely tracks the elements of the Restatement, but was written to provide more clarity for some of the more troublesome aspects of trade secret law.[41] As part of this effort, the UTSA defines a trade secret as:

> [I]nformation, including a formula, pattern, compilation, program, device, method, technique, or process, that:
>
> (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
>
> (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[42]

Both the Restatement's definition of a trade secret and the UTSA language implicitly make the breadth of "improper means" relevant to the analysis of what can be a trade secret. Take the UTSA as the starting point. The UTSA is conventionally viewed as requiring that a trade secret be (1) secret (not generally known or readily ascertainable); (2) economically valuable; and (3) protected by reasonable precautions.[43] The first and third of these elements depend in part on what means are proper. For the first, the question of what can be readily ascertained depends in large part on what one can do to ascertain it. Quite a lot may be readily ascertained by watching who meets with a business person or the flow of supplies to and from a factory, if those are permissible. For the third, the precautions that are "reasonable under the circumstances" depend on what kind of efforts to penetrate those precautions are expected and permitted. Is satellite or thermal imaging permissible? If so, a company must do far more to conceal its secrets.

Because the extent of proper and improper means informs what can be classified as a trade secret, the issue of improper means remains relevant even in trade secret cases brought under a breach of confidence theory. Imagine a trade secret case brought against a former employee. This is a common set of facts—more than 85% of trade secret cases brought in federal court are against a former employee or business partner.[44] The former employee likely walked out the door with the secret in their head or on a flash drive instead of engaging in any sort of complex surveillance activity, but their former

41. UNIF. TRADE SECRETS ACT Prefatory Note (UNIF. LAW COMM'N 1985).

42. *Id.* § 1(4).

43. *See* Richard F. Dole, Jr., *The Contours of American Trade Secret Law: What Is and What Isn't Protectable as a Trade Secret*, 19 SMU SCI. & TECH. L. REV. 89, 92–103 (2016) (discussing the two-part definition of trade secret law). *See generally* ROWE & SANDEEN, *supra* note 35, ch. 3.B (reviewing definition and case-law about "generally known" and "readily ascertainable" language); *id.* ch. 4 (reviewing case-law and drafting history of UTSA's economic value requirement); *id.* ch. 5 (reviewing definition and case-law about reasonable efforts to maintain secrecy).

44. David S. Almeling, Darin W. Snyder, Michael Sapoznikow, Whitney E. McCollum, & Jill Weader, *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 303 (2009).

employer must still prove that the appropriated information can count as a trade secret. Consider a few cases in which this requirement caused problems for firms:

(1) A customer list was not secret because one could have followed an employee on his or her rounds and marked where he or she made deliveries.[45]

(2) Client identities were not secret because the firm invited all its clients to a social gathering and a person could have observed who attends.[46]

(3) The configuration of a chemical plant was not secret because it could be photographed from nearby public land.[47]

In each of these cases, the information was allegedly obtained through breach of confidence, but the court rejected the trade secret claim because the secrets could have been obtained through observation. In the modern era, quite a lot of surveillance is possible. Should courts take this into account, acknowledging that information can be obtained using satellites, drones, and public surveillance cameras? Or are those prohibited improper means?

In addition to its relevance to the definitional inquiry, appropriation by improper means also is an independent element of a trade secret claim under both the UTSA and the Restatement. To be liable under trade secret, a defendant must have misappropriated the secret by improper means or breach of confidence rather than have acquired it honestly, as through reverse engineering or independent invention.[48] This double use of improper means—both as part of the definition and as an element of the tort—makes the determination of whether a given means is "proper" central to trade secret liability.

Given this centrality, it is unfortunate that the "Definitions" section of the UTSA does not greatly clarify "improper means." In place of a definition, the UTSA lists a series of examples "includ[ing] theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means."[49]

---

45. Fulton Grand Laundry Co. v. Johnson, 117 A. 753, 754 (Md. 1922) ("[A competitor] could obtain this information by the simple process of observing each day for a week where he stopped on his daily rounds.").

46. Columbus Bookkeeping & Bus. Servs., Inc. v. Ohio State Bookkeeping, No. 11AP–227, 2011 WL 6938340, at *5 (Ohio Ct. App. Dec. 30, 2011) ("In 2008, plaintiff sponsored a social gathering for clients, spouses, and employees. In doing so, plaintiff made known to all present at least some of the names on its client list.").

47. Interox Am. v. PPG Indus., Inc., 736 F.2d 194, 201 (5th Cir. 1984) ("There is no wall around the plant, and most of the equipment is located outside the buildings. Interox admits that the plant, therefore, can be easily photographed or sketched from a number of angles. That which is readily visible and ascertainable cannot constitute a trade secret.").

48. UNIF. TRADE SECRETS ACT § 1 cmt. (UNIF. LAW COMM'N 1985).

49. *Id.* § 1(1).

So, means that are otherwise unlawful, such as theft or bribery, plainly constitute improper means. This approach to "improper means" is termed the "independent legal wrong" approach.[50] As we noted before, however, the comment to the UTSA specifies that "[i]mproper means could include otherwise lawful conduct which is improper under the circumstances."[51]

Intriguingly, the recent federal Defend Trade Secrets Act of 2016[52] specifically excludes the possibility that an otherwise lawful investigative means could give rise to federal trade secret liability,[53] though it does not preempt the state laws that do allow for this outcome.[54] This leads to an interesting and, to our knowledge, unexplored distinction between state trade secret law and the new federal statute. Somewhat oddly, the federal list of improper means mirrors the UTSA in including "misrepresentation," which—as we explore below—may be "lawful."[55]

The easy questions for trade secret law concern surveillance that violates some freestanding law. The hard questions concern behavior that is otherwise legal but contains an odor of impropriety. For example, lying about who you are may yield useful information but is ethically dubious according to many practitioners and scholars.[56] What level of disclosure is required when asking a person for valuable information? Further, it is apparently permissible to follow a delivery driver on their route to assemble a customer list.[57] Can one use electronic means to accomplish the same end at greatly reduced cost? The last few decades have seen dramatic reductions in the size and cost of video-monitoring technology, allowing for the widespread use of video surveillance in public and private spaces by a wide variety of actors. This creates new possibilities for commercial monitoring, and trade secret has yet to fully confront them.

B. COMPARATIVE CLARITY IN THE FOURTH AMENDMENT

Government actors are regulated primarily by the Fourth Amendment and a small list of statutes concerning particular means of surveillance, such as the Wiretap Act.[58] An almost endless series of cases have examined whether

50. *See, e.g.*, Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 178 (7th Cir. 1991).

51. UNIF. TRADE SECRETS ACT § 1 cmt. (UNIF. LAW COMM'N 1985).

52. Defend Trade Secrets Act of 2016, Pub. L. 114-153, 130 Stat. 375 (2016).

53. 18 U.S.C. § 1839(6) (2012). It excludes from the definition of "improper means" "reverse engineering, independent derivation, or *any other lawful means of acquisition*." *Id.* (emphasis added).

54. *Id.* § 1838.

55. *See infra* Section IV.B.

56. *See infra* notes 146–50; *infra* notes 227–28 (explaining the data collected from a survey of intelligence professionals).

57. *See supra* note 45 and accompanying text.

58. Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510–2522); 18 U.S.C. § 2705 (prohibiting bribery of witnesses and

the kinds of basic investigative techniques with which this Article is concerned are appropriate when used by the police without a warrant. As a result, there are far fewer open questions here than in the realm of trade secret; repeated consideration by the circuit courts, and repeated intervention by the Supreme Court, have led to greater doctrinal stability.[59] Though we normally think of the Fourth Amendment in the context of searches of individuals, it also applies to government searches of corporations. It therefore covers investigations of companies, including regulatory and criminal investigations.[60] This means that it is not uncommon for the same private actor to be concerned about both Fourth Amendment-style government monitoring as well as trade secret misappropriation. The Fourth Amendment only regulates actions by state actors, however.[61] Corporate surveillance by private citizens does not implicate its protections unless those private actors are working on behalf of the government.

The basic test under the Fourth Amendment was set out in Justice Harlan's concurring opinion in *Katz v. United States*.[62] Harlan wrote that police conduct amounts to a search, thereby implicating the Fourth Amendment, when "a person [exhibits] an actual (subjective) expectation of privacy and, [when] . . . the expectation [is] one that society is prepared to recognize as 'reasonable.'"[63] In subsequent cases, the Court has embraced this test and it has become the touchstone for determining whether surveillance constitutes a "search" within the meaning of the Fourth Amendment.[64] Thus, for nearly fifty years courts have spoken of "reasonable expectations of privacy."

Three general principles of Fourth Amendment law help us think through the kinds of investigative techniques most frequently at issue in trade

---

public officials); *id.* § 2703(a) (requiring "disclosure by a provider of electronic communications service of the contents of a wire . . . that has been in electronic storage").

59. There are, of course, many open questions in Fourth Amendment law. But, as is seen in Part IV, the Fourth Amendment has definite answers on many more of these particular issues than does trade secret.

60. *See, e.g.*, Burwell v. Hobby Lobby Stores, Inc., 134 S. Ct. 2751, 2768 (2014) (noting that the Fourth Amendment protects corporations); Dow Chem. Co. v. United States, 476 U.S. 227, 235 (1986) ("Plainly a business establishment or an industrial or commercial facility enjoys certain protections under the Fourth Amendment."); Marshall v. Barlow's, Inc., 436 U.S. 307, 311 (1978) ("The Warrant Clause of the Fourth Amendment protects commercial buildings as well as private homes.").

61. *See, e.g.*, Chandler v. Miller, 520 U.S. 305, 323 (1997) ("And we do not speak to drug testing in the private sector, a domain unguarded by Fourth Amendment constraints.").

62. Katz v. United States, 389 U.S. 347, 361 (1967); *see also* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 13 (2007) ("*Katz v. United States*, [is] the most important judicial decision on the scope of the Fourth Amendment." (footnote omitted)).

63. *Katz*, 389 U.S. at 361.

64. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 382 (1974) (describing *Katz* as "a watershed in fourth amendment jurisprudence"). For an examination of *Katz*'s backstory, see generally Peter Winn, Katz *and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1 (2009).

secret cases. The first of these is an emphasis on property rights, particularly property rights in land. In 1928, the Supreme Court held in *Olmstead v. United States* that the lack of a trespass on a defendant's property to install a wiretap meant that there was no Fourth Amendment violation.[65] By contrast, when a trespass did occur, even a comparatively trivial one, it was a Fourth Amendment violation.[66]

Though the history of this trespass-centric approach to the Fourth Amendment has been questioned,[67] it is still the starting point of modern Fourth Amendment analysis. The Court added the *Katz* reasonable expectation of privacy test to the existing trespass framework, creating a new way for non-trespasses to violate the Fourth Amendment.[68] But trespass remains an independently sufficient way to implicate Fourth Amendment protections. Two recent cases clearly illustrate the persistence (or re-creation) of the trespass test. In 2012, the Supreme Court held in *United States v. Jones* that the placement of a GPS tracking device on a car was a search because the attachment of a device to the defendant's property was a trespass.[69] The following year the Court held in *Florida v. Jardines* that bringing a drug-sniffing dog to the porch of a house was a search because "the detectives had all four of their feet and all four of their companion's firmly planted on the constitutionally protected extension of Jardines' home," and had neither express nor implied permission to be there.[70] Thus, any time the police need to trespass on land to conduct a search, that search will trigger Fourth Amendment protection unless the police can argue that they had license to enter the property.

The second basic principle is that the Fourth Amendment does not protect against false friends or breaches of confidence. Under the third-party doctrine, people do not have a reasonable expectation of privacy in most information voluntarily disclosed to another.[71] If that third-party wishes, it can disclose that information to the government. "[L]ower federal courts have

65. Olmstead v. United States, 277 U.S. 438, 466 (1928).

66. Silverman v. United States, 365 U.S. 505, 512 (1961) (finding the physical intrusion of inserting a "spike mike" into a wall is trespass).

67. Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67, 67–68 ("The standard account in Fourth Amendment scholarship teaches that the Supreme Court equated searches with trespasses until the 1960s. . . . [N]o trespass test was used in the pre-*Katz* era. Neither the original understanding nor Supreme Court doctrine equated searches with trespass.").

68. United States v. Jones, 565 U.S. 400, 409 (2012).

69. *Id.* at 404, 412–13.

70. Florida v. Jardines, 569 U.S. 1, 8 (2013).

71. United States v. Miller, 425 U.S. 435, 442–43 (1976); *see also* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (holding that the use of pen registers by telephone companies does not constitute a search, because telephone subscribers do not "harbor any general expectation that the numbers they dial will remain secret"). *But see* Carpenter v. United States, 138 S. Ct. 2206, 2217–20 (2018) (limiting the reach of *Miller* and *Smith* in the context of cellphone-derived location information).

applied the third-party disclosure doctrine to power records produced by utility companies, to records kept by Internet Service Providers ("ISPs"), and to credit card information."[72] Though the third-party doctrine has been criticized at a number of levels and for a variety of reasons,[73] it remains the law with the exception of a still nebulous carve-out for location-records over time generated by cell phone towers and similar data.[74]

A similar rationale leads to the holding that the use of police informants does not implicate the Fourth Amendment.[75] People know that they are running the risk that those with whom they share information will go to the police. This is a substantial point of contrast with trade secret, which instead assumes or even requires that confidences be kept and insists on only "relative secrecy."[76]

The third principle is that there is no protection under the Fourth Amendment for what is exposed to public view. "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[77] Even in the context of a private backyard, a relatively protected location under the trespass analysis, "[t]he Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares."[78] This has led courts to be skeptical of claims that the Fourth

72. United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (applying the third-party doctrine to permit disclosure of records of email metadata and websites visited kept by ISPs); United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) (applying the third-party doctrine to permit disclosure of records of ISP subscriber data); United States v. Alabi, 943 F. Supp. 2d 1201, 1207 (D.N.M. 2013) (applying the third-party doctrine to permit disclosure of credit card information); United States v. Porco, 842 F. Supp. 1393, 1398 (D. Wyo. 1994) (same); Timothy J. Geverd, *Bulk Telephony Metadata Collection and the Fourth Amendment: The Case for Revisiting the Third-Party Disclosure Doctrine in the Digital Age*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 191, 192–93 (2015) (citing United States v. McIntyre, 646 F.3d 1107, 1111–12 (8th Cir. 2011)) (applying the third-party doctrine to permit disclosure of records kept by utility companies).

73. *See, e.g.*, *Jones*, 565 U.S. at 413–18 (Sotomayor, J., concurring); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 245–46 (2006); Stephen E. Henderson, Comment, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 40–44 (2011).

74. *See Carpenter*, 138 S. Ct. at 2213–23.

75. Hoffa v. United States, 385 U.S. 293, 301–03 (1966); *see also* United States v. White, 401 U.S. 745, 749–52 (1971) (reaffirming the decision in *Hoffa*).

76. Sharon K. Sandeen, *Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law*, 2006 MICH. ST. L. REV. 667, 696. In one of the few academic papers that actively considered the relationship between trade secret privacy and Fourth Amendment privacy, Professor Sharon Sandeen highlighted the third party doctrine as a major point of divergence between the domains. She explained that "information can be protected as a trade secret even if it is known by multiple individuals or companies," describing it as a form of "relative secrecy." *Id.* Her central argument was that the rest of privacy law should follow the example of trade secret. *Id.*

77. Katz v. United States, 389 U.S. 347, 351 (1967).

78. California v. Ciraolo, 476 U.S. 207, 213 (1986).

Amendment is implicated by video surveillance of public areas.[79] Actions taken in a public area can hardly be private, can they?

These principles provide a framework for understanding how courts view the Fourth Amendment issues raised by most of the surveillance techniques described in Parts III and IV. They do not fully resolve questions about several techniques, however. Consider two small examples of the complications to come. First, in *Florida v. Jardines*, the easy question was whether the police had entered the defendant's property; they plainly had.[80] The harder question was whether they had implicit permission to do so. This question of implicit permission complicates the application of the trespass test to garbage searches, where police often trespass on the edges of a property but do so in the same way that a trash collector would.[81] Second, a lot about what goes on inside a home or office can be deduced from the street outside if one has the right equipment and an inquisitive nature. Though officers standing on public streets do not need to shield their eyes when glancing at a house, courts have shown some willingness to say that certain kinds of sensory enhancing equipment should not be aimed at a personal residence.[82] It is unclear exactly how much sensory enhancement is allowed.

C. A Fourth Amendment Floor for Trade Secret

There are natural parallels between trade secret law and the Fourth Amendment. Trade secret is concerned with reasonable precautions against intrusion and the acquisition of information that penetrates the protection of those precautions. The Fourth Amendment is concerned with reasonable expectations of privacy and government misconduct that violates those expectations. One might view both areas of law as asking a common question: Is something or someplace sufficiently private that the law should sanction those who seek to expose or invade it? Such a framing is consistent with seeing both areas of law as part of a broader project of privacy protection.[83]

We believe that both trade secret and the Fourth Amendment share a common underlying value of privacy. Even if we are granted this commonality, however, it is not immediately obvious *how* the two doctrinal areas should be related. Should the Fourth Amendment be more protective, or should trade secret? Or do cross-cutting policy concerns result in a mix,

79. *See, e.g.*, United States v. Houston, 813 F.3d 282, 287–88 (6th Cir.), *cert. denied*, 137 S. Ct. 567 (2016).

80. Florida v. Jardines, 569 U.S. 1, 9 (2013).

81. United States v. Redmon, 138 F.3d 1109, 1114 (7th Cir. 1998).

82. Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986).

83. *See, e.g.*, Pamela Samuelson, *Privacy As Intellectual Property?*, 52 STAN. L. REV. 1125, 1151–52 (2000); Sandeen, *supra* note 76, at 670–71; *see also* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (citing trade secret as one of the precursors to privacy law).

where neither regime is consistently more protective than the other? To properly analogize between the Fourth Amendment and trade secret, we need to know which domain protects against more means of privacy intrusion.

Guided by the data we present in Part III, we argue that trade secret should bar more means of surveillance than does the Fourth Amendment. Though we have found no one advocating for our view,[84] several scholars have pushed for the converse: that no means prohibited to private citizens should be permitted to the police without Fourth Amendment scrutiny. These scholars argue that the police should be required to get a warrant every time that they engage in an activity that would be illegal for an ordinary citizen. William Baude and James Stern, for example, would reframe the Fourth Amendment inquiry as, "[H]as a government actor done something that would be unlawful for a similarly situated nongovernment actor to do?"[85] Baude and Stern extend no privilege to the police; under their positive law model, law enforcement's power to invade privacy without a warrant is no greater than that of an ordinary citizen. Several scholars have gone further. Daniel Yeager, for one, has advocated that positive law should set a lower-bound for Fourth Amendment protection. In 1993, he wrote:

> A renewed faith in the positive law would provide a concrete inventory of expectations drawn from local property, tort, contract, and criminal laws. Only when the positive law recognizes no privacy interest in a given case need we resort to *Katz*, which certainly may recognize a privacy interest that the positive law has missed, but cannot be used to overcome a privacy interest that the positive law has identified.[86]

So not only should a warrant be required for an action prohibited to the public, actions that do not violate other laws but do violate expectations of privacy should also trigger Fourth Amendment protections. Richard Re makes a similar argument. Agreeing with the notion of a "Positive Law Floor," he contends that it is likely *more* objectionable for the government to encroach

---

84. With the possible exception of Sharon K. Sandeen, *supra* note 76, at 706. We do not read her as making as ambitious a claim as we are, however. We understand her work as arguing that trade secret privacy is broader in some ways than tort or Fourth Amendment privacy and that people working in those domains should consider importing some elements of trade secret privacy.

85. William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1831 (2016) (emphasis omitted) ("Stated differently, the Fourth Amendment is triggered if the officer—stripped of official authority—could not lawfully act as he or she did. Whether the Fourth Amendment applies to detectives using a thermal-imaging camera to learn about what goes on inside a house, for example, would depend on whether an ordinary citizen would breach any sort of legal duty by attempting to do the same thing in the same circumstances."). Trade secret law in particular is a thorny area for the application of the positive law model. As we discuss in Part IV, trade secret law is not as "positive" in its standard-setting or guidance from case law as a positivist might hope.

86. Daniel B. Yeager, *Search, Seizure and the Positive Law: Expectations of Privacy Outside the Fourth Amendment*, 84 J. CRIM. L. & CRIMINOLOGY 249, 251–52 (1993).

on privacy in a given way than it would be for a private party to do so.[87] For Re, the government poses "special threats" to people's security given its vast power and its ability to impose criminal sanctions and should therefore be subject to similarly special regulation.[88] The strong focus on private trespass law in the recent *Jones* and *Jardines* cases arguably supports this category of scholars,[89] and Justice Gorsuch favorably cited both the Baude and Stern piece and Re's article in his *Carpenter* dissent in 2018.[90] Gorsuch emphasized that the judiciary can use positive law to discern existing societal norms, and wrote that that greater use of state property law in Fourth Amendment cases could yield better and more predictable outcomes.[91] His support for greater use of property law and his embrace of a "constitutional floor" that would bar legislative efforts to use positive law to *limit* the scope of the Fourth Amendment substantially reinforces these academic theories.[92]

Many are deeply skeptical of drawing parallels between private law and the Fourth Amendment. Richard Posner thinks that the substantial differences between the two contexts make it impossible to draw neat connections.[93] In particular, he points to the different threshold requirements in each domain.[94] Orin Kerr is similarly somewhat cautious about analogizing to the Fourth Amendment from private law,[95] presumably including trade secret law. He says that "the positive law model," which evaluates whether a search would violate the law if conducted by a private actor, "does not work in every case."[96] Some violations of property rights do not, in his view, meaningfully infringe on privacy and should not be treated as problems under the Fourth Amendment.[97] He also believes the positive law will be underprotective in cases of technological change.[98] Other scholars, like

87. Richard M. Re, *The Positive Law Floor*, 129 HARV. L. REV. F. 313, 333 (2016).

88. *Id.* at 331–33.

89. Florida v. Jardines, 569 U.S. 1, 7–8 (2013); United States v. Jones, 565 U.S. 400, 404–09 (2012). *But see, e.g.*, Baude & Stern, *supra* note 85, at 1835–36 (arguing that the engagement with trespass law in those cases was superficial and that the Court's analysis turned on an "idealized" version of trespass law, rather than the actual laws of the states in question).

90. Carpenter v. United States, 138 S. Ct. 2206, 2268 (2018) (Gorsuch, J., dissenting).

91. *Id.* at 2265–66.

92. *Id.* at 2270–71.

93. Richard Posner, *Trade Secret Misappropriation: A Cost-Benefit Response to the Fourth Amendment Analogy*, 106 HARV. L. REV. 461, 467 (1992).

94. *See id.*; *see also infra* notes 120–23 and accompanying text (explaining how the trade secret law is not concerned with the intrusion itself unless the intrusion leads to knowledge because trade law concerns secrecy *per se*, but the Fourth Amendment is concerned with both secrecy and seclusion and therefore protects against both the intrusion and its fruits).

95. Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 516–19 (2007).

96. *Id.* at 533. He points to trespasses on the outskirts of large properties (fine under the Fourth Amendment, see *infra* Part IV), and Federal Aviation Administration regulations on low altitude overflights. *Id.*

97. *Id.*

98. *Id.* at 534.

Victoria Schwartz, take an extremely contextual view, looking to the relative capacities and motivations of public and private actors in a given context rather than adopting a blanket rule either for or against analogies.[99]

We agree with the pro-analogy scholars that one can and should draw a connection between the Fourth Amendment and restrictions on the intrusions permitted to private actors. In the context of trade secret, however, we disagree with Yeager, Baude, Stern, and Re on the direction of that relationship. The ultimate problem stems from a word that repeatedly appears in discussions of both areas: "reasonable." For the Fourth Amendment, searches must be "reasonable." For trade secret, the precautions that are overcome by improper means must have been "reasonable." Merriam-Webster defines reasonable to mean "not extreme or excessive" and "moderate, fair."[100] It is a word of balance and invites a balancing test.[101]

One side of this balancing test, in our view, is ripe for allowing analogies between the Fourth Amendment and trade secret. The weight on this analogy-friendly side of the scale is a generalized concern with intrusion and the penetration of private areas. We believe that this generalized privacy concern is hierarchical in nature. Some types of searches cause a great deal of privacy concern whereas others cause far less. We make the empirical prediction, supported by the study reported in Part III, that this hierarchy is largely the same regardless of whether the government or a private actor performs the search. Thus, knowing a search is extremely intrusive in a Fourth Amendment context strongly implies that it will also be extremely intrusive in trade secret. It follows that one can analogize from one domain to the other.

Thinking in terms of physical searches may make this idea of an intrusiveness hierarchy more intuitive. Imagine that either your employer or a government agent gives you a pat-down as you leave your workplace at the end of the day. You might feel more comfortable with one or the other performing the search but, for either searcher, you would be more comfortable with the pat-down than with a strip search. The hierarchy of searches is consistent regardless of the searcher.

The weight on the other side of the scale is the social benefit of allowing the search. The magnitude of this weight varies sharply depending on whether one is in trade secret or the Fourth Amendment. Trade secret concerns the acquisition of information by private parties for private advantage, usually commercial advantage. The Fourth Amendment concerns investigations carried out by the government in service of some public good,

---

99. Victoria Schwartz, *Overcoming the Public–Private Divide in Privacy Analogies*, 67 HASTINGS L.J. 143, 187 (2015).

100. *Reasonable*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/reasonable (last visited Jan. 2, 2019).

101. *See, e.g.*, United States v. Place, 462 U.S. 696, 703 (1983) ("We must balance the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.").

such as the discovery of crime or the apprehension of criminals. In the trade secret context, society generally wants the searched-for information to remain secret to protect the competitive advantage of the secret-holder. The whole point of trade secret law is to allow the efficient economic use of secret information without the need to invest in wasteful precautions.[102] In the Fourth Amendment context, society often wants the information sought to be exposed: police uncover evidence of the crime and a prosecutor brings charges to bring the perpetrator to justice. As the Court has repeatedly indicated, there is little *legitimate* interest in hiding illegal activity from the government.[103] There is the cost of the intrusion to privacy—recall that is on the other end of the scale—but no extra cost created by actually finding incriminating evidence.

In both contexts there is a significant legitimate interest in avoiding intrusive searches. This common interest—an immense normative weight that encompasses measures of liberty, dignity, and privacy—sits on one side of the scale. But in the Fourth Amendment context, the information being sought —the other side of the scale—is information that society generally wants to see exposed, such as criminal activity. Conversely in the trade secret context, the information being sought—such as commercial secrets uncovered for gain by a business rival—is information that society generally wants to remain hidden for the benefit of the secret-holder and economic efficiency. Given that the privacy interest is similar in both contexts but the weight in favor of searches is heavier in the Fourth Amendment context, more kinds of searches should be allowed under the Fourth Amendment.

Some would argue that this telling of government objectives overlooks the unique danger governmental surveillance poses to individual liberty.[104] Though the government *should* be investigating things like criminal activity, it

---

102. *See* David D. Friedman, William M. Landes & Richard A. Posner, *Some Economics of Trade Secret Law*, 5 J. ECON. PERSP. 61, 67–68 (1991) (establishing a simple model of cost–benefit analysis for the efficient pricing of maintaining trade secrecy, such that "the greater the value of the trade secret, and the more productive the expenditures on preventing its being lost . . . the more the firm will spend on protecting its trade secret"); David R. Ganfield II, *Protecting Trade Secrets: A Cost–Benefit Approach,* 80 ILL. B.J. 604, 606–08 (1992) (discussing Judge Posner's decision in *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 178 (7th Cir. 1991)). For the maximal argument against the secrecy requirement, see Edmund W. Kitch, *The Law and Economics of Rights in Valuable Information*, 9 J. LEGAL STUD. 683, 697–98 (1980) ("Why do the courts require that the plaintiff show, as a condition of recovery, that he has expended resources keeping the information secret? Are not all such protective expenditures wasteful?").

103. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 123 (1984) (holding a drug test of white powder reasonable for the same reason); United States v. Place, 462 U.S. 696, 707 (1983) (holding that a dog sniff was not a search because it would only reveal contraband and not impinge on the privacy of those with only non-criminalized belongings); *see also* Illinois v. Caballes, 543 U.S. 405, 408 (2005) ("We have held that any interest in possessing contraband cannot be deemed 'legitimate,' and thus, governmental conduct that only reveals the possession of contraband 'compromises no legitimate privacy interest.'" (emphasis omitted) (citing *Jacobsen*, 466 U.S. at 123)).

104. *See* Re, *supra* note 87, at 333.

may pursue a variety of goals, some far less admirable. Those familiar with China's government-run "social credit system" will recognize the force of this concern.[105] We are sensitive to this objection, and are not advocating for easing the restrictions that the Fourth Amendment currently places on the government. But we come at this problem from the perspective of trying to gain insight into trade secret law by looking at Fourth Amendment law as it now stands. Fourth Amendment law today weighs the value of legitimate government objectives against the privacy costs that the government's pursuit of them incurs.[106] Thus, if one is looking at Fourth Amendment doctrine and wondering what safely can be assumed about trade secret, then it is appropriate to think in these terms.

Though we would likely support greater protection for privacy interests under the Fourth Amendment than is currently afforded, we believe that corporations should not be given even greater leeway than the government to intrude on privacy given that their cause is far less beneficial to the public good. We also note that the First and Fourteenth Amendments have sometimes been used to shield political dissidents from scrutiny that would not normally pose a Fourth Amendment problem, providing an alternate means of protection against government surveillance that is aimed at improper ends.[107]

The Supreme Court emphasized the differing objectives of trade secret and the Fourth Amendment when it rejected a company's attempt to rely on a state law trade secret case to inform the Fourth Amendment's analysis of aerial photography. The earlier precedent was *duPont v. Christopher*.[108] There the Fifth Circuit had held that trade secret law prohibited aerial surveillance of a chemical plant under construction, deriding such observation as an unworthy trick.[109] But 16 years later, when Dow Chemical argued that this result under trade secret law indicated that it had an expectation of privacy against aerial surveillance by a government regulator, the Supreme Court

105. Xin Dai, Toward a Reputation State: The Social Credit System Project of China 47–50 (June 24, 2018) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3193577 (commenting on the authoritarian objectives the system allows the government to pursue).

106. *See supra* notes 101, 103; *infra* note 107.

107. *See, e.g.*, NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 460 (1958) (refusing to allow the state of Alabama to require disclosure of the NAACP's membership list because "[e]ffective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association, as this Court has more than once recognized by remarking upon the close nexus between the freedoms of speech and assembly. It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech." (citations omitted)). *But see* Citizens United v. Schneiderman, 882 F.3d 374, 385–86 (2d Cir. 2018) (stating that the risks posed by the disclosure of donors to a politically active nonprofit were "a far cry from the clear and present danger" posed to members of the NAACP in the prior case and therefore was not a problem under the First Amendment).

108. E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1016 (5th Cir. 1970).

109. *Id.*

disagreed. The Court observed "[t]he Government is seeking these photographs in order to regulate, not to compete with, Dow."[110] Though Dow might have good reason to be concerned by the actions of a commercial competitor who sought to photograph its premises, in the Court's view Dow had no legitimate interest in preventing the government from doing so. As the Court commented, "[g]overnments do not generally seek to appropriate trade secrets of the private sector."[111]

A consideration of doctrinal differences underscores the dissimilarity of these varying motives. The Fourth Amendment adopts a hard line on accidental disclosures. If some piece of evidence is left where a police officer can see it, then it does the defendant no good to argue that the evidence is normally kept under lock and key. In contrast, trade secret does not insist on perfect security; a trade secret owner need only take "reasonable precautions."[112] Similarly, a secret disclosed to another person in confidence is protected under trade secret law, but not under the Fourth Amendment.[113] These differences suggest that it is consistently harder for an investigator to violate the Fourth Amendment than trade secret, at least in regard to the means by which a search is carried out. In our review of trade secret law, we could not identify a single search that was permitted under trade secret law but prohibited under the Fourth Amendment, though there were some areas in which neither law was clear.[114]

As evidenced by *Dow Chemical*, courts have been reluctant to take a grant of trade secret protection as evidence that the Fourth Amendment should also extend protection. But there is more willingness to analogize in the other direction: taking a grant of Fourth Amendment protection as a reason to also grant trade secret protection, or a rejection of Fourth Amendment protection as a reason to reject trade secret. The two best examples of this are from trash search cases. In the earlier of the two, the Minnesota Court of Appeals held that, since the Fourth Amendment would have prohibited a government trash search, California trade secret law should as well:

> This rule was devised in the context of a Fourth Amendment search by law officers. We see no reason for applying a different standard in the civil mode. One has the same expectation of privacy in property regardless of whether the invasion is carried out by a law officer or by a competitor; business has as great a right to protection from industrial espionage as it has from any other theft.[115]

---

110. Dow Chem. Co. v. United States, 476 U.S. 227, 232 (1986).

111. *Id.* at 231–32.

112. Posner, *supra* note 93, at 468.

113. *Id.*; Bruce T. Atkins, Note, *Trading Secrets in the Information Age: Can Trade Secret Law Survive the Internet?*, 1996 U. ILL. L. REV. 1151, 1182–83.

114. *See infra* Part IV.

115. Tennant Co. v. Advance Mach. Co., Inc., 355 N.W.2d 720, 725 (Minn. Ct. App. 1984).

In our framework, this decision is correct in equating the weight of the privacy intrusion across the two searchers. We disagree, however, that there are no relevant differences in the weight of the searcher's motives.

The second example came seven crucial years later, after the Supreme Court had determined that the Fourth Amendment did *not* protect against trash searches. The court in this later trade secret case, faced with the same basic legal question, decided the Fourth Amendment law was again "persuasive."[116] As it explained, "it is rather difficult to find that one has taken reasonable precautions to safeguard a trade secret when one leaves it in a place where, as a matter of law, he has no reasonable expectation of privacy from prying eyes."[117]

There is much more to say on even the limited topic of trash searches. For one thing, state legislatures sometimes take the question of whether a trash search is an improper means under trade secret out of the hands of courts altogether. Connecticut, for example, specifically prohibits these searches.[118] Nonetheless, these two opposing results highlight a common insight: To some people it feels odd to say that whether trash is protected from a search depends on who is doing the searching.

Here we advocate a reversal of the usual flow of the analogies. Rather than looking to positive law to inform the Fourth Amendment, we instead look to the Fourth Amendment to inform positive law. In doing so, we take seriously the language from the Supreme Court in *Dow Chemical* that the government's interests in performing a search are qualitatively different than those of a competitor. We believe that it is perfectly sensible to permit the government to use a search technique but deny that technique to a corporate actor. By our logic, the first of the trash search cases was correct: a grant of Fourth Amendment protection against a search should inevitably imply a grant of trade secret protection. The second case was wrong, however: There is nothing odd about imposing greater restrictions on espionage aimed at commercial competition than at investigations aimed at promoting the public good.

There are two differences between trade secret and the Fourth Amendment that may count against our simple model. First, the Fourth Amendment can be violated by a search even if the search reveals nothing, but trade secret law is only violated if the information obtained by the misappropriator satisfies the other requirements of trade secret (not generally

116. Frank W. Winne & Son, Inc. v. Palmer, No. 91-2239, 1991 WL 155819, at *4 (E.D. Pa. Aug. 7, 1991).

117. *Id.*

118. CONN. GEN. STAT. ANN. § 35-51(a) (West 2015) ("'Improper means' includes theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means, including searching through trash."); *see also* Harry Wingo, Note, *Dumpster Diving and the Ethical Blindspot of Trade Secret Law*, 16 YALE L. & POL'Y REV. 195, 215–16 (1997).

known or readily ascertainable, etc.).[119] Richard Posner explains this difference in terms of the privacy intrusion each area of law, in his view, is designed to prevent. He argues that trade secret law is predominantly concerned with secrecy per se, whereas the Fourth Amendment is concerned with both secrecy and also seclusion, the desire to be free from intrusion or interference.[120] Thus trade secret law is not concerned with the wrong of the observation itself unless that wrong leads to the revelation of a secret, whereas the Fourth Amendment protects against both the intrusion and its fruits. By imposing a greater cost on Fourth Amendment searches, this argument calls into question our proposition that any time the "heavy" Fourth Amendment interest in disclosure is insufficient to outweigh a privacy concern, then the "light" trade secret interest will similarly be unable to do so.

We believe that this does not create a substantial problem for our analysis because we are focused primarily on *search methods,* and whether information is discovered is a threshold qualification. Threshold qualifications, like the need for the search to reveal valuable information for trade secret or the need for the searcher to act on behalf of the government for the Fourth Amendment, do not change whether the improper *method* has been used. A search is either improper, or it is not. The threshold qualifications are about whether it is worth punishing a *particular* improper search. One might view this as a question of remedies, with the Fourth Amendment needing to prohibit even fruitless searches given the strong ex-ante incentives of the police to conduct searches. On the trade secret side, however, there may be a greater interest in preventing a flood of corporate privacy litigation. Bruce Atkins justified differences between the Fourth Amendment and trade secret in part based on a fear that an overly broad trade secret cause of action could "lead to an onslaught of litigation by . . . deep-pocketed corporations."[121] He observed that "[a] Fourth Amendment-like privacy interest [in trade secret] is therefore too sweeping; it would create unnecessary causes of action that presently do not exist and would undermine trade secret law by reducing the need for security measures."[122]

Warrants present another threshold issue. A search that is prohibited under the Fourth Amendment without a proper warrant is generally permissible with one. There is no similar procedure to allow use of otherwise improper means to dig up a trade secret. This distinction need not detain us because we are primarily interested in whether a search method is regulated at all, not the extent to which it is regulated. In addition, this distinction, unlike the last one, appropriately gives greater leeway for searches governed

119. Posner, *supra* note 93, at 467.
120. *Id.* at 466.
121. Atkins, *supra* note 113, at 1183.
122. *Id.*

by the Fourth Amendment, given the greater public interest that we posit underlies law enforcement searches.

The second issue with our model is that the government, generally, has more surveillance capacity than private actors. There are some technologies that are peculiarly accessible to it, and some surveillance economies of scale are beyond the means of most corporations. Courts are sometimes sensitive to the kinds of tools the government can employ. The aforementioned *Dow Chemical* case, for instance, noted, "[i]t may well be, as the Government concedes, that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant."[123] Orin Kerr has suggested that Fourth Amendment law can be seen as an attempt by courts to balance growing governmental surveillance capacity against advances in concealing technologies that might thwart the government's law enforcement aims.[124] Paul Ohm puts this even more starkly "[t]hrough the Fourth Amendment the Framers provided a fixed ratio between police efficiency and individual liberty, and as technological advances change this ratio, judges can interpret the amendment in ways to change it back."[125] Taking Kerr and Ohm's insights into the domain of trade secret, Victoria Schwartz has argued that the relative information-gathering capacities of the government and corporate competitors should affect how one analogizes between the two legal contexts.[126] This sort of concern feeds back into the "special threats" language of Richard Re; the government is more dangerous than most private parties.[127]

The strongest form of the argument can be restated like this: Certain government searches need to be prohibited because they reveal more to the government than the same search would reveal to a private party. One could imagine an issue where government databases, containing a greater wealth of information than private databases, can find linkages that are simply invisible to private parties. We cannot entirely reject this critique. It may be that such information asymmetries between private and public actors exist, but this is very difficult to determine. So, for now, we bracket the issue of peculiarly revealing government searches as a category for which our model may break down.

The weaker form of the argument is more easily dealt with. Some forms of surveillance can only be conducted with government resources, so the government poses a special threat to privacy. In a case where this special threat

123. Dow Chemical Co. v. United States, 476 U.S. 227, 238 (1986).

124. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 526–27 (2011).

125. Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1346 (2012).

126. Schwartz, *supra* note 99, at 187.

127. Re, *supra* note 87, at 333.

leads to a finding of a Fourth Amendment violation, there is no harm in requiring that this also be an improper means under trade secret. The whole point of the special threat language is that private parties *cannot* match the government. Prohibiting a company from doing something that it cannot do imposes no cost.

We therefore advocate a Fourth Amendment floor for trade secret. As shown in Part IV, this is a relatively modest proposal: There is no search which trade secret law permits that the Fourth Amendment does not. We are therefore not advocating a doctrinal transformation of existing trade secret law. Instead we are seeking to provide a framework for trade secret to draw upon as it addresses novel issues. In both trade secret and the Fourth Amendment, courts must weigh a generalized privacy concern against some interest in disclosure. Though the nature of this disclosure interest differs between our two contexts, the Fourth Amendment interest in disclosure outweighs the trade secret interest. Therefore, for any given search, we know that if it is prohibited under the Fourth Amendment, it should also be prohibited under trade secret.

In addition to creating a clearer framework for analogizing between the two areas of law, this approach also provides a practical benefit to trade secret law. Due to the greater volume of Fourth Amendment cases, it is likely that any new major issue under trade secret will have previously arisen in the Fourth Amendment context. If trade secret can crib from the Fourth Amendment's notes, it will have a substantial head start on addressing emerging issues such as prolonged video surveillance and use of sensory enhancing devices.[128] This guidance is likely to be especially useful when evaluating areas where trade secret law is comparatively sparse, such as the use of sensory-enhancing technologies.

III. EMPIRICALLY DEMONSTRATING PRIVACY HIERARCHIES

Our theory of the Fourth Amendment floor for trade secret requires establishing two different hierarchies in public expectations of privacy. The first is the privacy hierarchy within contexts. This hierarchy assesses whether the public ranks different types of searches in roughly the same order regardless of whether law enforcement or a corporate competitor conducts the search. If the public shows this consistency, one can look to the Fourth Amendment to determine where a new search in trade secret fits in relation to other, known, searches.

The second hierarchy is the hierarchy between contexts. Holding techniques constant, do people judge law enforcement searches to be lesser privacy violations than corporate surveillance? If so, then knowing a search is prohibited to the government under the Fourth Amendment implies that it

128. *See infra* Section IV.C.

should also be prohibited under trade secret, as people would be even more opposed to a corporate actor conducting the search.

Here, we seek empirical support by testing our theory through a survey of public expectations. Do people create the same hierarchy of searches within contexts regardless of which entity is doing the searching, and do they think that the government should be allowed to conduct more types of searches between contexts? As we show below, the answers are yes and yes. In Part IV, we review our results and discuss the extent to which they are consistent with how trade secret and the Fourth Amendment have treated various search types doctrinally.

A. STUDY SAMPLE AND PROCEDURE

Toluna, a professional survey firm with an established panel, recruited a representative sample of adult American citizens. The exact demographics are reported in Table 1. Toluna recruited the sample to match the national population in gender, age, race and ethnicity, educational attainment, and region of residence.[129] Participants who failed either of two attention check questions were not able to complete the study, and those who finished the study in less than one-third the median completion time were removed from analysis.[130] The final sample consisted of 1,019 respondents.

We chose a representative sample for this study for three reasons. First, we approach the question of privacy hierarchy from a standpoint of generalized privacy concern. We are looking for broad, if not universal, rules for what is and is not appropriate, and a general population sample provides the best method to gauge societal norms. Also, were there an industry particularly lacking in corporate morality—such that we would get different results if we surveyed them—it is unclear that we would want to defer to its norms rather than force it to play by the same rules as society as a whole.

---

129. Following census convention, "Hispanic" was asked separate from the racial categories. In a change from some of our past research, participants were allowed to mark an "other" box for gender. A small number of participants did this, and two of these explicitly indicated transgender or nonbinary identifications. Compare this Article, with Kugler & Strahilevitz, *Actual Expectations*, *supra* note 18, at 245, 256, and Kugler & Strahilevitz, *Fourth Amendment Circularity*, *supra* note 18, at 1802. In those papers this option was omitted to avoid confusion and to allow greater conformity with census data, which does not provide such an alternative. Here, two participants who listed "other" gave clarifying comments that classified them as either male or female. They were recoded accordingly.

130. This is a standard measure to eliminate responses filled out so quickly that quality, accuracy, and validity could be negatively affected. This cut-off reduced the sample by approximately 3%.

Table 1: Demographics of the Sample

	Sample		Census[131]
% Female	51.8		50.8
% Male	47.6		49.2
% Other	.6		
Age (Years)			
Median	46		
Mean	46.26	(16.54)	
Political Orientation (1–7)[132]			
Economic	4.12	(1.70)	
Social	3.89	(1.79)	
Overall	4.02	(1.67)	
Race/Ethnicity (%)			
White	76.1		76.6
Black or AA	13.2		13.4
Indian or Native	.8		1.3
SE Asian	4.4		5.8
Hawaiian/Pacific	.2		.2
Multiracial	2.7		2.7
Other	2.6		
Hispanic (%)	16.71		18.1
Education			
Less than HS	13.3		11.0
HS Diploma/GED	30.4		28.9
Two-Year College	28.7		28.6
Four-Year College	18.0		20.0
Graduate Degree	9.7		11.4

Note: For age and political orientation, the numbers in parentheses represent standard deviations. Hispanic identity was assessed in a separate question.

Second, we draw on the rich tradition of looking to ordinary individuals' perceptions of fairness in tort law as a whole.[133] Research on community code agreement—the degree to which lay attitudes are consistent with legal rules

131. Ethnicity and gender statistics are from the "Quick Facts" page of the Census.gov website. *Quick Facts: United States*, U.S. CENSUS BUREAU, https://www.census.gov/quickfacts/fact/table/US/PST045217 (last visited Jan. 2, 2019). Educational attainment figures were calculated from data in the 2017 Census publication. *Educational Attainment in the United States: 2017*, U.S. CENSUS BUREAU (Dec. 14, 2017), https://www.census.gov/data/tables/2017/demo/education-attainment/cps-detailed-tables.html.

132. The survey assessed political orientation with 7-point Likert scales ranging from Very Liberal to Very Conservative. Participants rated themselves on "economic issues," "social issues," and "overall."

133. For a rich account of tort law motivated by concerns of fairness, see ARTHUR RIPSTEIN, EQUALITY, RESPONSIBILITY, AND THE LAW 48–93 (1999).

—finds that citizens are more likely to respect legal rules when they are consistent with the citizens' own views or when deviations from those views are modest or explicable.[134] If a case is to be tried in front of a jury composed of everyday people, the law should generally make sense to them when it touches on issues of public norms.

Third, the competitive intelligence literature—which examines the law and ethics of corporate surveillance—suggests public opinion plays a crucial role in determining what methods are appropriate. When trying to decide what is and is not ethical, competitive intelligence researchers Professors Linda Treviño and Gary Weaver describe commercial investigators considering "the 'public disclosure' test."[135] How does the investigator think people would respond were it publicly disclosed that they conducted the search? The implicit audience here is the general public.

Upon entering the study and giving their demographic information, the survey presented participants with one of two instruction screens. These screens informed respondents that the next several questions would concern either police officers conducting investigations or employees of one company investigating that company's competitor. This is a between-subject design; participants saw either the competitor instructions and questions or the law enforcement instructions and questions, but not both. On the following nine pages, participants saw the investigation scenarios in a randomized order. For example, a participant may have seen this scenario as their first:

> As part of a police investigation, police search the dumpster behind an office building looking for discarded confidential letters and office memos from ABC Corp. The dumpster is located on public property, but ABC Corp. owns the building.

For each of the scenarios, participants were asked two questions. The first: "Does this violate a reasonable expectation of privacy?" Participants gave their responses on scales ranging from 1–"Definitely Not" to 5–"Definitely Yes." Points 2 and 4 were labeled "Probably Not" and "Probably Yes." This

---

134. *See generally* NORMAN J. FINKEL, COMMONSENSE JUSTICE: JURORS' NOTIONS OF THE LAW (2001) (exploring the need for community sentiment in the judicial process); PAUL H. ROBINSON & JOHN M. DARLEY, JUSTICE, LIABILITY, AND BLAME: COMMUNITY VIEWS AND THE CRIMINAL LAW (1995) (analyzing how notions of what "justice" requires stems from community standards and consensus); TOM R. TYLER, WHY PEOPLE OBEY THE LAW (1990) (noting the importance of legitimacy in the lawmaking and enforcement context); Janice Nadler, *Flouting the Law*, 83 TEX. L. REV. 1399 (2005) (noting how perceived legitimacy of a legal result may impact one's willingness to comply with unrelated laws); Paul H. Robinson & John M. Darley, *The Utility of Desert*, 91 NW. U. L. REV. 453 (1997) (arguing for a system of criminal liability that considers the community's shared principles); Tom R. Tyler & Robert J. Boeckmann, *Three Strikes and You Are Out, But Why? The Psychology of Public Support for Punishing Rule Breakers*, 31 L. & SOC'Y REV. 237 (1997) (linking community support for punishments to shared understandings of community conditions and community values).

135. Linda Hlebe Treviño & Gary A. Weaver, *Ethical Issues in Competitive Intelligence Practice: Consensus, Conflicts, and Challenges*, 8 COMPETITIVE INTELLIGENCE REV. 61, 70 (1997).

question mirrors what one author previously used to measure expectations of privacy in the law enforcement context.[136] Use of this question in both contexts allowed us to conduct an apples-to-apples comparison between searches conducted by the government versus corporate investigators.

Our review of the literature did not suggest an obvious parallel trade secret question. The language of the UTSA distinguishes between proper and improper means, and some of the court decisions refer to the norms of commercial morality or business ethics. Yet the connotations of the words "proper" and "moral" are far broader than we think the law means to require here.[137] For our second question on commercial competition searches we therefore asked simply "Should a competitor be legally allowed to look for information this way?" This question was rephrased slightly for the police searches because the general public has some background knowledge of law enforcement procedures from popular culture and the news: "Should the police be legally allowed to look for information this way *without a warrant*?" (emphasis not present in survey). This was to avoid having participants assume the presence of a warrant. Both forms of this question were answered with a "yes" or "no."

At the close of the study, participants also completed the authoritarian submission scale developed by John Duckitt and colleagues. The social psychological theory of authoritarianism defines authoritarians as people who are especially willing to submit to authority, who believe that it is particularly important to yield to traditional conventions and norms, and who are hostile and punitive toward those who question authority or who violate such conventions and norms.[138] Duckitt's authoritarian submission scale is intended to measure the first of those impulses: the extent to which people believe that authority should be respected and obeyed rather than challenged and questioned.[139] Previous work has shown that authoritarianism is related to privacy expectations regarding law enforcement searches.[140]

---

136. Kugler & Strahilevitz, *Actual Expectations*, *supra* note 18, at 246.

137. We pilot tested the wording "Would it be wrong for ____ to look for information this way [without a warrant]," and found that it correlated extremely well with the expectation of privacy question, making the repetition somewhat redundant.

138. *See generally* Bob Altemeyer, *The Other "Authoritarian Personality,"* 30 ADVANCES IN EXPERIMENTAL SOC. PSYCHOL. 47 (1998) (discussing authoritarianism).

139. Items include "It's great that many young people today are prepared to defy authority [reverse coded]," and "What our country needs most is discipline, with everyone following our leaders in unity." The response scale ranged from 1–Strongly Disagree to 6–Strongly Agree. Higher scores indicate stronger endorsement of authoritarian ideologies. John Duckitt, Boris Bizumic, Stephen W. Krauss & Edna Heled, *A Tripartite Approach to Right-Wing Authoritarianism: The Authoritarianism–Conservatism–Traditionalism Model*, 31 POL. PSYCH. 685, 711 (2010). The other two authoritarianism scales developed by Duckitt and colleagues (authoritarian aggression and traditionalism) were also administered. *Id.* at 711–13. We believe that authoritarian submission is a better measure of the ideology construct for these purposes, however.

140. Kugler & Strahilevitz, *Actual Expectations*, *supra* note 18, at 254–55.

B. SEARCH VIGNETTES

Each vignette described a search of something related to ABC Corp. The first lines of each vignette reinforced the identity of the searching party. The police scenarios began, "As part of a police investigation," and the commercial competition scenarios began "In order to obtain information on a commercial competitor . . . ." The longest police scenario was 50 words, and the shortest was 25 words.

There is an obvious problem with drawing solely on published trade secret cases in assembling our list of surveillance techniques: Trade secret thieves do not willingly disclose their methods and conclusions in open court. The most successful thieves are likely never detected, let alone sued. Law enforcement, by contrast, must display the results of its investigations to prosecute and convict criminals.[141] This is particularly a problem for our "Visual Surveillance" category, because that surveillance trespasses on no land and leaves no obvious physical trace, making it very difficult to detect.

Those studying competitive intelligence are well aware of this problem. Professors Linda Treviño and Gary Weaver interviewed a number of people in the competitive intelligence field and noted the "intense pressure" that could be brought to bear on those working in the industry.[142] One of their respondents explained: "I would be lying if I said that people don't want you to be a little underhanded because they do. They want the information. They don't care how you get it."[143] Others Treviño and Weaver spoke to thought that it was the exception rather than the rule for clients to give investigators clear ethical guidelines, and that companies strategically preferred to be ignorant about exactly how information was obtained.[144]

We therefore drew on indications of industry practice as well as published trade secret cases. One scholar writing in competitive intelligence, Professor Lynn Sharp Paine, identified four major areas of "questionable intelligence gathering" that raise ethical concerns:

1. "[T]hose involving deceit or some form of misrepresentation;"
2. "[A]ttempts to influence the judgment[s] of [those] entrusted with confidential information" (e.g., bribery);
3. Covert surveillance; and
4. Theft.[145]

---

141. *But see* Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. ONLINE 101, 103–23 (2017) (describing police efforts to conceal their use of "stingray" devices that trick cellphones into connecting to a false cellular relay operated by law enforcement in order to track location and identifying information).

142. *See generally* Treviño & Weaver, *supra* note 135 (discussing data gathered from interviewing people in the competitive intelligence field).

143. *Id.* at 69.

144. *Id.* at 66–67.

145. Lynn Sharp Paine, *Corporate Policy and the Ethics of Competitor Intelligence Gathering*, 10 J. BUS. ETHICS 423, 425–26 (1991).

She explains that "questionable techniques are generally employed to obtain information which the firm has not disclosed, is not obligated to disclose, and probably would not be willing to disclose publicly."[146] This is in contrast to relying on publicly available information, including information that firms are obligated to disclose to government regulators.[147] A review of industry ethical codes suggests that Paine's categories encompass the most commonly cited ethical dilemmas. For example, the Code of Ethics for the Society of Strategic and Competitive Intelligence Professionals ("SCIP") discusses misrepresentation (unethical), bribery (unethical), covert surveillance (ethical, within limits), and wiretapping (unethical and illegal).[148] Fuld + Co, a competitive intelligence company based in Boston, similarly discusses misrepresentation (unethical), bribery (unethical), and wiretapping and a host of other independent legal violations (unethical).[149] Fuld omits references to covert surveillance, but this may be because their guidelines focus very heavily on what *not* to do rather than what *to* do. Treviño and Weaver cite similar categories.[150]

We therefore focused our inquiry, and our scenarios, on three classes of intelligence gathering: independent wrongs such as wiretap and trespass, pretexting and misrepresentation, and covert visual surveillance. The scenarios drew from many of the examples we describe in further detail in Part IV. They are:

- A review of public financial documents.
- A telephone wiretap.
- A trespass in the CEO's backyard that revealed confidential documents.
- A trash search of a company's dumpster.
- Questioning a high-level employee's friend to find out non-public information.
- Pretending to be a potential customer to find out non-public information.
- A drone flying over a facility and taking pictures of it.
- Installing a camera across the street from the office to watch comings and goings.
- Use of a high-power lens to see through the company's window.

Appendix A provides the full text of each vignette presented to respondents. We created these vignettes with the intent to represent a range of possible conduct. The wiretap, a violation of clear statutory law, should

146. *Id.* at 426.
147. *Id.*
148. *Code of Ethics*, *supra* note 2.
149. FULD + CO, *supra* note 23.
150. Treviño & Weaver, *supra* note 135, at 63–64.

evoke a maximal response; there is little that can be said to legally defend that search by either actor. We also included a scenario where the investigator only reviewed public financial documents. We intended this vignette to evoke a minimal response as it is not a violation of either trade secret law or the Fourth Amendment. The other searches ranged between the minimal and maximal responses. As described in Part IV, only the wiretap, the trespass, and, likely, the use of the high-powered lens might be considered violations under the Fourth Amendment. Those cases, the misrepresentation vignette, the drone, and the trash search (depending on jurisdiction) would likely be viewed as improper under trade secret law.[151]

One potential area of complexity involves the dumpster search. Even if one does not have a privacy expectation in one's trash generally, one very well might have such an expectation of privacy in the trash's location. A trash can sitting on a public street would have no extra protection, for example, but one sitting in a home's kitchen would receive full protection (under either area of law) because one would need to trespass in the home to access it.[152] The corporate context suggests two possible dumpster locations that might arguably produce different outcomes. If the dumpster is on the company's own property, trespass would be necessary to reach it. One could imagine a dumpster in a private loading dock area, for example. But the dumpster could also be on a public street or in a shared trash room, as was the case in *Greenpeace v. Dow Chemical*.[153] We therefore created two versions of the dumpster search to reflect these different possibilities. One variant said that the dumpster was behind the ABC Corp. building but on public land, and the other said that the dumpster was on land owned by ABC Corp. but outside the building. To avoid giving undue weight to the trash searches, participants only saw one of the two trash search variants; their presentation was randomized between subjects.

Based on previous research in the Fourth Amendment context, we expected that people would think several of these searches were violations of their expectations of privacy. Specifically, Christopher Slobogin and Joseph Schumacher found that people in their survey reported that use of an undercover informant at a company was moderately intrusive, if not as intrusive as tapping a corporation's computer.[154] This suggests that people may find an expectation of privacy in the pretexting and false friend scenarios, contrary to doctrine. The same dataset suggests a number of points of agreement between public expectations and doctrine, however. Their

151. *See infra* Part IV.

152. *See infra* Section IV.A.3.

153. Greenpeace, Inc. v. Dow Chem. Co., 97 A.3d 1053, 1058 (D.C. 2014). The plaintiff in that case voluntarily dismissed the trade secret claim so it could appeal the dismissal of the trespass action, the trade secret claim having been one of the few to survive the motion to dismiss and permission for an interlocutory appeal having been denied. *Id.* at 1056 n.2.

154. Slobogin & Schumacher, *supra* note 18, at 738–39.

participants rated monitoring of a telephone for thirty days as one of the most intrusive searches in their sample, consistent with Fourth Amendment doctrine and the Wiretap Act.[155] They also found that searching a garage or fenced-in property and using binoculars to observe a person on the person's own property were quite intrusive, consistent with the treatment of curtilage—the part of a property closest to a house.[156] Similarly, convergent with doctrine, respondents found examining trash at the curbside much less intrusive than these other cases, putting it on par with observing a property from a helicopter at an altitude of 400 yards.[157]

Though the Slobogin and Schumacher data are especially comprehensive, addressing fifty different search types, the dataset is over twenty-five years old and based on a small and non-representative sample.[158] Prior research has shown that sample demographics matter in the Fourth Amendment context,[159] and the age of a survey may be relevant in domains where technology and social mores are changing.[160] More recent surveys of Fourth Amendment attitudes have not covered the same breadth of issues addressed by Slobogin and Schumacher but have included a few of the scenarios considered in this project. One recent study found that people did not think a camera in a public park violated their expectations of privacy, consistent with the doctrinal prediction in the camera-across-street vignette.[161] Another recent study by Henry Fradella and colleagues with a non-representative sample found no expectation of privacy in garbage at the curbside.[162] If the curbside is public property—a fair inference—this result would be consistent with the doctrinal prediction. The same study further found a strong expectation of privacy in the case of wiretaps, again consistent with doctrine.[163]

Two studies have suggested that the public is likely to be divided on the use of drones. The sample in the Fradella and colleagues study almost

155. *Id.* at 739.

156. *Id.* at 738.

157. *Id.*

158. *Id.* at 737, 750.

159. Kugler & Strahilevitz, *Actual Expectations*, *supra* note 18, at 248–49 (reporting a study that shows much higher expectations of privacy in Amazon's unrepresentative Mechanical Turk population than in a representative sample).

160. *See* Shiva Maniam, *Americans Feel the Tensions Between Privacy and Security Concerns*, PEW RES. CTR. (Feb. 19, 2016), http://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns (noting that events such as the Snowden revelations and the San Bernardino terrorist attacks correlated with dramatic shifts in polling on security and civil liberties).

161. Kugler & Strahilevitz, *Actual Expectations*, *supra* note 18, at 259.

162. Henry F. Fradella, Weston J. Morrow, Ryan G. Fischer, & Connie Ireland, *Quantifying* Katz: *Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 342, 357 (2011).

163. *Id.* at 359.

perfectly split on whether it was appropriate for law enforcement to use a low-flying aircraft to view a backyard when the aircraft was at 1,000 feet, but was opposed to warrantless observation at 400 feet.[164] Another study found that a majority of people thought that the police would not be violating an expectation of privacy to monitor people in public places using drones, but should need a warrant to monitor a backyard.[165] Taken together, these studies suggest that people have a contextual view of aerial surveillance, and it is difficult to predict how they will respond to surveillance of a commercial facility.

C. RESULTS

The first question we sought to answer was whether the privacy hierarchy of searches is consistent across the trade secret and law enforcement domains. As Table 2 shows, it generally is. Taking each search as a datapoint, the mean expectations of privacy correlate $r(8) = +.943$, $p < .001$ across contexts. The percentages of participants who thought the searches should be allowed also strongly correlate $r(8) = .819$, $p = .004$. Despite the difference in average scores across domains, the rank order of the searches is relatively constant. That which bothers more people in one context also bothers more people in the other. As expected, participants considered the independent legal wrongs of wiretap and trespass to curtilage to be the largest privacy violations in each context. Investigation of the dumpster on public land and the review of public documents were the least.

164. *Id.* at 356–57.

165. Alisa Smith, Sean Madden, & Robert P. Barton, *An Empirical Examination of Societal Expectations of Privacy in the Digital Age of GPS, Cell Phone Towers, & Drones*, 26 ALB. L.J. SCI. & TECH. 111, 133 (2016).

Table 2: Expectations of Privacy and Permissibility Judgements

	Expectation of Privacy						Police–Trade Secret Difference			Should be Allowed	
	Trade Secret			Police			F		η^2	Trade Secret	Police
Wiretap	4.44	a	(1.11)	3.98	a	(1.24)	38.85	***	.037	9.6%	17.7%
Trespass to Curtilage	4.31	a	(1.18)	3.91	a	(1.26)	27.24	***	.026	9.6%	17.9%
Dumpster, Private Land	3.71	cd	(1.32)	2.99	c	(1.39)	34.94	***	.066	22.0%	50.2%
Dumpster, Public Land	3.04	e	(1.39)	2.34	e	(1.42)	32.55	***	.059	42.6%	71.3%
Pretexting	3.69	c	(1.28)	3.19	bc	(1.37)	36.19	***	.034	29.2%	39.9%
False Friend	3.59	d	(1.27)	3.01	c	(1.36)	50.48	***	.047	30.6%	47.5%
Drone	3.88	bc	(1.26)	3.04	c	(1.35)	104.84	***	.093	20.4%	44.0%
Camera Across Street	3.60	d	(1.32)	2.71	d	(1.40)	108.73	***	.097	28.8%	58.7%
Lens Through Window	4.04	b	(1.27)	3.29	b	(1.35)	83.08	***	.076	16.7%	42.4%
Public Financial Documents	2.16	f	(1.47)	1.97	f	(1.34)	4.57	*	.004	77.3%	72.3%

Note: The expectation of privacy column contains means and standard deviations for the question asking participants whether a search violated a reasonable expectation of privacy. These answers were on a 5-point scale, with 5 being labeled "Definitely Yes" and 1 being labeled "Definitely Not." Means within a column that do not share alphabetical subscripts are significantly different from each other.[166] F statistics are for the Trade Secret–Law Enforcement comparison. *** $p < .001$; *, $p < .05$.

Looking further at the cross-vignette variation reveals several other interesting patterns. In the independent legal wrong category, current law bars both competitors and the government from trespass and wiretapping. The harder case here is the dumpster search. Somewhat surprisingly, there is a substantial difference between the public and private land dumpster searches in both contexts. For the police search, it is a 21.1 percentage point difference, for the trade secret search it is a 20.6 percentage point difference.

166. Means within a context (police or trade secret) were compared using a mixed model because of the missing data from the dumpster search questions; recall that people received either the public or private land variants, but not both. To correct for multiple comparisons, differences are only labeled as significant if they were at the $p < .01$ level.

Recall that people only saw one or the other of the two dumpster search vignettes, and that the difference in scenario wording was quite small. That the data shows such a strong difference despite these factors suggests that participants were quite sensitive to this small shift in the fact pattern. Consistent with the approach of some courts post-*Jardines*,[167] it matters a great deal to participants whether trash is being left "in public" for collection or is still on a person's private property. A literal application of these results would mirror Fourth Amendment doctrine: The police would be allowed to search a dumpster on public land, and it is a coin flip whether they can search one on private land (recall that the question was binary yes/no. 50.2% saying that it should be allowed implies that 49.8% said it shouldn't be). Corporate competitors would be barred in both cases, as is the law in some states.[168]

There are two interesting nuances for the misrepresentation and false friend vignettes. First, consistent with Slobogin and Schumacher,[169] people are much more skeptical of law enforcement use of these techniques than one might expect based on the doctrine. Second, misrepresentation is arguably an odd fit for the improper means category. The Supreme Court found little wrong with its use by law enforcement, and "loose lips sink ships" is a phrase with a long pedigree.[170] Yet here people say that companies should not be allowed to play this kind of trick on each other, endorsing the notion that misrepresentation is inappropriate in the trade secret context.

The visual surveillance data reveal two interesting patterns. First, in terms of the Fourth Amendment, the drone and camera-across-the-street vignettes were about as worrying to people as the minor trespass of searching a private dumpster. As described in Part IV, doctrine tends in favor of allowing such visual searches though it would likely prohibit the dumpster examination. Second, respondents found the use of the high-powered lens fairly worrying, more so than either of the other visual searches or the private dumpster search. Thinking about this kind of technologically aided observation, one could draw a parallel to *Jardines*, which commented on the difference between glancing in a window and walking up to a house and sticking one's nose up against it.[171] So it may be fine to take a passing look in a window, but not to make a business of it. Were a court inclined to adopt this view, it would be an interesting extension of *Kyllo*'s attempt to differentiate between rare and advanced surveillance technology (e.g., thermal imaging) and everything else.[172] These results, to our knowledge novel in this area, may help inform courts as they consider this question.

---

167. *See infra* Section IV.A.3.

168. CONN. GEN. STAT. ANN. § 35-51(a) (West 2015).

169. Slobogin & Schumacher, *supra* note 18, at 737–39.

170. *The Meaning and Origin of the Expression: Loose Lips Sink Ships*, PHRASE FINDER, https://www.phrases.org.uk/meanings/237250.html (last visited Jan. 2, 2019).

171. Florida v. Jardines, 569 U.S. 1, 5–6 (2013).

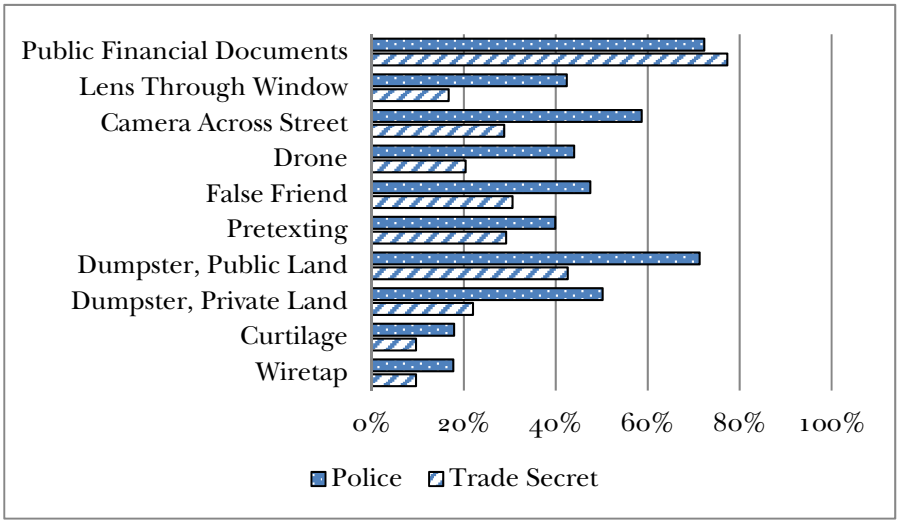
172. Kyllo v. United States, 533 U.S. 27, 34 (2001).

The second point regarding visual surveillance is the public's great skepticism about companies using it. One might think, consistent with the Fourth Amendment jurisprudence, that anything a company leaves where it can be seen, even seen using substantial aid, is something that is no longer private. Participants here strongly reject that view.

The second question we investigated was the relationship between trade secret and Fourth Amendment expectations overall. There is a significant difference between the two on every single search. This includes searches that almost everyone surveyed thought should not be permitted to either party (wiretaps and trespasses) as well as searches that almost everyone thought should be permissible to both parties. Except for searches of public financial documents, the difference is in favor of permitting more government searches. This supports our theoretical position that any search prohibited to the government should also be prohibited to private parties. Note the extent to which the reverse proposition would conflict with public views: There are many searches that people would permit the government to conduct but would bar to companies.

There was a further interesting difference between contexts. In the police surveillance domain, the average expectation of privacy score correlates with authoritarianism, $r(509) = -.23$, $p < .001$. Those who were higher in authoritarianism had lower expectations of privacy. This was not true in the trade secret context, where the correlation was non-significantly in the other direction, $r(510) = +.053$, $p = .23$. Similarly age was correlated with privacy expectations in the police context, $r(509) = -.18$, $p < .001$. Those who were younger had greater expectations of privacy against police searches. There was again no significant effect in trade secret, however, $r(510) = +.024$, $p = .59$.

Figure 1: Showing the Percentage of Respondents Believing that Either the Police or Corporations Should be Able to Conduct a Given Type of Search



Given the tepid and inconsistent support for government surveillance in the United States,[173] some might find it surprising that the difference between the police and corporate surveillance vignettes is both large and in favor of the government. But many scholars have noted an equally powerful anti-corporate bias in the tort context. There appears to be something about business activities that either prompts people to distrust corporate defendants or hold them to higher standards.[174] People are harsher toward corporate defendants even when the wealth of corporate and individual defendants is equated,[175] and are more inclined to hold corporate actors liable for accidental harms than identically situated individual actors.[176] This tendency to be skeptical of corporate defendants even exists in the criminal context. In a study on the Computer Fraud and Abuse Act, a meaningful minority of participants were willing to assign criminal liability to a company for monitoring a competitor's website to undercut their prices.[177] However much people may distrust the government—something we did not measure—it is entirely possible that they also did not trust the motives of corporate investigators.

This potential distrust of corporations could lead to a separate concern. In this data, we compared Fourth Amendment searches of corporations to trade secret searches of corporations. Most Fourth Amendment law is grounded in searches of individuals, however. If one looks to Fourth Amendment case law to analogize to trade secret, it may be that one is comparing Fourth Amendment-individual cases to trade secret-corporate cases. This could create a problem if Fourth Amendment protection is higher for individuals than it is for corporations.

Despite the prior literature on anti-corporate bias, we see little evidence in the present study that corporations are being denied *privacy* protection. Some of our law enforcement scenarios overlapped with prior work that used

---

173. *See, e.g.*, Mieke Eoyang, Ben Freeman, & Benjamin Wittes, *The Public Is Not That Fussed About the Surveillance State: Confidence in the Intelligence Community and Its Authorities*, LAWFARE (Nov. 8, 2017, 1:00 PM), https://www.lawfareblog.com/public-not-fussed-about-surveillance-state-confidence-intelligence-community-and-its-authorities (reporting a survey finding that 45.5% of Americans chose the neutral "strongly enough" option while slightly less than 40% found privacy laws not strong enough); Maniam, *supra* note 160 (describing the volatility of public sentiment on surveillance based on events such as secret surveillance carried out by the government and terrorist attacks).

174. Robert J. MacCoun, *Differential Treatment of Corporate Defendants by Juries: An Examination of the "Deep-Pockets" Hypothesis*, 30 LAW & SOC'Y REV. 121, 125–27, 140–41 (1996) (showing that defendant's corporate status, rather than wealth, produced a pro-plaintiff bias).

175. *Id.* at 125–27, 140.

176. Sanders et al., *supra* note 19, at 24–27 (showing that respondents were harsher toward a tort defendant when they had inflicted the plaintiff's injury while on business).

177. Matthew B. Kugler, *Measuring Computer Use Norms*, 84 GEO. WASH. L. REV. 1568, 1587–88 (2016) (showing that a meaningful minority of people thought that even a fairly trivial effort to learn about a commercial competitor using web-scraping should give rise to some liability).

individual criminal defendants as surveillance targets. Despite our use of a corporation rather than an individual as the subject of surveillance, we replicated the results of several prior projects in finding no expectation of privacy in garbage left in a container on public land.[178] We also had approximately the same reactions to our drone surveillance[179] and camera-across-the-street vignettes as have been observed in prior research.[180] These comparisons are imperfect—no prior scholar asked exactly the same questions as we did—but the balance of the evidence shows no reason to expect an individual–corporate difference.

IV. TRADE SECRET AND FOURTH AMENDMENT PERSPECTIVES ON COMPETITIVE INTELLIGENCE TECHNIQUES

In this Part, we examine the trade secret and Fourth Amendment case law in each of the areas covered by our study and relate our results to the doctrine. As suggested in Part II, there is more clarity in the Fourth Amendment's approach to these areas than there is in that of trade secret. Nevertheless, we can draw some common conclusions. In particular, and consistent with the idea of a Fourth Amendment floor, we find no area in which trade secret clearly permits a search that the Fourth Amendment clearly prohibits.

A. INDEPENDENT LEGAL WRONGS

Cases involving independent legal wrongs represent some of the easiest under trade secret: The commission of independent wrongs is almost always an improper means for obtaining a trade secret. The Fourth Amendment generally agrees on this point, but there is an interesting distinction: Some minor trespasses are excused under Fourth Amendment law even though they are likely prohibited under trade secret.

1. Wiretap

Some of the clearest cases under both Fourth Amendment and trade secret law involve the use of a wiretap to monitor telephone or other electronic communication. From the Fourth Amendment perspective, this is answered by *Katz* itself: "The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[181] The Court recognized that this was a departure from the earlier trespass line of cases but believed its previous decisions had been so eroded that a new rule

178. *See supra* note 162 and accompanying text.
179. *See supra* note 165 and accompanying text.
180. *See supra* note 161 and accompanying text.
181. Katz v. United States, 389 U.S. 347, 353 (1967).

was necessary.[182] Under its new thinking, "[t]he fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance."[183]

The Electronic Communications Privacy Act ("ECPA") further governs the use of wiretaps by law enforcement.[184] Under its provisions, a "'super' search warrant" must be obtained before a wiretap can be authorized.[185] Other means of evidence collection must either have been tried or be shown to be unlikely to succeed.[186] The interception of nonrelevant communications must be minimized.[187] The length of time a wiretap can run without further judicial review is also limited.[188] Given the clarity of the ECPA provisions and the holding of *Katz* itself, a straightforward wiretap of a telephone conversation is definitely a violation of privacy expectations.

Trade secret law is similarly clear on this point. The UTSA prohibits "espionage through electronic or other means,"[189] all but explicitly mentioning wiretapping. Further, the ECPA regulates both government and private wiretaps, and provides for a private right of action,[190] as do the laws of many states. Since wiretapping is illegal, it easily satisfies the independent legal wrong standard for whether a means is improper. Both the Code of Ethics of SCIP and the recommendations of Fuld + Co stress that wiretapping is illegal and unethical.[191]

Our results show that public opinion here is congruent with the doctrine of both the Fourth Amendment and trade secret law. Respondents rated the use of a wiretap as the greatest violation of privacy expectations of all the vignettes. Only 9.6% of respondents in the trade secret context and 17.7% of respondents in the police variant thought the practice should be allowed. Following the general trend of the privacy hierarchy across contexts, respondents found the use of wiretap in the corporate context to be slightly more of a privacy violation than its use by the police without a warrant (averages of 4.44 versus 3.98 on a 5-point scale).

---

182. *Id.*

183. *Id.*

184. 18 U.S.C. § 2511 (2012).

185. *Id.* § 2518; Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 620–21, 631–32 (2003).

186. 18 U.S.C. § 2518(1)(c).

187. *Id.* § 2518(5).

188. *Id.*

189. UNIF. TRADE SECRETS ACT § 1.1 (UNIF. LAW COMM'N 1985).

190. 18 U.S.C. § 2511(4)(a).

191. *Code of Ethics*, *supra* note 2; FULD + CO, *supra* note 23.

2. Trespass

Many privacy protections are linked to rights in real property and enforced in part through doctrines developed in cases of physical trespass.[192] The common law of trespass is straightforward, holding a person liable "if he intentionally . . . enters land in the possession of the other, or causes a thing or a third person to do so . . . ."[193] This makes trespass an easy case for trade secret. The ethics literature on competitive intelligence is unsurprisingly uniform in condemning trespass.[194]

Despite the central focus on trespass in several recent Fourth Amendment cases,[195] not all trespass is equal from the law enforcement perspective. Some trespasses are sufficiently minimal or sufficiently customary that they do not violate reasonable expectations of privacy. This is not counter to general intuitions. We can understand that citizens' "reasonable expectations of privacy" might differ between an open front yard abutting a busy thoroughfare—perhaps wandered through by postal carriers, overeager dogs, and stray children—and a back porch in a secluded yard that is safer from intruders. The law recognizes these different expectations through the distinction between curtilage and open fields.

Historically, open fields are not protected by the Fourth Amendment.[196] The Court reaffirmed this open fields rule after it adopted the *Katz* test, holding that a "highly secluded" field of illicit marijuana guarded by a locked gate and several "No Trespassing" signs counted nevertheless as an "open field."[197] The Court clarified that "'open fields' may include any unoccupied or undeveloped area outside of the curtilage. An open field need be neither 'open' nor a 'field' as those terms are used in common speech."[198]

In contrast to an open field, a house's curtilage (the land closest to it) receives full Fourth Amendment protection. The Supreme Court has defined curtilage as "the area to which extends the intimate activity associated with the 'sanctity of a man's home and the privacies of life.'"[199] The Court thought that "the boundaries of the curtilage will be clearly marked" in the majority of cases and the distinction between what was curtilage and what was open field would be "easily understood from our daily experience."[200] More recently, the role of trespass and the primacy of the protection of curtilage played a central part in *Florida v. Jardines*.[201] There, Justice Scalia, writing for the majority,

192. *See supra* Section II.B.
193. RESTATEMENT (SECOND) OF TORTS § 158 (AM. LAW INST. 1965).
194. Paine, *supra* note 145, at 428; FULD + CO, *supra* note 23; *Code of Ethics*, *supra* note 2.
195. *See supra* Section II.B.
196. Hester v. United States, 265 U.S. 57, 59 (1924).
197. Oliver v. United States, 466 U.S. 170, 173 (1984).
198. *Id.* at 180 n.11.
199. *Id.* at 180 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).
200. *Id.* at 182 n.12.
201. Florida v. Jardines, 569 U.S. 1, 5–6 (2013).

reaffirmed "the traditional property-based understanding of the Fourth Amendment" and avoided the reasonable expectations of privacy test, noting that the property-based model "keeps easy cases easy."[202]

To capture public sentiment about the trespass doctrine where protections are relatively strong, we focused our vignette on a scenario meant to invoke the curtilage of a private residence—a police officer or private investigator hired by a rival firm enters the back porch of a CEO's home and spots sensitive documents on a lawn chair. Consistent with the general trend of the privacy hierarchy across contexts, respondents found the violation of privacy greater when conducted by a corporate competitor versus a police officer (4.31 v. 3.91 on a five-point scale). Slightly more than 90% of respondents stated that this kind of intrusion should not be used in the trade secret context, while 82.1% reported that it should not be used in a warrantless law enforcement search. As expected, prohibitions in both doctrinal domains on searches within a curtilage are congruent with the vast majority of public sentiment.

3. Dumpster-Diving

As one scholar commented, "[d]umpster diving is one of the easiest and safest ways of gathering confidential information, and yield secrets ranging from corporate executives' travel itineraries to descriptions of company merger plans."[203] Corporations generate huge amounts of sensitive paper and, when these companies are careless, enterprising investigators can fish this valuable corporate information from the rubbish bin.[204] As a result, many privacy-minded corporations have employed document management strategies that include shredding sensitive documents, often on-site.[205]

In *California v. Greenwood*, the Supreme Court set forth a judicial presumption that there is no reasonable expectation of privacy in trash, thus answering the general question for Fourth Amendment purposes.[206] This presumption against trash-privacy was extended in dicta to trade secret law by a federal district court in *Frank W. Winne & Son, Inc. v. Palmer*.[207] Winne, a rope manufacturer, ordered an employee to collect the trash of rival Palmer, and then used the proprietary information found in the trash to expand his

202. *Id.* at 11.

203. Wingo, *supra* note 118, at 200 (footnote omitted).

204. *See id.* at 199–202 (describing the degree of care corporations use to securely dispose of sensitive information).

205. *Id.* at 202–03.

206. California v. Greenwood, 486 U.S. 35, 41–42 (1988); *see* Carpenter v. United States, 138 S. Ct. 2206, 2266 (2018) (Gorsuch, J., dissenting) (lambasting the Court's logic in *Greenwood* while pointing out its inconsistency with California's state law).

207. Frank W. Winne & Son, Inc. v. Palmer, No. 91-2239, 1991 WL 155819, at *1–4 (E.D. Pa. Aug. 7, 1991).

sales territory.[208] The court in *Palmer* noted that "[i]t is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public."[209] Because placing sensitive information in a place readily accessible to the public did not meet the "reasonable precautions" element of trade secret law, looking through the trash of a commercial competitor was not considered to be improper means.[210]

Similarly, in *Greenpeace, Inc. v. Dow Chemical Co.*, Dow Chemical allegedly hired agents to recover documents from the dumpsters and recycling bins used by Greenpeace.[211] While Greenpeace had voluntarily dismissed its trade secret claim earlier in the litigation to allow for the appeal to the D.C. Circuit, the appellate court did address Greenpeace's privacy interest in its trash in the context of corporate espionage and its claim of conversion.[212] Here, the court held that Greenpeace had forfeited its privacy interest in the trash by throwing it out. In fact, the *Greenpeace* court found that even documents discarded in a locked communal trash room inaccessible to the general public constituted abandonment in the absence of evidence of a "'special arrangement' intended to make the garbage 'inviolate.'"[213] Other cases provide evidence of the practice of trade secret misappropriation through dumpster-diving and other trash thievery.[214]

Given the usefulness of trash in the investigation of drug crimes —discarded drug paraphernalia often shows traces of incriminating substances—it is not surprising that trash searches have been frequently litigated under the Fourth Amendment. The complexity here is quite small. We know from *Greenwood* that there is no expectation of privacy in trash that has been put out for collection as a general matter. A number of courts —framing this result in terms of abandonment—have held that a search of trash is permissible under the Fourth Amendment even if conducting the

208. *Id.* at *1.

209. *Id.* at *4.

210. *Id.*

211. Greenpeace, Inc. v. Dow Chem. Co., 97 A.3d 1053, 1057–58 (D.C. 2014).

212. *Id.*

213. *Id.* at 1063 (quoting Danai v. Canal Square Assocs., 862 A.2d 395, 403 (D.C. 2004)).

214. In *CDI International, Inc. v. Marck*, CDI, a corporation, claimed that the defendants induced a third party to bring its trash to Marck rather than dispose of it as agreed in order for Marck to harvest trade secrets; the record had not been developed at the motion to dismiss stage, and litigation did not progress. CDI Int'l, Inc. v. Marck, No. 04-4837, 2005 WL 327536, at *1–2 (E.D. Pa. Feb. 8, 2005). In *AlphaMed Pharmaceuticals Corp. v. Arriva Pharmaceuticals, Inc.*, AlphaMed accused Arriva of pulling trade secret documents from its trash. AlphaMed Pharm. Corp. v. Arriva Pharm., Inc., No. 03-20078-CIV, 2005 WL 5960935, at *3 (S.D. Fla. Aug. 24, 2005). In *Frosty Bites, Inc. v. Dippin' Dots, Inc.*, the court declined to recognize trade secret protection because Frosty Bites did not use "reasonable means" to protect its trade secret when it threw out "storage bags and boxes in public trash bins with no restrictions on the methods of disposal." Frosty Bites, Inc. v. Dippin' Dots, Inc., No. 3-01-CV-1532-M, 2003 WL 21196247, at *4 (N.D. Tex. May 19, 2003).

search requires trespassing on private land.[215] These cases have often distinguished between land that is off-limits—fenced off and only accessible to a property owner—and land that others may have either had a legitimate right to access or the practical ability to enter.[216] In *United States v. Hall*, for example, the court upheld the government's search of a company's dumpster even though accessing the dumpster required walking forty feet onto private property.[217] There the court fixated on the lack of signs, barricades, and similar obstacles to public access.[218] This represents an exception to the general rule that trespasses are Fourth Amendment searches.

As noted in Section III.B, however, two recent Supreme Court cases have reaffirmed the role of trespass in the Fourth Amendment analysis and call the reasoning of these earlier decisions into question. In *United States v. Jones,* the Court held that the *Katz* reasonable expectations of privacy test supplemented, rather than replaced, an earlier test focused on trespass.[219] It therefore may violate the Fourth Amendment when a government agent trespasses on property to obtain information even if the trespass is small. The Court similarly held in *Florida v. Jardines* that the police could not trespass on a property to bring a drug-sniffing dog up to a suspect's front door; the suspect was said to have not implicitly consented to this entry into his domain.[220]

Lower courts are somewhat divided on how much these new cases undermine the broad use of implied consent in earlier trash search jurisprudence. Some courts have begun drawing substantial distinctions between the curtilage of a property and all other portions of it, borrowing from the open fields doctrine.[221] Several state supreme courts have also interpreted their state constitutions as protecting against trash searches, going

215. *See, e.g.*, United States v. Redmon, 138 F.3d 1109, 1114 (7th Cir. 1998) (en banc) (holding that trash left out for collection should be treated as abandoned property, not requiring a search warrant, even if the point of collection is on the defendant's property).

216. *Id.* (discussing the number of people who needed to access the shared area from which the trash was taken).

217. United States v. Hall, 47 F.3d 1091, 1096–97 (11th Cir. 1995) (holding that the fact that a trespass onto private land was required did not make it a violation of a reasonable expectation of privacy).

218. *Id.* at 1096.

219. United States v. Jones, 565 U.S. 400, 405–07 (2012).

220. Florida v. Jardines, 569 U.S. 1, 3–4, 11–12 (2013).

221. United States v. Jackson, 728 F.3d 367, 373–75 (4th Cir. 2013) (construing curtilage narrowly to allow the search of a trash can that was not yet put to the curb for collection but was in a common area while suggesting that, post-*Jardines*, a trash pull from inside the curtilage of a home would have been a Fourth Amendment violation); Commonwealth v. Ousley, 393 S.W.3d 15, 33 (Ky. 2013) (drawing on *Jones* to hold that that removal of trash from the curtilage of a property does violate the Fourth Amendment under *Greenwood*); *see also* United States v. Castleman, 795 F.3d 904, 913 (8th Cir. 2015), *cert. denied*, 136 S. Ct. 912 (2016) (holding officers could search trash bags found in "a[n open] field without a warrant" (alterations in original) (quoting Oliver v. United States, 466 U.S. 170, 173 (1984))).

further than the federal Fourth Amendment.[222] Most recently, the Supreme Court held in *Collins v. Virginia* that the automobile search exception does not allow a police officer to enter the curtilage of a property to examine a motorcycle that was parked under a tarp.[223] This resistance to allowing incidental trespass to curtilage in the automobile context may signal that the Court would take a similar view of trash search trespasses. Since *Collins* was decided in May 2018, however, it remains to be seen how lower courts will interpret it.

Overall, we largely have convergence between trade secret law and the Fourth Amendment on this question. The Fourth Amendment is generally friendly toward trash searches, but this tendency is complicated if the police need to enter a property to collect the trash.[224] Trade secret, drawing on *Greenwood* and the Fourth Amendment, also treats trash as public.[225] But this may be qualified by a requirement that collecting the trash not involve a trespass into a territory exclusively controlled by the trade secret owner.

To capture the complexity of dumpster-diving based on the location of the trash, we tested two variants of a dumpster-diving scenario for each context, specifying that the dumpster was located on either private or public land when police officers or private investigators searched for confidential letters or office memos owned by a corporation. Following the general trend of privacy hierarchy between contexts, respondents found that the trash search was a greater violation of the expectation of privacy in the trade secret context compared to a warrantless police search in both variants.

As expected from the review of case law above, respondents were less likely to think the search should be allowed on private land than public land (22.0% versus 42.6% for trade secret; 50.2% versus 71.3% for a police search). Though more than 70% of respondents supported police searches of public trash (the most clearly permissible scenario of the four vignettes), it is a borderline case if the officer trespasses (50.3% support). Trespassing on private land to search trash under trade secret was roundly rejected (22.0% support), but it is a closer case when no trespass is required (42.6% support). In our view, this ambiguity is an appropriate match with the fact-dependent and occasionally contradictory court decisions discussed above.

222. *See, e.g.*, State v. Goss, 834 A.2d 316, 319 (N.H. 2003) (holding that the New Hampshire constitution does protect against trash searches, going further than *Greenwood*); State v. Hempele, 576 A.2d 793, 814–15 (N.J. 1990) (holding the same, under the New Jersey constitution and further concluding that *Greenwood* did not distinguish between trash on public property and trash on the curtilage of a home).

223. *See* Collins v. Virginia, 138 S. Ct. 1663, 1672–73 (2018).

224. *See supra* note 221 and accompanying text.

225. *See supra* note 214 and accompanying text.

B. FALSE FRIENDS AND PRETEXTS

Trade secret and the Fourth Amendment diverge in the domain of misrepresentation. In trade secret, the ethical acceptability of soliciting information under false pretenses is fiercely disputed. Many ethical guidelines advise against such tactics,[226] and both the UTSA and federal Defend Trade Secrets Act explicitly list "misrepresentation" as an improper means.[227] In one somewhat dated survey of competitive intelligence professionals, however, between around 30% and 45% of respondents said their company uses misrepresentations to gather information, and twice as many thought other firms would do so.[228] For example, 39.3% said their company might have someone pose as a graduate student doing a thesis to gather information, and 85.6% thought another company would employ that technique.[229] This pattern extended to other questionable methods of information gathering as well. 63.2% of those surveyed thought their company would buy a competitor drinks at a conference with the aim of asking the (now intoxicated) competitor hard questions later in the night, and 91.1% thought other companies would do so.[230]

It is a challenge to define the acceptable boundaries of deceit and misdirection in trade secret. Businesses sometimes conduct pretextual negotiations in bad faith to obtain trade secrets and other valuable information. For example, Seismograph Services ("Seismograph") promised to enter into a joint venture with an inventor to acquire patent rights.[231] While the inventor worked in good faith on the joint venture, Seismograph worked on its own system and planned to forego partnership with the inventor.[232] Seismograph neglected to inform the inventor of its plans after hearing competitors were interested in his work,[233] and "even conjured up a fake demonstration" before cancelling it by way of a fraudulent excuse.[234] Based on this subterfuge, the court announced, "[t]he importance of the equitable issues in this case transcends the interest of the parties. . . . The robber baron morality of another day is no longer acceptable. Courts are insisting on

226. Paine, *supra* note 145, at 426. This practice is discouraged by the code of ethics of both SCIP and Fuld + Co. Strategic and Competitive Intelligence Professionals. *See* FULD + CO, *supra* note 23; *Code of Ethics*, *supra* note 2.

227. 18 U.S.C. § 1839(6) (2012); UNIF. TRADE SECRETS ACT § 1.1 (UNIF. LAW COMM'N 1985).

228. William Cohen & Helena Czepiec, *The Role of Ethics in Gathering Corporate Intelligence*, 7 J. BUS. ETHICS 199, 201 (1988).

229. *Id.*

230. *Id.*

231. Seismograph Serv. Corp. v. Offshore Raydist, Inc., 135 F. Supp. 342, 348 (E.D. La. 1955), *aff'd*, 263 F.2d 5 (5th Cir. 1958).

232. *Id.* at 348–49.

233. *Id.* at 348.

234. *Id.* at 355.

increasingly higher standards of commercial integrity."[235] The court employed its equitable authority to right Seismograph's fraudulent conduct.[236]

Such misrepresentations also occur at the individual level. In one particularly colorful case, a corporate executive at Exxon Office Services had a yet-to-start new hire, named Halpern, arrange a demonstration of a competitor's product.[237] Halpern contacted the competitor under the name of her soon to-be-ex employer and was able to get extensive information from the other company by posing as a potential customer.[238] She then passed the information on to Exxon. The court described this action as a "misappropriation" of the competitor's secret information and ordered the case to prepare for trial on the issue of damages.[239]

Despite the occasional lecture and sanction from the judiciary, corporate trickery by both employers and employees persists, particularly in the context of company-level bad faith negotiations and pretextual customer demonstrations[240] and employee-level undisclosed conflicting loyalties. [241]

Given the survey evidence suggesting that misrepresentation is widespread, it is interesting that the society of Strategic and Competitive Intelligence Professionals specifically condemns posing as a customer or student to gain information about a competitor.[242] It states that their code of ethics "expects that its members must accurately disclose all relevant information, including one's identity and organization, prior to all

235. *Id.* at 354.

236. *Id.* at 354–56.

237. Cont'l Data Sys., Inc. v. Exxon Corp., 638 F. Supp. 432, 435 (E.D. Pa. 1986).

238. *Id.* at 435–36.

239. *Id.* at 441–43.

240. *See* EchoMail, Inc. v. Am. Express Co., 529 F. Supp. 2d 140, 144–45 (D. Mass. 2007) (alleging that EchoMail's customer American Express conducted an "architecture review" of the EchoMail product that American Express used as a pretext for IBM, EchoMail's direct competitor, to obtain confidential and proprietary technology); Den–Tal–Ez., Inc. v. Siemans Capital Corp., 566 A.2d 1214, 1232–33 (Pa. Super. Ct. 1989) (granting a three-year injunction prohibiting acquisition of either competitor where a corporation led on two separate firms about the possibility of a merger, concealing and lying about negotiations to one firm to glean confidential information useful in choosing the better acquisition).

241. *See* Advanced Fluid Sys., Inc. v. Huber, 28 F. Supp. 3d 306, 313–15 (M.D. Pa. 2014) (describing how Advanced Fluid Systems alleged that its salesman Kevin Huber served as a double agent, taking part in a long-running conspiracy to funnel confidential information to a major competitor using his access as an employee to forward sensitive digital information on upcoming projects and commercial strategy); Pope v. Kem Mfg. Corp., 295 S.E.2d 290, 291 (Ga. 1982) ("During the spring of 1981, Kem discovered that Pope, through a corporation acquired by his wife in late 1980, was selling competing products; that is, while calling on Kem's customers and selling Kem's products at Kem's expense, he was also selling competing products to the profit of his wife's corporation. . . . Kem brought suit . . . seeking damages for the period in which it alleges Pope was acting as a double agent . . . ."). Competing employee loyalties also sound in the law of agency, beyond the scope of this Article.

242. *Code of Ethics*, *supra* note 2.

interviews."[243] Further, it adds, "depending on the jurisdiction, misrepresentation may be illegal."[244] Nevertheless, stories of such activities abound,[245] and questioning persons under false pretenses is not a violation of common law privacy in some jurisdictions.[246]

In the context of the Fourth Amendment, however, such strategies are generally permissible. The legality of soliciting information under false pretenses closely relies on a series of precedents that are now known as the "third-party doctrine".[247] Building on the *Katz* test of reasonable expectation of privacy, the third-party doctrine's basic tenet is that there is no reasonable expectation of privacy against warrantless search in information revealed to someone else.

Though the third-party doctrine has had far-reaching effects on electronic surveillance,[248] the principle originates in face-to-face encounters with police informants or undercover agents. For example, in *Hoffa v. United States*, James Hoffa disclosed his participation in several illegal acts to a government informant.[249] The Court held that the Fourth Amendment does not "protect[] a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[250] The Supreme Court further elaborated this principle in *United States v. White*, stating that "one contemplating illegal activities must realize and risk that his companions may be reporting to the police. . . . [I]f he has no doubts, or allays them, or risks what doubt he has, the risk is his."[251] As a result, police informants or undercover policemen may freely solicit or receive incriminating information or observe illicit behavior from suspects without first obtaining a warrant.[252] This use of informants spans a wide range of cases, including disclosing

243. *Id.*

244. *Id.*

245. *See* Sasha Smith, *Spying: How Far Is Too Far? What You Should Know Before Diving in a Dumpster or Cracking a Safe*, CNN MONEY (June 1, 2001), http://money.cnn.com/magazines/fsb/fsb_archive/2001/06/01/304095/index.htm (giving examples of the use of misrepresentation in competitive intelligence).

246. Nader v. Gen. Motors Corp., 255 N.E.2d 765, 770 (N.Y. 1970) (applying D.C. law).

247. United States v. Miller, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."); *see also* Smith v. Maryland, 442 U.S. 735, 745 (1979) (holding that third party doctrine allows phone companies to provide phone records to police without a warrant).

248. *See, e.g.*, Geverd, *supra* note 72, at 198–203 (discussing the case-law establishing records collection and its application by the U.S. Government to electronic data).

249. Hoffa v. United States, 385 U.S. 293, 298–300 (1966).

250. *Id.* at 302.

251. United States v. White, 401 U.S. 745, 752 (1971).

252. For an in-depth discussion of "false friend" cases before the Supreme Court, see Donald L. Doernberg, *"Can You Hear Me Now?": Expectations of Privacy, False Friends, and the Perils of Speaking Under the Supreme Court's Fourth Amendment Jurisprudence*, 39 IND. L. REV. 253, 275–92 (2006).

incriminating information to informants in internet chat rooms,[253] serving alcohol to under-aged undercover agents,[254] selling obscene materials to an undercover officer,[255] and revealing a marijuana grow operation to a customer-turned-police-informant.[256]

We therefore have an interesting contrast between the Fourth Amendment and trade secret. Under the Fourth Amendment, lies and trickery in the service of uncovering criminal activity are perfectly permissible. Under trade secret, they are condemned by some courts and professional organizations but nevertheless are used with at least moderate frequency. This makes the issue of misrepresentation particularly interesting for our purposes.

Public opinion does not diverge as dramatically as the doctrine, however. For the false friend vignette, we presented respondents with an attempt by a police officer or private investigator to pose as a friend of a high-level executive asking about projects and co-workers. For the pretexting vignette, the police officer or private investigator posed as a potential customer seeking information not publicly available. Following the general trend of privacy hierarchy between contexts, respondents found the use of both tactics to be more of a violation of a reasonable expectation of privacy with a corporate investigator looking for trade secrets. Support for misrepresentation by law enforcement has less than majority support in both the false friend (47.5%) and pretexting (39.9%) vignettes, however, despite the fact that they are doctrinally clearly permissible. These results are consistent with earlier work by Slobogin and Schumacher.[257] Tracking disapproval by competitive intelligence scholarship and some courts, we found even less public support for the false friend (30.6%) and pretexting (29.2%) vignettes in the corporate information search context.

C. VISUAL SURVEILLANCE

Visual surveillance occupies a peculiar place in privacy law. It can often be accomplished without committing trespass, thereby avoiding the concerns of the now-familiar property-centric model of Fourth Amendment privacy protection. Consequently, one line of cases suggests that citizens have essentially no reasonable expectation of privacy if their actions can be observed from a public place. The Supreme Court held in *United States v. Knotts* that a suspect could be surveilled through a hidden, battery-controlled tracking device both when he travelled on public roads and when he was located on private property because "[v]isual surveillance from public places

253. *See* United States v. Charbonneau, 979 F. Supp. 1177, 1185 (S.D. Ohio 1997) (holding that defendant did not have a reasonable expectation of privacy in a chat room shared with undercover FBI agents in a child pornography case).

254. Winkel v. Reserve Officer of Beloit, 773 F. Supp. 1487, 1489–90 (D. Kan. 1991).

255. *See* Maryland v. Macon, 472 U.S. 463, 469–71 (1985).

256. United States v. Ward, 703 F.2d 1058, 1062 (8th Cir. 1983).

257. *See* Slobogin & Schumacher, *supra* note 18, at 737–38.

. . . or adjoining [the private property in question] would have sufficed to reveal all of these facts to the police."[258] Not only that, "[n]othing in the Fourth Amendment prohibit[s] the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afford[s] them."[259]

Yet, as we describe below, this is not the end of the story. The use of some sensory-enhancing technologies does implicate the Fourth Amendment, and lower courts are divided on whether video surveillance over an extended period is qualitatively distinct from moment by moment observation.[260]

The propriety of visual surveillance in the context of trade secret law is murky at best, with little guiding case law. One difficulty is whether information that can be publicly observed constitutes a trade secret at all—if information is publicly visible, it may be considered "readily ascertainable by proper means."[261] Another difficulty is that, given the miniaturization of video and still cameras and the availability of high-powered lenses, there are obvious difficulties in detecting whether one is being surveilled. Though law enforcement generally reveals its surveillance techniques during later criminal proceedings, trade secret thieves have little incentive to disclose their successes to their victims. Therefore, we do not have a clear sense of how prevalent visual surveillance is in trade secret cases. This relative paucity of trade secret cases makes this is an important domain for reasoning by analogy.

1. Drones

Aerial photography has a venerable history in the law of trade secret. In *E.I. duPont deNemours v. Christopher*, the Christophers flew over a new plant, under construction by DuPont, to take aerial photography for a commercial rival.[262] The Fifth Circuit held that a claim of trade secret misappropriation does not require a trespass or other illegal conduct, writing:

> [O]ur devotion to free wheeling industrial competition must not force us into accepting the law of the jungle as the standard of morality expected in our commercial relations. Our tolerance of the espionage game must cease when the protections required to prevent another's spying cost so much that the spirit of inventiveness is dampened. Commercial privacy must be protected from

258. United States v. Knotts, 460 U.S. 276, 282 (1983).

259. *Id.* The Supreme Court went on to quote *United States v. Lee*'s holding that the use of a search light or a telescope was not prohibited by the Fourth Amendment to support technologically enhanced visual surveillance within the ambit of a reasonable expectation of privacy. *Id.* at 282–83 (quoting United States v. Lee, 274 U.S. 559, 563 (1927)).

260. *See infra* Sections IV.C.2–.3.

261. UNIF. TRADE SECRETS ACT § 1.4(1) (UNIF. LAW COMM'N 1985).

262. E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1013 (5th Cir. 1970).

> espionage which could not have been reasonably anticipated or prevented.[263]

As aerial photography becomes more ubiquitous through the use of satellite imagery in popular applications like Google Maps or through the use of drones, the scope of what can be "reasonably anticipated or prevented"[264] may have changed from the Fifth Circuit's analysis of more than four decades ago. Drone use has filtered into many aspects of public life, from recreation to entrepreneurship.[265] The low-cost of drones and their unprecedented maneuverability also allows a level of privacy invasion far beyond the top-down photography at issue in *Christopher*. Drones may be able to fly up to a second-story window to peer into a bedroom or capture intimate footage of families on private property.[266] This technology could also allow commercial competitors to photograph trade secrets of their rivals. While a trade secret case using drones has not yet reached the courts, the likelihood that a drone will be used to uncover a trade secret will rise as the number of drones in private hands increases overtime. Courts will then need to determine whether the rule from *Christopher* still applies.

In contrast to trade secret law, the issue of a drone overflight does not present substantial complications under the Fourth Amendment. Even in 1986, long before drones became commonplace, the Supreme Court was willing to hold in *California v. Ciraolo* that aerial observation does not present a Fourth Amendment problem.[267]

> Any member of the public flying in this airspace who glanced down could have seen everything that these officers observed. . . . [W]e readily conclude that respondent's expectation that his garden was protected from such observation is unreasonable and is not an expectation that society is prepared to honor.[268]

This is a fairly straightforward application of the principle that the police are free to observe, from a lawful location, anything that occurs in a public place.

---

263. *Id.* at 1016.

264. *Id.*

265. *See, e.g.*, Timothy T. Takahashi, *Drones and Privacy*, 14 COLUM. SCI. & TECH. L. REV. 72, 81–91 (2012) (providing a detailed explanation of what a drone is and what it can do); Aili McConnon, *Drones Pique the Interest of Entrepreneurs*, N.Y. TIMES (May 25, 2016), https://www.nytimes.com/2016/05/26/business/smallbusiness/drones-pique-the-interest-of-entrepreneurs.html (discussing the use of drones in agriculture, aerial photography, and construction); Carol Pogash, *Santa Delivered the Drone. But Not the Safety and Skill to Fly Them.*, N.Y. TIMES (Jan. 8, 2017), https://www.nytimes.com/2017/01/08/business/drone-safety-risk-popular.html (describing the challenges of drone ownership for everyday consumers).

266. *See* Timothy T. Takahashi, *The Rise of the Drones—The Need for Comprehensive Federal Regulation of Robot Aircraft*, 8 ALB. GOV'T L. REV. 63, 117–18 (2015) (discussing early incidents of invasion of privacy via drone complaints by members of the public).

267. California v. Ciraolo, 476 U.S. 207, 213 (1986).

268. *Id.* at 213–14.

One might think that drone surveillance is qualitatively different than the kinds of observation that would have been at issue in 1986. Drones can and usually do fly quite close to the ground, and they can hover. Though the issue of drones has not yet been litigated at the Supreme Court level, the issue of low-flying helicopters arose not long after *Ciraolo*. In 1989, the Court in *Florida v. Riley* held, consistent with its earlier decision, that observation from a helicopter flying at 400 feet did not violate reasonable expectations of privacy.[269] The Court observed that helicopters flying at 400 feet are sufficiently common that the defendant could have reasonably anticipated that his property would be observed from that altitude.[270] This seems somewhat debatable—how often do helicopters fly over most houses?—but drone flight does not seem to be *rarer* than that of helicopters. Drones are, for one thing, quite a lot cheaper.

There is one ground that might lead to a drones-are-different rule. The Court in *Riley* stressed that it was legal for the helicopter to be where it was.[271] A fixed-wing plane could not have legally flown at that altitude, but a helicopter could.[272] A person in a state or locality that banned drone flight,[273] or drone flight at a given altitude, might have a reasonable expectation of privacy against drone surveillance under *Riley*.

The drone surveillance vignette specified drone surveillance of an industrial complex at seventy feet with detailed photography of the complex. While this vignette also followed the general trend of respondents finding trade secret surveillance more of a violation of privacy than a similar search by law enforcement, drone surveillance revealed a large split between corporate and law enforcement surveillance (3.88 v. 3.04 on a five-point scale). Slightly more than twice as many respondents thought warrantless drone surveillance by law enforcement should be allowed (44.0%) versus the trade secret context (20.4%). The relatively low level of support for the use of a drone overflight in the trade secret context shows some basis in public opinion for the "commercial morality" justification provided by the *Christopher* court, updated for contemporaneous technology. The higher but still low level of support for police use of drones also suggests that it might be time to reconsider Fourth Amendment case law on aerial surveillance.

269. Florida v. Riley, 488 U.S. 445, 450–51 (1989).

270. *Id.*

271. *Id.* at 451. *But see id.* at 455 (O'Connor, J., concurring) (rejecting that basis for the holding and instead suggesting that frequency of flight, rather than legality, should be the crucial test).

272. *Id.* at 451; *see also* 14 C.F.R. § 91.119 (2018).

273. *See generally* Inst. for Nat'l Sec. & Counterterrorism, *Local Regulation*, DOMESTICATING THE DRONE, http://uavs.insct.org/local-regulation (last visited Jan. 2, 2019) (listing regulations by state and municipality).

2. Camera Across Street

Does surveillance of a competitor's store front from across the street with a video camera constitute an improper means of acquiring a trade secret? One commentator on corporate surveillance notes that "it may be possible to ascertain the volume of product that competitors are shipping by observing from public property the number of tractor-trailers leaving the plant's loading bays and by noting the size of the product in relation to the size of the trailers."[274] Although this could be accomplished by a diligent agent without any technological assistance, the use of a video camera from a public place or even private property owned by a competitor is likely less conspicuous and more cost-effective. Similarly, even the fairly cautious ethical standards of the SCIP say that it is "advisable" to investigate the executives at competitors and that it is ethical and legal to hire private investigators to surveil them for that purpose.[275]

While state laws sometimes prohibit "criminal surveillance," the definition of criminal surveillance may not include surveillance from a public place. For example, Alabama law defines criminal surveillance as "intentionally engag[ing] in surveillance while trespassing in a private place."[276] In *Ages Group, L.P. v. Raytheon Aircraft Co., Inc.*, a defendant corporation argued successfully that video surveillance that they conducted from a car did not constitute criminal surveillance under Alabama law because the car was on a public street.[277] Surveillance from a public place appears not to be per se illegal, and no case law provides guidance on when surveillance from a public place might constitute improper means. We can then tentatively conclude that videotaping of public places does not constitute improper means.

Most courts have held that such surveillance is not a search under the Fourth Amendment either. In one typical case, Alcohol Tobacco and Firearms ("ATF") agents had placed a camera on a utility pole across from the defendant's property. As the Sixth Circuit found, the

> agents only observed what [the defendant] made public to any person traveling on the roads surrounding the farm. . . . While the ATF agents could have stationed agents round-the-clock to observe [the defendant]'s farm in person, the fact that they instead used a

274. Paine, *supra* note 145, at 428.

275. *Code of Ethics*, *supra* note 2.

276. ALA. CODE § 13A-11-32 (2015). The associated commentary states, "Surveillance is defined . . . to mean the secret observation of the activities of another person for the purpose of spying upon and invading the privacy of the person observed." *Id.* § 13A-11-32 cmt.

277. Ages Grp., L.P. v. Raytheon Aircraft Co., Inc., 22 F. Supp. 2d 1310, 1321 (M.D. Ala. 1998).

> camera to conduct the surveillance does not make the surveillance unconstitutional.[278]

This is a natural extension of the logic from the drone example: The camera is where it is lawfully allowed to be and is observing only that which the investigation's target has chosen to do in public.

This rule is not without controversy, however. Unlike drones and airplanes, pole-cameras can persist for extended periods, often weeks. Given this possibility, some scholars have called for Fourth Amendment regulation of long-term camera surveillance.[279] Courts are not universally unsympathetic to this perspective.[280] An earlier Sixth Circuit panel had tried to duck the question of pole cameras aimed at backyards, saying "we confess some misgivings about a rule that would allow the government to conduct long-term video surveillance of a person's backyard without a warrant."[281] The South Dakota Supreme Court recently held that pole camera surveillance of a front yard for two months was a Fourth Amendment violation.[282] Nevertheless, the majority rule is that warrants are not required for these kinds of cameras.

This creates an interesting question from the standpoint of trade secret analogies. If the Fourth Amendment is found to prohibit long term video surveillance, this would create a situation where—in contrast to every other

---

278. United States v. Houston, 813 F.3d 282, 287–88 (6th Cir. 2016), *cert. denied*, 137 S. Ct. 567 (2016); *see also* United States v. Jackson, 213 F.3d 1269, 1281 (10th Cir. 2000) (holding that a pole camera is not a search even if it observes the curtilage of a property), *cert. granted, judgment vacated on other grounds*, 531 U.S. 1033 (2000). *Jackson* is still the law of the 10th Circuit. *See* United States v. Cantu, 684 F. App'x 703, 703 (10th Cir. 2017); *see also* United States v. Brooks, 911 F. Supp. 2d 836, 843 (D. Ariz. 2012) (holding that law enforcement's use of a pole camera for long-term surveillance did not violate Fourth Amendment protections). *But see* United States v. Cuevas-Sanchez, 821 F.2d 248, 251 (5th Cir. 1987) (holding that such camera surveillance is a search given the fences erected by the defendant).

279. *See, e.g.*, Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 529–30 (2017); *see also* Jonathan Witmer-Rich, *Metaphysical Fourth Amendment Question: How Long Could a Tiny ATF Agent Sit Atop a Telephone Pole?*, PRAWFSBLAWG (Feb. 8, 2016, 3:49 PM), http://prawfsblawg.blogs.com/prawfsblawg/2016/02/ten-week-camera-surveillance-and-reasonable-expectation-of-privacy.html (arguing various reasons why Fourth Amendment protection is needed for targets of continued law enforcement surveillance).

280. *See, e.g.*, *Cuevas-Sanchez*, 821 F.2d at 251 ("This type of surveillance provokes an immediate negative visceral reaction: indiscriminate video surveillance raises the spectre of the Orwellian state. Here, unlike in *Ciraolo*, the government's intrusion is not minimal. It is not a one-time overhead flight or a glance over the fence by a passer-by. Here the government placed a video camera that allowed them to record all activity in Cuevas's backyard. It does not follow that *Ciraolo* authorizes any type of surveillance whatever just because one type of minimally-intrusive aerial observation is possible."); *see also* Order Granting Defendant's Motion to Suppress at 20, United States v. Vargas, No. CR-13-6025-EFS (E.D. Wash. Dec. 15, 2014) (similarly distinguishing prolonged video monitoring because it "is so different in its intrusiveness that it does not qualify as a plain-view observation").

281. United States v. Anderson-Bagshaw, 509 F. App'x 396, 405 (6th Cir. 2012).

282. State v. Jones, 903 N.W.2d 101, 113–14 (S.D. 2017).

mode of surveillance—the government is more restricted than private parties. We would argue that such a rule, if it arises, should be imported into trade secret. This may be another place where the recent *Carpenter* decision may move Fourth Amendment law.[283] Though *Carpenter* technically only extended protection to cell site location data, it stands with *Jones* and *Riley* as an indication that the Court is open to revisiting apparently settled doctrine in light of changing technology.

The camera-across-the-street vignette asked respondents to evaluate the invasion of privacy presented by a camera set up across the street from the entrance of a corporation, collecting information on who enters and exits. No time duration was specified. The vignette followed the general trend of finding warrantless police surveillance more of a privacy violation than commercial surveillance. Somewhat surprisingly, this vignette produced the largest discrepancy in ratings between trade secret (3.60) and law enforcement contexts (2.71). At 58.7%, support for camera-across-the-street surveillance by law enforcement was strong, only eclipsed by support for trash searches of dumpsters on public land and searches of public financial documents. All three scenarios involve police investigation of essentially public information. Nevertheless, only 28.8% supported this kind of video surveillance for commercial competitors.

3. Lens Through Window

Our final hypothetical is essentially an amplified version of video surveillance by a standard camera. Is there a difference between video surveillance that reveals no more than what can be seen with the naked eye and technology-aided surveillance capable of seeing much more?

There are only a few references to such techniques in the trade secret case law. One brief mention of the use of a high-powered lens in a trade secret context comes from the same case mentioned in the previous hypothetical, *Ages Group*.[284] In that case, an employee of the surveilled company noticed a telephoto lens, a camera attachment that enables the optical magnification of distant objects, on the dashboard of the car used for surveillance.[285] The case does not discuss the use of a telephoto lens as an aggravating factor in determining whether the visual surveillance was improper, however. There is a similar passing mention of vision-enhancing technology in *Columbus Bookkeeping and Business Services v. Ohio State Bookkeeping, LLC*: The plaintiff in a trade secret case testified that information about a client list would be visible inside of an office only with the use of binoculars.[286] But the court found that

283. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

284. Ages Grp., L.P. v. Raytheon Aircraft Co., 22 F. Supp. 2d 1310, 1316 (M.D. Ala. 1998).

285. *Id.* at 1316.

286. Columbus Bookkeeping & Bus. Servs. v. Ohio State Bookkeeping, LLC, No. 11AP-227, 2011 WL 6938340, at *2 (Ohio Ct. App. Dec. 30, 2011).

the information at issue was not a trade secret for other reasons without discussing whether information visible with the use of binoculars from a public place would be readily ascertainable or if the use of binoculars would constitute improper means.[287]

Courts sympathetic to the "corporate morality" justification exemplified by *E.I. duPont deNemours & Co. v. Christopher* could find the use of high-powered lens to reveal the interior of offices to be "espionage which could not have been reasonably anticipated or prevented."[288] Requiring that any private business information be completely obscured from outside observation because text could possibly be read from thousands of feet away through sophisticated technology would arguably "cost so much that the spirit of inventiveness is dampened."[289] It seems ambitious to conclude that corporate America must abandon any view of the outside world when conducting business involving trade secrets, especially given the proverbial prominence of the corner office as a symbol of corporate success. Otherwise one could imagine using a high-powered lens[290] to capture video of a computer screen through the window of a skyscraper from several blocks away, and employing optical character recognition technology[291] to generate a fairly accurate copy of any written material that appears. This level of intrusion is technologically plausible but would likely run afoul of the ambiguous "corporate morality" standard.

Fourth Amendment law is also somewhat unclear on this issue, though the tendency in the case law is to find a violation of suspects' rights if a telescopic lens is used. A police officer strolling down the street is not required to avert their eyes from an unobstructed window; the police are generally free

287. *Id.* at *6 (finding alleged trade secret of client list made readily ascertainable through "social functions, through the office and computers, through business cards on the receptionist's desk, and through unlocked cabinet files").

288. E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1016 (5th Cir. 1970).

289. *Id.*

290. *See, e.g.*, Adam Derewecki, *Are Drones Better Than Telephoto Lenses for Spying? The Answer May Creep You Out*, PETAPIXEL (Aug. 21, 2015), https://petapixel.com/2015/08/21/are-drones-better-than-zoom-lenses-for-spying-the-answer-may-creep-you-out (concluding that a commonly available lens with a double magnification teleconverter is capable of capturing better detail than a camera-equipped drone, showing fine-detail from almost a block away); *see also* Bob Sullivan, *Superzoom Camera is Amazing, But Puts New Lens on Privacy*, THIRD CERTAINTY (July 16, 2015), http://thirdcertainty.com/news-analysis/superzoom-camera-is-amazing-but-puts-new-lens-on-privacy (describing a $600 lens released in 2015 that can magnify an image 83 times). For a look at how the combination of high-powered lenses and drones can threaten privacy, see Jason Koebler, *This Drone Zoom Lens Can Identify Your Face From 1,000 Feet Away*, VICE MOTHERBOARD (Feb. 25, 2015, 2:39 PM), https://motherboard.vice.com/en_us/article/8qxe93/this-drone-zoom-lens-can-identify-your-face-from-1000-feet-away.

291. Optical character recognition ("OCR") converts digital images into machine-readable text files. *What is OCR and OCR Technology*, ABBYY, https://www.abbyy.com/en-us/finereader/what-is-ocr (last visited Jan. 2, 2019). Real-time OCR is commercially available and incorporated in many applications for smartphones and other platforms. *See, e.g.*, ABBYY REAL-TIME RECOGNITION SDK, https://rtrsdk.com (last visited Jan. 2, 2019).

to observe whatever may be seen from a place where they are entitled to be.[292] As the Fifth Circuit somewhat voyeuristically put it, "occupants who leave window curtains or blinds open expose themselves to the public's scrutiny of activities within that part of the house that can be seen from outside the premises."[293] But open curtains do not end the Fourth Amendment analysis. In the apparently rare case that this technologically-aided observation has been discussed, courts have sometimes found that use of a telescopic lens does implicate the Fourth Amendment.[294]

More recent case law has buttressed this somewhat unexpected result. In *Kyllo v. United States*, the Court considered the use of a thermal imaging device to monitor the heat signature of a private home.[295] There the Court held "that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use."[296] There are several obvious differences—the heat-sensor in *Kyllo* is much more exotic than a pair of binoculars and a home is more private than an office. But the result shows that the Court is willing to recognize a distinction between enhanced and unenhanced observations. Similarly, the Court stated in *Florida v. Jardines* that, though the police could generally approach a front door and knock, they could not hang about on a front porch and peer through a window.[297]

Technologically aided visual surveillance is again a case where the Fourth Amendment analogy is of great interest to trade secret law. Restricted to citing trade secret cases, one would have a difficult time assessing whether this use of technology is an improper means. With access to the analogous Fourth

292. *See* Florida v. Riley, 488 U.S. 445, 449–50 (1989).

293. United States v. York, 895 F.2d 1026, 1029 (5th Cir. 1990); *see also* United States v. Fields, 113 F.3d 313, 321 (2d Cir. 1997) ("Although society generally respects a person's expectations of privacy in a dwelling, what a person chooses voluntarily to expose to public view thereby loses its Fourth Amendment protection.").

294. *See* United States v. Smith, 978 F.2d 171, 180 (5th Cir. 1992) (reviewing cases) ("Yet this does not mean that the Fourth Amendment never applies when the curtains are open."); United States v. Taborda, 635 F.2d 131, 138–39 (2d Cir. 1980) ("The vice of telescopic viewing into the interior of a home is that it risks observation not only of what the householder should realize might be seen by unenhanced viewing, but also of intimate details of a person's private life, which he legitimately expects will not be observed either by naked eye or enhanced vision."); United States v. Kim, 415 F. Supp. 1252, 1257 (D. Haw. 1976) ("By opening his curtains, an individual does not thereby open his person, house, papers and effects to telescopic scrutiny by the government.").

295. Kyllo v. United States, 533 U.S. 27, 28 (2001).

296. *Id.* at 34 (citation omitted).

297. Florida v. Jardines, 569 U.S. 1, 6 (2013) ("This right would be of little practical value if the State's agents could stand in a home's porch or side garden and trawl for evidence with impunity; the right to retreat would be significantly diminished if the police could enter a man's property to observe his repose from just outside the front window.").

Amendment cases, the task is clarified. Since these means would often be barred under the Fourth Amendment, they should also be viewed as improper under trade secret.

Our survey results support viewing this lens through the window vignette as extremely intrusive. Respondents rated the vignette as more of a violation of privacy than any of the others except wiretap and trespass to curtilage, both of which are plainly barred. 42.4% thought the lens through the window should be permitted for law enforcement uses, and just 16.7% thought it should be permitted in the trade secret context. These results suggest that courts would match popular opinion if they found that the use of a powerful lens to detect information in corporate spaces constitutes an improper means under trade secret law, and that courts are right to be skeptical even in the Fourth Amendment context.

V. CONCLUSION

These results establish several important propositions for trade secret law. First, we have shown the privacy hierarchy within contexts: The ranking of privacy violations of searches in the trade secret context is very similar to the ranking of searches in the Fourth Amendment context. This is the *sine qua non* for allowing analogies between the two areas; what is more a violation of privacy expectations in one context will also be more of a violation in the other.

Second, we find substantial support for the independent legal wrong approach to improper means within the trade secret. People most strongly condemned searches that violated other laws, such as trespass or wiretapping. Public sentiment also condemned dumpster diving on both public and private land, however, even though only one of these involves a trespass. And the rejection of several techniques of visual surveillance suggests a certain amount of skepticism for emerging technologies. Video cameras and drones are not given a free pass despite their availability in the consumer market and their lack of physical intrusion on protected areas. Hedge funds now sometimes employ satellite imagery to track industrial trends,[298] and these data suggest that use of them to uncover a trade secret would face skepticism from the average jury member.

Finally, public norms support our proposition of a Fourth Amendment floor for trade secret. People drew an extremely strong distinction in favor of allowing more law enforcement searches than commercial ones, establishing the privacy hierarchy between contexts. This suggests that, for a given level of privacy invasion, the threshold for banning a method is higher when the goal of the method is to enforce laws than when the goal is to learn corporate

298. Bradley Hope, *Tiny Satellites: The Latest Innovation Hedge Funds Are Using to Get a Leg Up*, WALL ST. J. (Aug. 14, 2016, 4:37 PM), https://www.wsj.com/articles/satellites-hedge-funds-eye-in-the-sky-1471207062.

secrets. Thus, any search that was even debatably too much for law enforcement was strongly rejected for trade secret.

These empirical findings leave us with three independent justifications for the Fourth Amendment floor for trade secret. The first, as we have just reviewed, is that people want and expect more restrictions on corporate surveillance. One could question this finding in its details. For example, one could insist that the norms of business people, or of business people in a particular industry, are more important than those of the general population. But we see no reason to expect that samples drawn from those populations would meaningfully alter this pattern. Regardless, to the extent that our consideration of public norms draws on theories of democratic legitimacy, we should care about the views of the public as a whole, not some narrow section of it.

The second justification is that treating the Fourth Amendment as a floor for trade secret is entirely consistent with the doctrine. We were not able to identify any search clearly prohibited by the Fourth Amendment that was allowed under trade secret law. Since the hierarchy of searches is relatively similar within the Fourth Amendment and trade secret, it makes sense that one domain would be consistently more or less protective than the other. Here, the doctrine signals that it is the Fourth Amendment, rather than trade secret, that allows more searches.

The final justification is normative. We started with the unexceptional claim that surveillance comes at some privacy cost, and some elements of that cost will be constant regardless of privacy domain. This leads to the conclusion that it will often be informative to consider whether a mode of surveillance is permitted in one area of privacy law when assessing the propriety of the mode in a related domain. The goal in doing so is to extract that which is common —the gravity of the intrusion—while leaving room to differentiate on that which is distinct—often the social value of allowing the search. The empirical consistency in the hierarchy of searches across contexts suggests that there is at least some commonality in gravity of the intrusions between domains. It may be that the commonality is lessened—a search being very intrusive when conducted by the government but less so when conducted by a corporation —when certain kinds of exotic searches are considered, but we saw no indication of that in the moderately-wide range of searches evaluated here.

That commonality having been shown, the remaining question is the one on which the weight of prior scholarship disagrees with us. Many of those who see value in analogizing between the Fourth Amendment and the positive law think that the positive law should set a floor for the Fourth Amendment.[299] That the Fourth Amendment should bar (without a warrant or exception to the warrant requirement) at least as much as is barred by the positive law. We think that, at least in the trade secret domain, this is exactly backwards.

299. *See supra* Part II.

The issue here is one of social value. We want companies to be able to keep trade secrets from each other because it allows for the efficient exploitation of inventions that are ill-suited to other intellectual property regimes. Because we recognize the value in allowing this secrecy, we further want to make the secrecy cheap by allowing companies to rely on a strong trade secret regime rather than investing in costly and wasteful physical precautions. Thus, we restrict the surveillance capabilities of one company to give greater freedom to another. There is not a similar societal interest in allowing corporations to hide criminal activities from the government.

A limitation of this work is that trade secret law concerns, almost exclusively, searches of corporations, whereas the Fourth Amendment concerns searches of both corporations as well as individual citizens. One might object to our claims about the scope of Fourth Amendment privacy and that of trade secret by saying that we have only investigated the Fourth Amendment rights of corporations, and that perhaps individuals can or should get more protection. But corporations only exist through the persons who own, run, and work at them. Surveillance of a corporation is surveillance of those who work there. Chief Justice Roberts based his controversial result in *Burwell v. Hobby Lobby* on exactly this insight:

> [I]t is important to keep in mind that the purpose of this fiction [of the corporate form] is to provide protection for human beings. A corporation is simply a form of organization used by human beings to achieve desired ends. An established body of law specifies the rights and obligations of the *people* (including shareholders, officers, and employees) who are associated with a corporation in one way or another.[300]

An examination of our scenarios shows that this equation of corporations and their (individual and human) members is largely borne out in our study materials: many of the scenarios do involve watching, questioning, or deceiving a company's human employees. That the search was targeted at the corporation does not make the invasion of their individual privacy irrelevant.[301] It is therefore hard to draw a firm line between individual and corporate privacy in this way.[302] Also, as we noted at the close of Part III, our Fourth Amendment results for corporate searches largely parallel what has been found in prior work on Fourth Amendment searches of individuals.

300. Burwell v. Hobby Lobby Stores, Inc., 134 S. Ct. 2751, 2768 (2014).

301. It is somewhat ambiguous in the scenario whether the search of the CEO's backyard targeted the CEO or their company, for example. But that ambiguity would also be present in any actual case.

302. This sets to the side "the home" and "the bedroom," which have no corporate equivalents. But if Jim is walking down the street the police do not need to worry about whether they are surveilling him for his own sake or because of who he works for.

Both empirically and theoretically, therefore, we do not see a strong distinction here.

Our Fourth Amendment floor for trade secret therefore has three independent foundations. It reflects the empirically measured expectations of the ordinary public, it is consistent with outcomes in much of the existing case law and doctrine, and it best serves the theoretical goals of each doctrine.

APPENDIX

A. Instructions and Vignettes

1. Introductory Text:

Law Enforcement

For the next several questions you will be asked to think about police officers conducting investigations. Please read each case carefully and give your honest reactions.

Commercial
For the next several questions you will be asked to think about investigators working for one company trying to learn about that company's competitor. Please read each case carefully and give your honest reactions.

2. Drone

Law Enforcement

As part of a police investigation, a camera-equipped drone controlled by the police flies over an industrial complex at a height of seventy feet. The drone captures detailed photographs of the complex. The complex is owned by ABC Corp., the subject of investigation.

Commercial

In order to obtain information on a commercial competitor, a camera-equipped drone controlled by XYZ Corp. flies over an industrial complex at a height of seventy feet. The drone captures detailed photographs of the complex. The complex is owned by ABC Corp., a competitor of XYZ Corp.

3. Dumpster Searches (Public property and private)

Law Enforcement

As part of a police investigation, police search the dumpster behind an office building looking for discarded confidential letters and office memos from ABC Corp. The dumpster is located on public property, but ABC Corp. owns the building.

As part of a police investigation, police search the dumpster behind an office building looking for discarded confidential letters and office memos from

ABC Corp. The dumpster is located on ABC Corp's private property, but outside the building.

Commercial

In order to obtain information on a commercial competitor, private investigators search the dumpster behind an office building looking for discarded confidential letters and office memos from ABC Corp. The dumpster is located on public property, but ABC Corp. owns the building.

In order to obtain information on a commercial competitor, private investigators search the dumpster behind an office building looking for discarded confidential letters and office memos from ABC Corp. The dumpster is located on ABC Corp's private property, but outside the building.

4. False Friend

Law Enforcement

As part of a police investigation, a police officer questions a friend of Aaron, a high-level employee of ABC Corp., about what she knows about his work, including the projects he works on and who he works with on a daily basis. This information is not publicly known or available.

Commercial

In order to obtain information on a commercial competitor, an employee of XYZ Corp. questions a friend of Aaron, a high-level employee of ABC Corp., about what she knows about his work, including the projects he works on and who he works with on a daily basis. This information is not publicly known or available.

5. Pretexting

Law Enforcement

As part of a police investigation, a police officer solicits detailed information about an unreleased product of ABC Corp. by pretending to be an interested customer. This information is not publicly known or available.

Commercial

In order to obtain information on a commercial competitor, an employee of XYZ Corp. solicits detailed information about an unreleased product of ABC

Corp. by pretending to be an interested customer. This information is not publicly known or available.

6. Camera Across Street

Law Enforcement

As part of a police investigation, a police officer installs a video camera across the street from the entrance to ABC Corp., collecting information that can be used to identify who enters and exits the business and when.

Commercial

In order to obtain information on a commercial competitor, an employee of XYZ Corp. installs a video camera across the street from the entrance to ABC Corp., collecting information that can be used to identify who enters and exits the business and when.

7. Wiretapping

Law Enforcement

As part of a police investigation, a police officer uses an electronic device to secretly listen in on telephone conversations between ABC Corp. and its customers concerning orders for the upcoming month.

Commercial

In order to obtain information on a commercial competitor, an employee of XYZ Corp. uses an electronic device to secretly listen in on telephone conversations between ABC Corp. and its customers concerning orders for the upcoming month.

8. Trespass on Curtilage

Law Enforcement

As part of a police investigation, a police officer walks to the back of a home belonging to ABC Corp.'s CEO. The backyard is not visible from the street. The officer walks onto the back porch and sees sensitive documents on a lawn chair near the back door.

Commercial

In order to obtain information on a commercial competitor, an employee of XYZ Corp. walks to the back of a home belonging to ABC Corp.'s CEO. The backyard is not visible from the street. The employee walks onto the back porch and sees sensitive documents on a lawn chair near the back door.

9. Lens through Window

Law Enforcement

As part of a police investigation, a police officer uses a high-powered lens to take photographs through a window of ABC Corp. from across the street.

Commercial

In order to obtain information on a commercial competitor, an employee of XYZ Corp. uses a high-powered lens to take photographs through a window of ABC Corp. from across the street.

10. Public Financial Documents

Law Enforcement

As part of a police investigation, a police officer reads through publicly posted financial filings to learn about ABC Corp.'s business practices and business partners.

Commercial

In order to obtain information on a commercial competitor, an investigator working for XYZ Corp. reads through publicly posted financial filings to learn about ABC Corp.'s business practices and business partners.