TRADE SECRET PRIVACY EXPECTATIONS

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

ABSTRACT

This Article explores the relationship between trade secret law and privacy in the Fourth Amendment context. It argues that Fourth Amendment restrictions on police surveillance should be viewed as a "floor" for trade secret restrictions on commercial surveillance. This approach to the relationship between public and private surveillance flips that advocated recently by several prominent scholars, but is consistent with the Supreme Court's understanding of trade secret law.

To support this argument, we surveyed a representative sample of adult Americans to assess their understandings of commercial privacy. These participants distinguished sharply between the appropriate privacy rules for law enforcement and competing corporations, rating many more searches permissible when conducted by the government. Within the realm of commercial surveillance, participants create a sensible hierarchy of searches that is broadly consistent with the existing doctrine and suggests a general skepticism of allowing unfettered use of the novel kinds of surveillance permitted by emerging technologies.

[*] 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 Erin Delaney, Laura Pedraza-Fariña, and Nadav Shoked for comments on earlier drafts and Conor Tucker for helpful research assistance.

I. PRIVACY IN THE TRADE SECRET AND FOURTH AMENDMENT CONTEXTS 7

A. TRADE SECRET LAW AND THE AMBIGUITY OF "IMPROPER MEANS" 8
B. COMPARATIVE CLARITY IN THE FOURTH AMENDMENT 14
C. A FOURTH AMENDMENT FLOOR FOR TRADE SECRET 18

II. EMPIRICALLY COMPARING EXPECTATIONS 28

A. STUDY SAMPLE AND PROCEDURE 29
B. SEARCH VIGNETTES 33
C. RESULTS 38

III. TRADE SECRET AND FOURTH AMENDMENT PERSPECTIVES ON COMPETITIVE INTELLIGENCE TECHNIQUES 43

A. INDEPENDENT WRONGS 43
B. FALSE FRIENDS AND PRETEXTS 52
C. VISUAL SURVEILLANCE 56

CONCLUSION 66

APPENDIX 69

A. INSTRUCTIONS AND VIGNETTES 69

Common to both trade secret law and the Fourth Amendment are questions of what is and is not private. Is trash private when it is 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? Or corporate competitive intelligence professionals? Companies often have commercially sensible, if morally debatable, reasons to check up on their competitors. Where is the line for them?

We turn to trade secret law to answer this question. Trade secret allows for a cause of action when one person or company obtains secret and valuable commercial information from another by "improper means."[2] Surveillance is therefore permitted if it is "proper" but can lead to liability if it is "improper." Some means of investigation are obviously improper because they violate other legal rules. For example, physical trespasses and conversion give

[1] *See* Part III.A.3.
[2] *See* Part I.A.

rise to simple torts,[3] and wiretaps and computer hacks violate state and federal statutes.[4] Trade secret easily labels these independent legal violations as "improper means" for obtaining the sensitive secrets of a company, adding its penalties to those already invoked under the other, broken, laws.

There are many harder cases, however. As explained by the comments to the Uniform Trade Secret Act (UTSA),[5] "[i]mproper means could include otherwise lawful conduct which is improper under the circumstances." So in addition to unlawful techniques being improper, there is also a broader set of forbidden techniques that cannot be readily deduced by consulting other laws. Drawing on the Restatement (First) of Torts, the same comment to the UTSA also tells us that "a complete catalogue of improper means is not possible."[6] This creates something of a puzzle for inquisitive corporations that are looking to push the limits of competitive advantage while remaining within the boundaries of the law.

Making matters even less clear, 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."[7] 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."[8] This is hardly a crazy conclusion, but it does not suggest an easy method of categorizing whether acts are improper. As the Court there observed, "'Improper' will always be a word of many nuances, determined by time, place, and circumstances."[9] Similarly, the Supreme Court of Pennsylvania

---

[3] (A casebook?)

[4] 18 U.S.C. § 1030, Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 (2013). *See also* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes,* 78 N.Y.U. L. REV. 1596, 1643 (2003) (describing the prevalence of computer misuse legislation).

[5] *See* Uniform Trade Secrets Act cmt. to § 1 (1985 Amendments) http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf (hereinafter "UTSA").

[6] *Id. See also* RESTATEMENT (FIRST) OF TORTS, § 757 (1939).

[7] *Kewanee Oil Co. v. Bicron Corp*., 416 U.S. 470, 481 (1974).

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

[9] *Id.* at 1017.

has observed that trade secret law depends in part on the amorphous "standards of the business community."[10] Though this reliance on commercial morality leads to some confusion, it has a lengthy pedigree in trade secret. As Catherine Fisk observed, "in the early to middle nineteenth century, courts and firms assessed firm ownership of workplace knowledge as much in ethical as in economic terms. The moralistic tone in which judges, litigants, and businesses framed the debate seems odd to the modern sensibility."[11]

There is similar ambiguity under the Fourth Amendment. Though a trespass or wiretap will generally suffice to implicate Fourth Amendment protections,[12] there are several hard questions involving visual surveillance and minor intrusions onto a person or company's property.[13] These questions turn on whether the government has violated a person's "reasonable expectations of privacy" in conducting their investigation. As with "standards of commercial morality," this phrase is also not overly illuminating.

There is a growing literature in Fourth Amendment law that seeks to give content to the catchphrase "reasonable expectations of privacy" by taking seriously the privacy expectations of ordinary citizens.[14] This literature argues that it is socially efficient and normatively desirable to make the question of reasonable expectations empirical. In part, this uses conformity with public attitudes as a way of ensuring that people are not surprised by a legal standard; if the law is what people expect it to be, one need not worry too much about notice. This can be very helpful in the privacy domain, and the point applies as well in

---

[10] *Coll. Watercolor Grp., Inc. v. William H. Newbauer, Inc.*, 468 Pa. 103, 113 (1976).

[11] 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).

[12] *See* Part III.A.

[13] *See* Part III.A.3 and Part III.C.

[14] *See, e.g.*, Christopher Slobogin & Joseph 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 (1993); Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205 (2016). Matthew B. Kugler & Lior Jacob Strahilevitz, *The Myth of Fourth Amendment Circularity*, 84 U. CHI. L. REV. 1747 (2017), 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 (2016), Bernard Chao, Catherine S. Durso, Ian P. Farrell & Christopher T. Robertson, *Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology*, CAL. L. REV. __ (forthcoming 2017).

commercial privacy as it does in the criminal sphere.[15] For example, a company that thinks its trash is private may inadvertently expose its secrets to public view if it turns out that competitors are indeed allowed to dig. Alternatively, a company that thinks it has no legal recourse against aerial photography may spend inordinate resources taking excessive physical security precautions when instead they could have relied on legal protections.

As surveys have been used to illuminate expectations of privacy in the Fourth Amendment context, we sought to similarly use one to investigate norms of commercial surveillance. There is a rich tradition of looking to the surveys of moral intuitions to get a scientific understanding of such public norms. This is particularly common in the tort context, 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.[16] 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,[17] and to examine whether people really feel free to decline police requests to search their persons and property.[18]

We surveyed a sample of adult Americans that was representative in terms of 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 permit a commercial competitor to gather information using each technique. Consistent with an independent legal wrong approach to improper means, people generally condemned searches that violated other legal rules, such as trespass or wiretapping. They also condemned many other searches, however, including

---

[15] Compare to the Fourth Amendment arguments in, *e.g.*, Kugler & Strahilevitz, *Actual Expectations*, *supra* note 14 at 227.

[16] 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 (2014); Pam Mueller, Lawrence M. Solan, & John M. Darley, *When Does Knowledge Become Intent? Perceiving the Minds of Wrongdoers*, 9 J. EMPIRICAL LEGAL STUDIES 859 (2012).

[17] Janice Nadler & Shari Seidman Diamond, *Eminent Domain and the Psychology of Property Rights: Proposed Use, Subjective Attachment, and Taker Identity*, 5 J. EMPIRICAL LEGAL STUDIES 713 (2008).

[18] Janice Nadler & J.D. Trout, *The Language of Consent in Police Encounters* (with J.D. Trout), *in* OXFORD HANDBOOK OF LANGUAGE AND LAW, L. Solan, P. Tiersma, eds., 326–39, Oxford University Press (2012).

dumpster diving, use of aerial drones, and video surveillance of public places. This represents a sensible hierarchy of searches that is broadly consistent with the existing doctrine and that suggests a general skepticism of new technologically-enabled surveillance.

This survey also gave us an opportunity to explore whether public expectations differed in the government and corporate surveillance contexts. In addition to our trade secret vignettes, we constructed parallel stories in which it was the government, rather than a competitor, conducting the surveillance using those same techniques without a warrant. Intriguingly, people drew an extremely strong distinction in favor of allowing more law enforcement searches than commercial ones.

These results provide a new perspective on the appropriate relationship between public and private privacy standards. Several scholars have argued that the positive law, such as trade secret law and trespass, should be used to inform Fourth Amendment standards. Some have argued that the Fourth Amendment should be read to restrict the government from performing a search without a warrant if that search would be prohibited to a private actor. 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 the positive law.[19] In the trade secret context, these conclusions are not supported by the public's expectations. Instead, people believe and expect the government to have *more* freedom to surveil than do commercial parties, rather than the reverse.

Normatively, we believe that the public is right to draw the line between public and commercial surveillance as it does with the Fourth Amendment, setting a "floor" for trade secret rather than the reverse. Given the different motivations of government actors and corporate competitors, it makes sense for competitors turning to spycraft to labor under greater restrictions than government investigators. From a standpoint of economic efficiency, we want companies to be able to keep trade secrets from each other. This allows for the efficient exploitation of inventions that are ill-suited to other intellectual property

[19] *See* Part I.C.

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 or evade government regulation. Having stronger protection under trade secret is also consistent with historical understandings of trade secret as promoting corporate morality, not corporate privacy.

In Part I, we will begin by reviewing the doctrinal understanding of improper means in trade secret and the connection between trade secret law and Fourth Amendment law. We will discuss previous efforts to link public and private privacy law and lay out the theoretical basis for our proposition for a Fourth Amendment floor to trade secret. We will also establish the empirical questions at the heart of our proposal. Most especially, we will discuss the need to demonstrate that the hierarchy of searches is constant regardless of whether the searcher is a commercial competitor or the government. In Part II, we will present our empirical survey of people's commercial privacy expectations. Here we will show that the hypothesized consistency in the search hierarchy is empirically correct. We will also show that people generally do believe that more search techniques should be permitted to law enforcement than to commercial competitors. We will then turn, in Part III, to current doctrine relevant to the vignettes used in our survey, reviewing trade secret law as it relates to particular means of gathering information and attempting to establish where the ethical lines are drawn. Here we will demonstrate that the idea of a Fourth Amendment floor is consistent with the doctrinal outcomes in the current case law and our survey results. We will conclude by discussing the implications of these results for trade secret doctrine.

I. PRIVACY IN THE TRADE SECRET AND FOURTH AMENDMENT CONTEXTS

Some means of investigation are plainly proper and non-invasive. Much can be learned from a review of a company's

public quarterly financial reports, or by tracking mentions of it in the media.[20] For instance, one competitive intelligence firm suggests looking at local newspapers, press accounts, public court and permit filings, annual reports, and trade show and exhibit documents when performing an initial assessment of a company.[21] This form of information gathering considers only public information, and does not raise concerns under either trade secret or the Fourth Amendment. But other methods are more problematic. Before we review the status of what we view as 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. At the end of the section we will explain our perspective on how the two areas of law should relate to each other—the Fourth Amendment floor for trade secret—and comment briefly on the perspective of prior scholars on this issue.

A. Trade Secret Law and the Ambiguity of "Improper Means"

We first take a step back and review the basic principles of trade secret law. While the protection of techniques and specialized knowledge by individual artisans or guilds is an age-old practice,[22] the roots of trade secret law took hold only in the late nineteenth century.[23] 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 that of the individual employee.[24] By 1868, U.S. courts recognized the duty of employees to protect trade secrets from dissemination as an element of express contracts and, by the turn of the century, as they viewed this as "an implied term in *all* employment."[25] This shift helped transform trade secrets from a specific feature of

---

[20] For example, the competitive intelligence consulting firm Competitive Futures describes how it used of 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. https://www.competitivefutures.com/our-work/competitive-intelligence/ (retrieved August 6, 2017).

[21] Fuld + Co, *Code of Ethics: A Legal and Ethical Competitive Intelligence Guide for Clients* (2014), http://insights.fuld.com/hs-fs/hub/17073/file-1386048874-pdf/Resources/Legal_and_Ethical_Guidelines_for_Clients_%C2%A9_2014.pdf. Fuld + Co is a competitive intelligence firm in Boston.

[22] For a fascinating discussion of the role of European guilds and apprenticeships in the dissemination and regulation of specialized knowledge, *see* David de la Croix, Matthias Doepke, & Joel Mokyr, *Clans, Guilds, and Markets: Apprenticeship Institutions and Growth in the Pre-Industrial Economy*, NAT'L BUREAU ECON. RES. WORKING PAPERS (Mar. 2017).

[23] Fisk, *supra* note 11.

[24] *Id.* at 446.

[25] *Id.* at 483, 494.

certain employment agreements to a widespread element of commerce. Beyond changing the relationship of employers and employees, however, the doctrine of trade secret law also began the nebulous task of setting the boundaries of 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 Uniform Trade Secrets Act (UTSA). Versions of the UTSA have been widely adopted in many states and courts in many jurisdictions—including some that have adopted the UTSA—have borrowed heavily from the language of the *Restatement*. These two sources of law address two related issues. First, what can count 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 law. The new federal Defend Trade Secrets Act largely mirrors the UTSA on these questions with a small exception, noted below.[26]

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.[27] 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."[28] 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 the measures the owner takes to guard it, and the ease with which a competitor could properly acquire it.[29]

Section 757 of the Restatement describes the basic elements of trade secret misappropriation. Note the use of "improper

---

[26] Seyfarth Shaw, *The Defend Trade Secrets Act: What Employers Should Know*, 2016, http://www.seyfarth.com/uploads/siteFiles/practices/163502DefendTradeSecretsActGuideM1.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). This is further discussed below.

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

[28] *See also* RESTATEMENT (FIRST) OF TORTS, § 757, cmt. b.

[29] *Id.*

means," the focus of our survey.

> One who discloses or uses another's trade secret, without privilege to do so, is liable to the other if:
>
> (a) he discovered the secret by improper means, or
> (b) his disclosure or use constitutes a breach of confidence reposed in him by the other in disclosing the secret to him, or
> (c) he learned the secret from a third person with notice of the facts that it was secret and that the third person discovered it by improper means or that the third person's disclosure of it was otherwise a breach of duty to the other, or
> (d) he learned the secret with notice of the facts that it was secret and that its disclosure was made by mistake.[30]

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."[31] The Restatement therefore provides imperfect guidance on this question.

The Uniform Trade Secrets Act, 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 Massachusetts, New York, and North Carolina.[32] The UTSA closely tracks the elements of the Restatement, but was written to provide more clarity for some of the more troublesome or difficult to define aspects of trade secret law. As part of this effort, the UTSA defines a trade secret as:

> information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

---

[30] RESTATEMENT (FIRST) OF TORTS, § 757 (1939)

[31] *Id.*, cmt. f.

[32] Legislative Enactment Status: Trade Secrets Act, UNIFORM LAW COMMISSION (2017) (presenting map where New York, Massachusetts, and North Carolina have not adopted the Act).

> (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.[33]

Both the Restatement's definition of a trade secret and this language from the UTSA implicitly make the breadth of "improper means" relevant to the definitional analysis. Take the UTSA language 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.[34] The first and third of these requirements 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 with whom a business person meets, if one is permitted to surveil them. For the third, the precautions that are "reasonable under the circumstances" will depend on what kind of efforts to penetrate those precautions are expected and permitted. Is satellite or thermal imaging permissible? If so, one must do far more to conceal one's secrets than if such means are prohibited.

Because the extent of proper and improper means informs what can be classified as a trade secret, the issue of improper means is 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, as more than 85% of trade secret cases brought in federal court are against a former employee or business partner.[35] The former employee likely walked out the door with the secret in their head

---

[33] Uniform Trade Secrets Act, § 1.4

[34] *See* Richard F. Dole, Jr. *The Counters of American Trade Secret Law: What Is and Isn't Protectable as a Trade Secret*, 19 SMU SCI. & TECH. L. REV. 89, 94–104 (2016) (discussing the three-part definition of trade secret law); *see generally* Rowe & Sandeen, *supra* note 27, ch. 3.B (reviewing definition and case-law about "generally known" and "readily ascertainable" language); *id.* at ch. 4 (reviewing case-law and drafting history of UTSA's economic value requirement). *id.* at ch. 5 (reviewing definition and case-law about reasonable efforts to maintain secrecy).

[35] David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 303 (2010).

or on a flash drive rather than engaging in any sort of complex surveillance activity, but their old employer must still prove that the appropriated information can count as a trade secret. Consider a few examples of how this requirement can cause problems for firms:

1.) A customer list is not secret if one can follow an employee on his or her rounds and mark where they make deliveries.[36]
2.) Client identities also can be exposed if the firm invites all its clients to a social gathering if a person might observe who attends.[37]
3.) The configuration of a chemical plant may not be a secret if it can be photographed from nearby public land.[38]

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. This double use of improper means makes the determination of whether a given means is "proper" central to trade secret liability.

Given this centrality, it is unfortunate that the "Definitions"

---

[36]Fulton Grand Laundry Co. v. Johnson, 140 Md. 359, 361–62 (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").

[37] Columbus Bookkeeping & Bus. Servs. v. Ohio State Bookkeeping, 2011 Ohio App. LEXIS 5655, *13 ("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.")

[38] Interox America v. PPG Industries, 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.")

section of the UTSA does not greatly clarify "improper means." Rather than provide a definition, the UTSA instead lists a series of examples:

> "Improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means.[39]

In a comment, the UTSA also provides the inverse: a listing of means of discovering a trade secret that are clearly proper:

> 1. Discovery by independent invention;
> 2. Discovery by "reverse engineering", that is, by starting with the known product and working backward to find the method by which it was developed. The acquisition of the known product must, of course, also be by a fair and honest means, such as purchase of the item on the open market for reverse engineering to be lawful;
> 3. Discovery under a license from the owner of the trade secret;
> 4. Observation of the item in public use or on public display;
> 5. Obtaining the trade secret from published literature[40]

From this discussion, it seems clear that means that are otherwise unlawful, such as theft or bribery, constitute improper means. This is sometimes phrased as an "independent legal wrong" approach to determining improper means.[41] However, the UTSA also specifies that "[i]mproper means could include otherwise lawful conduct which is improper under the circumstances."[42]

Intriguingly, the recent federal Defend Trade Secret Acts specifically excludes the possibility that an otherwise lawful investigative means could give rise to federal trade secret

---

[39] Uniform Trade Secrets Act, §1.1

[40] Uniform Trade Secrets Act, § 1 cmt.

[41] *See, e.g.*, Rockwell Graphic Systems, Inc. v. DEV Industries, Inc. 925 F.2d 174, 178 (7th Cir. 1991).

[42] Uniform Trade Secrets Act, § 1 cmt.

liability,[43] though it does not preempt the state laws that do allow for this outcome.[44] 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 follows the example of the UTSA in including "misrepresentation," which—as we explore below—may be "lawful."

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, misrepresentation may yield useful information but is ethically dubious according to many practitioners and scholars.[45] What level of disclosure is needed when asking a person for valuable information? Further complicating matters, the limits of propriety are nebulous at best and may rapidly shift with changes in public attitudes and access to new technology. It is apparently permissible to follow a delivery driver on their route to assemble a customer list. What about using electronic means to accomplish the same end, but at greatly reduced cost? The last few decades have seen dramatic reductions in the size and cost of video-monitoring technology, for example, allowing for the widespread use of video surveillance in public and private spaces by a wide variety of actors. In some cases, the impropriety of a company's action seems to derive from the technique's novelty. A court in 1970 thought that aerial photography was unforeseeable by a reasonable person and declared it an improper means.[46] Now that aerial drones and satellite photography have become ubiquitous, the standards of propriety may have changed. How should courts respond to such shifting norms?

B. Comparative Clarity in the Fourth Amendment

Government actors are regulated primarily by the Fourth Amendment and a small list of statutes regulating particular means of surveillance, such as the Wiretap Act.[47] An almost

---

[43] 18 U.S.C. § 1839(6). It excludes from "improper means" "reverse engineering, independent derivation, or *any other lawful means of acquisition*." (emphasis added).

[44] 18 U.S.C. § 1838.

[45] *See* the ethical codes and academic literature cited in notes 116–120 and the survey data cited in Part III.B.

[46] E. I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1013, 1016 (5th Cir. 1970).

[47] Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 (2013); *id.* § 201; *id.* § 2703

endless series of cases have examined whether the kinds of basic investigative techniques that we are concerned with in this project are appropriate when used by the police without a warrant. As a result, there are many fewer open questions here than in the realm of trade secret.[48] 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 investigations.[49] 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.[50] So corporate surveillance by private citizens will 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*.[51] He 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.'" In subsequent cases, this test was embraced by the Court and has become the key touchstone for determining whether any particular form of surveillance constitutes a "search" within the meaning of the Fourth Amendment.[52] Thus, for nearly fifty years courts have spoken of "reasonable expectations of privacy."

There are three general principles of Fourth Amendment law that help us think through the kinds of investigative techniques most frequently at issue in trade secret cases. The first of these is

---

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

[49] *See*, *e.g.*, Dow Chem. Co. v. United States, 476 U.S. 227, 232 (1986).

[50] *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").

[51] 389 U.S. 347, 362 (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.").

[52] 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* Peter Winn, Katz *and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1 (2009).

an emphasis on property rights, particularly property rights in land. In 1928, the Supreme Court held in *Olmsted 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.[53] By contrast, when a trespass did occur, even a comparatively trivial one, it was a Fourth Amendment violation.[54]

Though the history of this trespass-centric approach to the Fourth Amendment has been questioned,[55] it is still the starting point of modern Fourth Amendment analysis. The *Katz* reasonable expectation of privacy test was added to the existing trespass framework, creating a new way for non-trespasses to violate the Fourth Amendment.[56] 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.[57] 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 they did not have either express or implied permission to be there.[58] Thus, any time the police need to trespass on land to conduct a search, that search is going to implicate the Fourth Amendment unless the police can argue that they had permission, explicit or implicit, to enter the property.

The second basic principle is that the Fourth Amendment does not protect against false friends or breaches of confidence. Under what is called the third-party doctrine, people do not have a reasonable expectation of privacy in information that they

---

[53] Olmstead v. United States, 277 U.S. 438, 466 (1928).

[54] Silverman v. United States, 365 U.S. 505, 512 (1961) (finding physical intrusion by inserting "spike mike" into wall is trespass).

[55] Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV 67, 67–68 (2013) ("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.").

[56] United States v. Jones, 132 S. Ct. 945 (2012

[57] Id.

[58] Florida v. Jardines, 133 S. Ct. 1409, 1415 (2013).

voluntarily disclose to another.[59] If that third-party wishes to, it can disclose that information to the government. "Lower federal courts have 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."[60] Though the third-party doctrine has been criticized at a number of levels and for a variety of reasons,[61] it is still the law. A similar rationale leads to the holding that the use of police informants does not implicate the Fourth Amendment. People know that they are running the risk that those with whom they share information will go to the police.[62] This is a substantial point of contrast with trade secret, which instead assumes or even requires that confidences be kept.

The third principle is that there is no protection under the Fourth Amendment for that which 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."[63] 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."[64] This has led courts to be skeptical of claims that the Fourth Amendment is implicated by video surveillance of public areas. [65] If the area is public, then the actions taken in that area can hardly be private, can they?

---

[59] United States v. Miller, 425 U.S. 435, 442–43 (1976); *see also*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

[60] Timothy J. Gevard, *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 & nn.11–12 (2014) (citing United States v. McIntyre, 646 F.3d 1107, 1111–12 (8th Cir. 2011) (utilities); United States v. Porco, 842 F. Supp. 1393, 1398 (D. Wyo. 1994) (utilities); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (email metadata and websites visited); United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) (ISP subscriber data); United States v. Alabi, 943 F. Supp. 2d 1201, 1207 (D.N.M. 2013), *aff'd*, 597 F. App'x 991 (10th Cir. 2015) (credit card magnetic strip information)).

[61] *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 957 (Sotomayor, J., concurring); Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 44 (2011); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 257 (2006).

[62] Hoffa v. United States, 385 US 293 (1966); *see also* United States v. White, 401 U.S. 745, 752 (1971) (re-affirming *Hoffa*).

[63] Katz v. United States, 389 U.S. 347, 351 (1967)

[64] California v. Ciraolo, 476 U.S. 207, 213 (1986).

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

These principles provide a framework for understanding how courts view the Fourth Amendment issues raised by most of the surveillance techniques described in Parts II and III. They do not fully resolve questions about several of them, however. 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. The harder question was whether they had implicit permission to do so. This question of implicit permission will complicate 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.[66] Second, quite 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.[67] It is unclear exactly how much sensory enhancement is allowed at the margins.

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 penetrate 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 it? This framing is consistent with the long pedigrees of both areas of law as stemming from broader privacy concerns.[68] For example, both are cited as examples of privacy rights in Warren and Brandeis's seminal piece *The Right to Privacy*.[69]

We believe that both trade secret and the Fourth Amendment

---

[66] *See* Part III.A.3,

[67] *See* Part III.C.3.

[68] *See, e.g.*, Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1152 (2000); Sharon K. Sandeen, *Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law*, 2006 MICH. ST. L. REV. 667, 670.

[69] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

concern some 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. Is the Fourth Amendment more protective, or is trade secret? Or do cross-cutting policy concerns result in a mix, where neither regime is consistently more protective than the other?

Guided by the data we present in Part II, we argue that trade secret should be read as barring more means of surveillance than the Fourth Amendment. Though we have found no one advocating for our view, a number of 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, in effect, 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 would reframe the Fourth Amendment inquiry as "has a government actor done something that would be unlawful for a similarly situated nongovernment actor to do?"[70] Several scholars have gone further. For example, Daniel Yeager has advocated that positive law should set a lower-bound for Fourth Amendment protection. 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.[71]

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 implicate Fourth Amendment protections. Richard Re makes a similar argument. Agreeing with the notion of a "Positive Law Floor," he notes that it is likely *more* objectionable for the government to encroach on privacy in a

---

[70] William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1831 (2016).

[71] 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).

given way than it would be for a private party to do so.[72] The government poses "special threats" to people's security given its vast power and its ability to impose criminal sanctions, and so it should therefore be subject to similarly special regulation.[73] The strong focus on private law trespass in the recent *Jones* and *Jardines* cases arguably supports this category of scholars.[74]

Many are deeply skeptical of the views of these pro-analogy scholars. Some, like Richard Posner, are doubtful that strong parallels can be drawn given the substantial differences between the two contexts.[75] In particular, Posner points to the different threshold requirements in each domain.[76] Orin Kerr is similarly somewhat cautious about analogizing to the Fourth Amendment from private law, presumably including trade secret law.[77] 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,"[78] noting substantial doctrinal differences. Kerr includes it as one of his four "models" of the Court's jurisprudence, however, because a number of Supreme Court opinions have drawn upon it. Others scholars, like 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.[79]

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

---

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

[73] *Id.*

[74] United States v. Jones, 132 S. Ct. 945 (2012); Florida v. Jardines, 133 S. Ct. 1409, 1415 (2013). *But see, e.g.*, William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1835–36 (2016) (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).

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

[76] *See id. See also* notes 95–97 and accompanying text.

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

[78] *Id.* at 533.

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

discussions of both areas: "reasonable." For the Fourth Amendment, expectations of privacy must be "reasonable." For trade secret, the precautions that are overcome by improper means must have been "reasonable." As Merriam-Webster teaches, reasonable can mean "not extreme or excessive" or "moderate, fair."[80] It is a word of balance or, in legal jargon, a balancing test.[81]

The thing with balancing tests is that they have two sides and one must consider both.[82] One of these sides, in our view, is ripe for allowing analogies between the Fourth Amendment and trade secret. This analogy-friendly side of the scale is a generalized concern with intrusion and the penetration of private areas. This dimension, call it generalized privacy concern, is hieratical in nature. Some searches cause a great deal of privacy concern and other searches cause far less. We make the empirical prediction, supported by the study reported in Part II, that this hierarchy is largely the same regardless of which sort of actor is performing the search. If data continues to support our view that this hierarchy is the same in both contexts, then it makes sense to draw connections. Knowing a search is extremely intrusive in the Fourth Amendment context strongly implies that it will also be extremely intrusive in trade secret.

It becomes clear that this is an unexceptional claim when considered in terms of physical searches. Imagine that either your employer or a government agent is giving 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 constant.

So analogies are appropriate for that side of the scale. But what sits on the other end? This is where the analogy project experiences difficulties. The weight that goes on the other end of the scale varies sharply depending on whether one is in trade

[80] https://www.merriam-webster.com/dictionary/reasonable

[81] *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.").

[82] *See, e.g.*, Caterpillar Inc. v. N.L.R.B., 803 F.3d 360, 366 (7th Cir. 2015) (explaining that the complete absence of weight on one side of a balancing test meant that the interests on the other side, however light, dominated).

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 by the government in service of some public good. In the trade secret context, we generally want the searched-for information to remain secret. 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.[83] In the Fourth Amendment context, we often want the information sought to be exposed. As the Court has repeatedly indicated, there is little *legitimate* interest in hiding illegal activity from the government.[84] 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 the trade secret and Fourth Amendment contexts there is a legitimate interest in avoiding intrusive searches. This common interest sits on one side of the scale. But in the Fourth Amendment context, the information being sought is information that we generally want to see exposed. In the trade secret context, the information being sought is information that we generally want hidden. Therefore, the weight in favor of searches is heavier in the Fourth Amendment context and will more often outweigh the privacy cost.

This logic can be seen in the Supreme Court's rejection of the relevance of a state law trade secret result to the Fourth Amendment's analysis of aerial photography. In *duPont v. Christopher*,[85] the Fifth Circuit held that trade secret law prohibited aerial surveillance of a chemical plant while it was

---

[83] *See* David D. Friedman, William M. Landes, & Richard A. Posner, *Some Economics of Trade Secret Law*, 5 J. ECON. PERSPECTIVES 61, 67–68 (1991) (establishing a simple model of cost–benefit analysis for the efficient pricing of maintain 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 (1992) (discussing Judge Posner's decision in *Rockwell Graphic Systems, Inc. v. DEV Industries, 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?").

[84] 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); United States v. Jacobsen, 466 U.S. 109, 123 (1984) (holding a drug test of white powder reasonable for the same reason); Illinois v. Caballes, 543 U.S. 405, 408 (2005) (explaining "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.").

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

under construction, deriding such observation as an unworthy trick. But sixteen years later, when Dow Chemical argued that this result under trade secret law indicated that it had an expectation of privacy against such surveillance by a government regulator, the Supreme Court disagreed. The Court observed "[t]he Government is seeking these photographs in order to regulate, not to compete with, Dow."[86] 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 it had no legitimate interest in preventing the government from doing so. As the Court commented, "Governments do not generally seek to appropriate trade secrets of the private sector."[87]

A consideration of the doctrinal differences underscores the dissimilarity in the weight given 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. Trade secret, however, does not insist on perfect security; a trade secret owner need only take "reasonable precautions."[88] Similarly, a secret disclosed to another person in confidence is protected under trade secret law, but not under the Fourth Amendment.[89] These differences suggest that it is consistently harder 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 for trade secret but prohibited under the Fourth Amendment, though there were some areas in which neither law was clear.[90]

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

---

[86] Dow Chem. Co. v. United States, 476 U.S. 227, 232 (1986).
[87] *Id.* at 231.
[88] Posner, *supra* note 75 at 468.
[89] *Id.* at 468; Bruce T. Atkins, *Trading Secrets in the Information Age: Can Trade Secret Law Survive the Internet?*, 1996 U. ILL. L. REV. 1151, 1182–83 (1996).
[90] *See* Part III.

as a reason to reject trade secret. The two best examples of this are from trash search cases. In the earlier of the two, a 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."[91] In our framework, this decision is correct in equating the weight of the privacy intrusion across the two searchers. It is somewhat questionable, however, in assuming 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 that case, faced with the same basic legal question, decided the Fourth Amendment law was again "persuasive."[92] 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."[93]

As detailed below, 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.[94] But these two opposing results highlight a common insight: it feels odd to say that whether trash is protected from a search depends on who is doing the searching.

---

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

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

[93] *Id.*

[94] Conn. Gen. Stat. Ann. § 35–51 (West) ("'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, *Dumpster Diving and the Ethical Blindspot of Trade Secret Law*, 16 YALE L. & POL'Y REV. 195, 215–16 (1997).

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, and that therefore it is perfectly sensible for a searching technique to be permitted the government but denied a corporate actor. So, by our logic, the first of the trash search cases was correct: a grant of Fourth Amendment protection against a particular type of 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 known or readily ascertainable, etc.).[95] Richard Posner explains this difference in terms of the privacy intrusion each area of law prevents. 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.[96] 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. Others have come to similar conclusions for largely similar reasons. Writing on this point, Bruce Atkins observes that "[a] Fourth Amendment-like privacy interest 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."[97]

---

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

[96] *Id.* at 466.

[97] Atkins, *supra* note 89.

In terms of our model, this concern speaks to the weight of the searcher's interest rather than to the magnitude of the privacy invasion. We are positing that the Fourth Amendment interest in searching will always be greater than the trade secret interest in searching. This allows us to say that any time the "heavy" Fourth Amendment interest in disclosure is insufficient to outweigh the privacy concern that the "light" trade secret interest will similarly be unable to do so. This argument questions that proposition: a search that reveals nothing is unpunished under the Fourth Amendment but not trade secret, so now greater costs are being imposed on the Fourth Amendment interest.

We believe that this does not create a substantial problem for our analysis because we are focused primarily on *search methods* and this is a threshold qualification. Threshold qualifications, like the search needing to reveal valuable information for trade secret or the searcher needing to act on behalf of the government for the Fourth Amendment, do not change whether the improper *method* element of the analysis is satisfied. 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 also view this as a question of remedies, with the Fourth Amendment needing to prohibit even fruitless searches given the ex ante incentives of the police. Therefore this difference in scope need not complicate our model.

The second issue raises a somewhat greater concern. The government, generally, has more surveillance capacity than private actors. There are some technologies that are peculiarly accessible to it, and some economies of scale with surveillance that are beyond the means of most corporations. Courts are sometimes sensitive to the kinds of tools the government is able to employ. The aforementioned *Dow Chemical* case, for instance, noted, "It 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."[98] 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

[98] 476 U.S.at 238.

concealing technologies that might thwart the government's law enforcement aims.[99] 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."[100] Taking the Kerr and Ohm 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.[101] This sort of concern feeds back into the "special threats" language cited from Richard Re; the government is more dangerous than most private parties.[102]

The strongest form of the argument could go something like this: There are searches that need to be prohibited for the government 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 the model may break down.

The weaker form of the argument is much 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 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.

---

[99] Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).

[100] Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1320–21 (2012).

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

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

We therefore advocate a Fourth Amendment floor for trade secret. As will be shown in Part III, this is a relatively modest proposal: There is no area in which clear trade secret law permits more searches than does the Fourth Amendment. We are therefore not advocating a doctrinal transformation of existing trade secret law. Instead we seek to provide a framework for trade secret to draw upon as it addresses novel issues. In both trade secret and the Fourth Amendment, a generalized privacy concern is being weighed 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, 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. 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.

II. EMPIRICALLY COMPARING EXPECTATIONS

Our theory of the Fourth Amendment floor for trade secret can benefit from two different empirical tests. The first is whether searches are arrayed in approximately the same rank order regardless of whether they are conducted by law enforcement or a corporate competitor. If this is true, then it is at least defensible to look to Fourth Amendment parallels to determine where a new search fits in the hierarchy of searches. If it is not true, there is a serious problem with our theory.

The second test is whether, holding techniques constant, people judge law enforcement searches to be more acceptable than corporate surveillance. In Part I.C., we laid out our normative justification for using the Fourth Amendment as a floor for trade secret protection. Our main points were that the hierarchy of searches is likely the same in each context, making

analogizing possible, and that *allowing* searches in the Fourth Amendment context more serves the public good than allowing them in commercial espionage, implying that the government should be permitted more searches. Here, we seek empirical support for our points by putting our theory to the test of public intuition. Do people create the same hierarchy of searches regardless of which entity is doing the searching, and do they think that the government should be allowed to conduct more types of searches? It turns out, yes and yes. In Part III, 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

A representative sample of adult American citizens was recruited by Toluna, a professional survey firm with an established panel. The exact demographics of each wave are reported in Table 1. The sample was recruited to match the national population in gender, age, race and ethnicity, educational attainment, and region of residence. Following the census convention, "Hispanic" was asked separate from the racial categories. In a change from some of our past research,[103] participants were allowed to mark an "other" box for gender. A small number of participants did this, and two of these explicitly indicated transsexual or nonbinary identifications. 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. The final sample consisted of 1019 respondents.

[103] *Compare* Kugler & Strahilevitz, *Actual Expectations*, *supra* note 14 at 245, 256 and Kugler & Strahilevitz, *Circularity*, *supra* note 14 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.

Table 1: Demographics of the sample.

% Female	51.8	
% Male	47.6	
% Other	.6	
Age (years)		
Median	46	
Mean	46.26	(16.54)
Political Orientation (1–7)[104]		
Economic	4.12	(1.70)
Social	3.89	(1.79)
Overall	4.02	(1.67)
Race/Ethnicity (%)		
White	76.1	
Black or AA	13.2	
Indian or Native	.8	
SE Asian	4.4	
Hawaiian/Pacific	.2	
Multiracial	2.7	
Other	2.6	
Hispanic (%)	16.71	
Education		
Less than HS	13.3	
HS Diploma/GED	30.4	
Two-Year College	28.7	
Four-Year College	18.0	
Graduate Degree	9.7	

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

We chose a representative sample for this study for several reasons. First, we approach the question of the search hierarchy from a standpoint of generalized privacy concern. We are looking for broadly, if not universally, applicable rules for what is and is not appropriate, and a general population sample is the best place to look for such societal norms. Also, were there an industry where corporate theft was more common, for example, 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.

Second, there is a rich tradition of looking to ordinary

[104] Political orientation was assessed on 1 to 7 Likert scales that ranged from Very Liberal to Very Conservative. Participants rated themselves on "economic issues," "social issues," and "overall."

individuals' perceptions of fairness in tort law as a whole.[105] Research on community code agreement—the degree to which lay attitudes are consistent with legal rules—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.[106] If a case is to be tried in front of a jury composed of everyday people, the law on an issue of public norms should generally make sense to them.

A final reason draws on the competitive intelligence literature. When trying to decide what is and is not ethical, Treviño and Weaver describe investigators as considering the "public disclosure" test.[107] 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, participants were presented with one of two instruction screens. These screens informed them 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, they 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.

---

[105] For a rich account of tort law motivated by concerns of fairness, *see* ARTHUR RIPSTEIN, EQUALITY, RESPONSIBILITY, AND THE LAW ch. 3 (1999).

[106] *See generally* NORMAN J. FINKEL, COMMONSENSE JUSTICE: JURORS' NOTIONS OF THE LAW (2001); Janice Nadler, *Flouting the Law*, 83 TEX. L. REV. 1399 (2005). Paul H. Robinson & John M. Darley, JUSTICE, LIABILITY, AND BLAME: COMMUNITY VIEWS AND THE CRIMINAL LAW (1995); TOM R. TYLER, WHY PEOPLE OBEY THE LAW (2006); Paul H. Robinson & John M. Darley, *The Utility of Desert*, 91 NW. U. L. REV. 453 (1997); Tom R. Tyler & Robert J. Boeckmann, *Three Strikes and You Are Out, but Why? The Psychology of Public Support for Punishing Rule Breakers*, 31 LAW & SOC'Y REV. 237 (1997).

[107] Linda H. Treviño & Gary A. Weaver, *Ethical Issues in Competitive Intelligence Practice: Consensus, Conflicts, and Challenges*, 8 COMPETITIVE INTELLIGENCE REV., 61, 69 (1997).

The full text of the instructional screen and all scenarios is given in Appendix A and they are further described in Part II.B.

For each of the scenarios, participants were asked "Does this violate a reasonable expectation of privacy?" They 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 question mirrors what one of us previously to measure expectations of privacy in the law enforcement context.[108] Use of this question in both contexts allowed us to conduct an apples-to-apples comparison between searches conducted by these two types of 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.[109] We therefore asked simply "Should a competitor be legally allowed to look for information this way?" for the commercial competition searches. Since the general public has some background knowledge of law enforcement procedures from popular culture and the news, this question was rephrased slightly for the police search: "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. This question was 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.[110] Duckitt's authoritarian

---

[108] Kugler & Strahilevitz, *Actual Expectations*, *supra* note 14.

[109] 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.

[110] *See* Bob Altemeyer, *The Other "Authoritarian Personality,"* 30 ADVANCES IN EXPERIMENTAL

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.[111] In previous work it was shown to be related to privacy expectations regarding law enforcement searches.[112]

B. Search Vignettes

The vignettes each described a search of something related to ABC Corp. The first line of each vignette reinforced the identity of the searching party. Each of the police scenarios began "As part of a police investigation. . ." and each of the commercial competition scenarios began "In order to obtain information on a commercial competitor. . ." The longest police scenario was fifty words, the shortest twenty-five 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, proudly displays the results of its investigations in order to prosecute and convict criminals.[113] This is particularly a problem for our "Visual Surveillance" category, because that surveillance trespasses on no land and leaves no obvious physical traces, making it very difficult to detect.

Those studying competitive intelligence are well aware of this problem. Linda Treviño and Gary Weaver interviewed a number of people in the competitive intelligence field and were struck by the "intense pressure" that could be brought to bear on those working in the industry. One of their respondents was quoted as saying "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.

SOCIAL PSYCHOLOGY 47–92 (1998).

[111] 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 et al., *A Tripartite Approach to Right-Wing Authoritarianism: The Authoritarianism–Conservatism–Traditionalism Model*, 31 POL. PSYCH. 685–715 (2010). The other two authoritarianism scales developed by Duckitt and colleagues (authoritarian aggression and traditionalism) were also administered. We believe that authoritarian submission is a better measure of the ideology construct for these purposes, however.

[112] Kugler & Strahilevitz, *Actual Expectations*, *supra* note 14 at 254–55.

[113] But see Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, N.Y.U. L. REV. ONLINE (2017) (describing police efforts to conceal their use of stingray devices).

They don't care how you get it."[114] Others they 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.[115]

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

1. Those involving deceit or some form of misrepresentation;
2. Attempts to influence the judgments of those entrusted with confidential information (e.g., bribery)
3. Covert surveillance
4. Theft[116]

She explains, "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."[117] This is in contrast to relying on publicly available information, including information that firms are obligated to disclose to government regulators.[118] 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).[119] 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).[120] Fuld omits references to covert surveillance, but this may be because the document focuses very heavily on what

---

[114] Treviño & Weaver, *supra* note 107 at 70.

[115] *Id.* at 66–67.

[116] Lynn S. Paine, *Corporate Policy and the Ethics of Competitive Intelligence Gathering,* 10 J. BUS. ETHICS. 423, 425–26 (1991).

[117] *Id.* at 426.

[118] *Id.*

[119] Strategic and Competitive Intelligence Professionals (SCIP), *Code of Ethics* (2017), http://www.scip.org/?page=CodeofEthics.

[120] Fuld + Co, *Code of Ethics, supra* note 21.

not to do rather than what *to* do. Treviño and Weaver cite similar categories.[121]

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 III. 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.

The full text of all vignettes is in Appendix A. These vignettes were intended to represent a range of possible conduct. The wiretap, a violation of clear statutory law, was intended to 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. This was intended to evoke a minimal response; it is very hard to argue that this could be a violation of either trade secret law or the Fourth Amendment. The other searches ranged between them. As described in Part III, 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 (state depending) would likely be viewed as improper under trade secret

[121] Treviño & Weaver, *supra* note 107 at 63–64.

law.[122]

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 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.[123] The corporate context suggests two possible dumpster locations that might arguably produce different outcomes. The dumpster could be on the company's own property, meaning that trespass would be necessary to reach it. For instance, one could imagine a dumpster in a private loading dock area. 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*.[124] There were therefore two versions of the dumpster search. One said that the dumpster was behind the ABC Corp. building but on public land, and one 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; 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.[125] This could lead to people finding an expectation of privacy in the pretexting and false friend scenarios. The Slobogin and Schumacher data suggest a number of points of agreement between public expectations and doctrine, however. Their participants rated monitoring of a telephone for thirty days as one of the most intrusive searches in their sample, consistent

---

[122] *See* discussion in Part III.

[123] *See* Part III.A.3

[124] 97 A.3d 1053, 1056 (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.

[125] Slobogin & Schumacher, *supra* note 14 at 737–38.

with Fourth Amendment doctrine and the Wiretap Act.[126] 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. Similarly convergent with doctrine, examining trash at the curbside was much less intrusive than these other cases, and was on par with observing a property from a helicopter at an altitude of 400 yards.[127]

Though the Slobogin and Schumacher data is especially comprehensive, addressing fifty different search types, it is over twenty-five years old at this point, and it was based on a small and non-representative sample.[128] Prior research has shown that sample demographics matter in the Fourth Amendment context,[129] and the age of a survey may be relevant in domains where technology is changing.[130] More recent surveys of Fourth Amendment attitudes have covered on 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.[131] Another recent study by Henry Fradella and colleagues with a non-representative sample found no expectation of privacy in garbage at the curbside.[132] If the curbside is public property—a fair if nonessential inference—that would be consistent with the doctrinal prediction. The same study further found a strong expectation in the case of wiretaps, again consistent with doctrine.[133]

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

---

[126] *Id.*

[127] *Id.*

[128] *Id.* at 737, 750.

[129] Kugler & Strahilevitz, *Actual Expectations*, *supra* note 14 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).

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

[131] *Id.* at 259.

[132] Henry F. Fradella et al., *Quantifying* Katz: *Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 357 (2011).

[133] *Id.* at 359.

colleagues study almost 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 were opposed to warrantless observation at 400 feet.[134] Another study found that a majority of people both thought that the police would not be violating an expectation of privacy to use drones to monitor people in public places, but should need a warrant to monitor a backyard.[135] 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 hierarchy of searches was consistent across the trade secret and law enforcement domains. As can be seen in Table 2, it generally was. 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. The independent legal wrongs of wiretap and trespass to curtilage are the largest privacy violations in each context, and the investigation of the dumpster on public land and the review of public documents are the least.

Looking further at the cross-vignette variation reveals a number of other interesting patterns. Regarding the independent wrong category, both competitors and the government are barred 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 percentage point difference, for the trade secret search it is a 20 percentage point difference. Recall that, unlike the other searches, the public and private land variants of the dumpster search were not shown to

---

[134] *Id.* at 354.

[135] 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, 132 (2016).

overlapping sets of participants—people only saw one or the other—and the difference in scenario wording was quite small. These factors suggest that the participants were quite sensitive to this small shift in the fact pattern. Consistent with the approach of some courts post-*Jardines,*[136] it apparently 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 land shockingly close to the 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. Corporate competitors would be barred in both cases, as is the law in some states.[137]

Table 2: Expectations of privacy and permissibility judgements.

	Expectation of Privacy				Police–Trade Secret Difference		Should be Allowed	
	Trade Secret		Police		F	η2	Trade Secret	Police
Wiretap	4.44 a	(1.11)	3.98 a	(1.24)	38.85 ***	.037	9.6%	17.7%
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 5 point scale question with higher numbers indicating greater violations of privacy expectations. Means within a column that do not share categories designated by letters are significantly different from each other.[138] F statistics are for the Trade Secret–Law Enforcement comparison. *** $p < .001$; *, $p < .05$.

[136] *See* Part III.A.3.

[137] Conn. Gen. Stat. Ann. § 35-51 (West).

[138] 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.

There are two interesting nuances for the misrepresentation and false friend vignettes. First, consistent with Slobogin and Schumacher,[139] people are much more skeptical of law enforcement use of these techniques than one might expect based on the doctrine. So, though our finding is surprising because it varies substantially from current law, it is not an unprecedented result. 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. 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.

Regarding visual surveillance, arguably a hard issue under the Fourth Amendment, we again have two interesting results. First comes from the perspective of the Fourth Amendment itself. The drone and camera-across-the-street vignettes were as worrying to people as the minor trespass of searching a private dumpster. The use of the high-powered lens was more worrying in both contexts. Borrowing from *Jardines*, one might view the use of a high-powered lens to be as offensive as walking onto the curtilage and sticking one's nose up against the window. 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. These results, to our knowledge novel in this area, may help inform courts as they consider this question.

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.

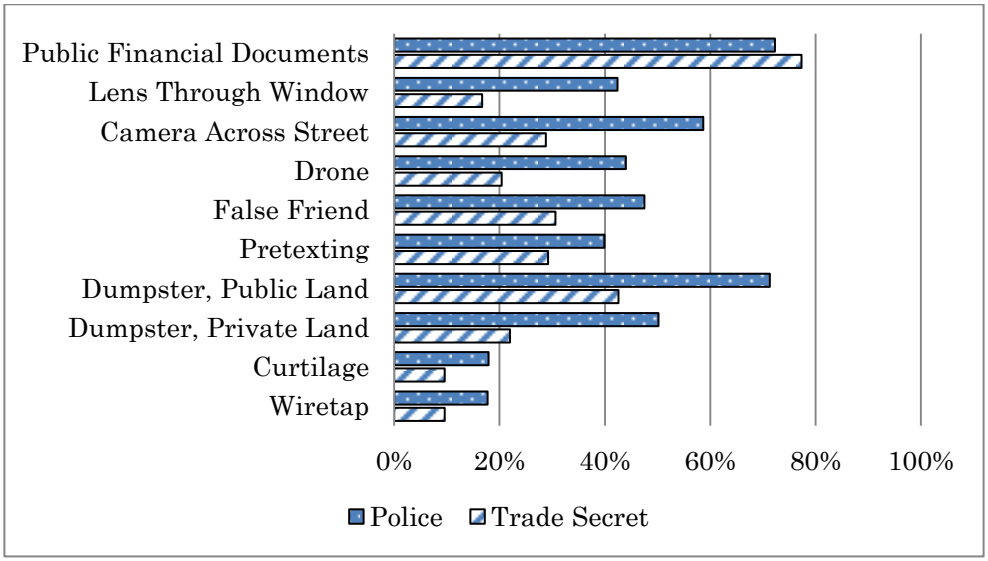
The second question we investigated was the relationship between trade secret and Fourth Amendment expectations overall. There is a significant difference on every single search. This includes searches that almost everyone thought should not be permitted to either party (wiretaps and violations of curtilage)

[139] Slobogin & Schumacher, *supra* note 14 at 737–38.

as well as searches that almost everyone thought should be permissible to both parties. In each case, 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 difficulties that would arise for the reverse proposition: many searches that people would bar to companies, they would not bar to the government.

There was a further interesting difference across contexts. In the police surveillance domain, the average expectation of privacy score correlates with authoritarianism, $r(507) = -.23$, $p < .001$. 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 $r(508) = +.053$, $p = .23$.

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,[140] some might find it surprising

[140] *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) (reporting a survey finding that 45.5% of Americans chose the neutral "strong enough" option while slightly less than 40% found privacy laws not strong enough) https://www.lawfareblog.com/public-not-fussed-about-surveillance-state-confidence-intelligence-

that the difference between the police and corporate surveillance vignettes is both large and more favorable to the government than corporate investigators. But many scholars have noted an equally powerful anti-corporate intuition 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.[141] People are harsher toward corporate defendants even when the wealth of corporate and individual defendants is equated.[142] People are more inclined to hold corporate actors liable for accidental harms than identically situated individual actors.[143] 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.[144] So 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 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 this data that corporations are being denied

---

community-and-its-authorities ; Rainie & Maniam, *supra* note 130 (describing the volatility of public sentiment on surveillance based on events such as secret surveillance carried out by the government and terrorist attacks).

[141] 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).

[142] *Id.* at 125–27, 140.

[143] 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 (2014) (showing that respondents were harsher toward a tort defendant when they had inflicted the plaintiff's injury while on business).

[144] 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).

privacy protection. Some of our law enforcement scenarios overlapped with prior work that used individual criminal defendants as the surveillance target. Despite our use of a corporation rather than an individual as the subject of surveillance, we replicated the results of several prior projects by finding no expectation of privacy in garbage left in a container on public land.[145] We also had approximately the same reactions to our drone surveillance[146] and camera-across-the-street vignettes as have been observed in prior research.[147] 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.

III. 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 these areas and review their relevance to our results. In our review, we seek to highlight both the clear rules and the challenging cases. As suggested in Part I, there is more clarity in the Fourth Amendment's approach to these areas than there is in that of trade secret. Nevertheless, some common conclusions can be drawn. 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 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 is generally agreed 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

One of the clearest cases under both Fourth Amendment and trade secret law is the use of a wiretap to monitor telephone or

[145] *See* note 132 and accompanying text.
[146] *See* notes 131–32 and accompanying text.
[147] *See* note 131 and accompanying text.

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."[148] 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 was necessary. 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."[149]

Use of wiretaps by law enforcement is governed at the federal level, by the Electronic Communications Privacy Act (ECPA).[150] Under its provisions, a "super search warrant" must be obtained before a wiretap can be authorized.[151] In addition to a statement of probable cause, a super warrant requires a specific description of how the communication will be intercepted, the type of communication, and the duration of the interception.[152] The interception of nonrelevant communications must be minimized.[153] The length of time a wiretap can run without further judicial review is also limited.[154] 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."[155] Wiretapping is therefore all but explicitly mentioned. Further, the ECPA regulates both government and private wiretaps, and provides for a private right of action,[156] as do the laws of many states. Civil wiretap claims are not uncommon, and arise in a variety of contexts, including divorce cases.[157] Since wiretapping

---

[148] Katz v. United States, 389 U.S. 347, 353 (1967).

[149] *Id.*

[150] 18 U.S.C.A. § 2511.

[151] 18 U.S.C.A. § 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, 631–32 (2003).

[152] 18 U.S.C.A. § 2518(4).

[153] 18 U.S.C.A. § 2518(5).

[154] *Id.*

[155] Uniform Trade Secrets Act, §1.1.

[156] 18 U.S.C.A. § 2511 (4)(a).

[157] Epstein v. Epstein, 843 F.3d 1147, 1149–50 (7th Cir. 2016).

is illegal, it easily satisfies the independent legal wrong standard for whether a means is improper. Hard questions of commercial morality need not be reached. Both the Code of Ethics of SCIP and the recommendations of Fuld + Co stress that wiretapping is illegal and unethical.[158]

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, 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 v. 3.98 on a 5-point scale, significant at the $p < .001$ level). The legal sanction for wiretapping enjoys strong support from the public.

2. Trespass

Many privacy protections are linked to rights in real property and enforced in part through doctrines developed in cases of physical trespass.[159] The common law of trespass is straightforward. "One is subject to liability to another for trespass, irrespective of whether he thereby causes harm to any legally protected interest of the other, if he intentionally . . . enters land in the possession of the other, or causes a thing or a third person to do so. . . ."[160] This makes trespass an easy case for trade secret. As an independent legal wrong, trespass is a per se improper means in trade secret law. The ethics literature on competitive intelligence is unsurprisingly uniform in condemning trespass.[161]

Despite the central focus on trespass in several recent Fourth Amendment cases,[162] 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

---

[158] SCIP, *Code of Ethics, supra* note 119; Fuld + Co, *Code of Ethics, supra* note 21.

[159] *See* Part I.B.

[160] Restatement (Second) of Torts § 158 (1965)

[161] Paine, *supra* note 116, at 428; Fuld + Co, *Code of Ethics, supra* note 21; SCIP, *Code of Ethics, supra* note 119.

[162] *See* Part I.B.

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. [163] The Court reaffirmed this open fields rule after it adopted the *Katz* test. In *Oliver v. United States,*[164] the police obtained evidence from a field of "highly secluded" illicit marijuana by putting up a locked gate and several "No Trespassing" signs.[165] Nonetheless, the Court held that the owner did not have a reasonable expectation of privacy, explaining "open fields do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or surveillance" and that it is difficult to completely prevent open fields in rural areas from being observed by the public.[166] The Court clarified that "[o]pen 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."[167]

In contrast to an open field, the land closest to a house, its curtilage, receives full Fourth Amendment protection. The text of the Fourth Amendment explicitly grants protection to the home, and a curtilage is typically viewed as an extension of the home.[168] In *Oliver*, the Supreme Court 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.'"[169] The Court thought that in the majority of cases "the boundaries of the curtilage will be clearly marked" and the definition necessary to distinguish between what was curtilage and what was open field would be

---

[163] *Hester v. United States*,265 U.S. 57, 59 (1924).

[164] Katz, 389 U.S. at 351. This property- and place-based conception of privacy has been revived more recently. *See*, *e.g.*, Florida v. Jardines, 569 U.S. 1, 7 (2013) (identifying curtilage as a "constitutionally protected area" and eschewing a discussion of reasonable expectation of privacy) (Scalia, J.).

[165] *Id.*

[166] *Id.* at 179.

[167] *Id.* at 180, n.11.

[168] *See* Brendan Peters, *Fourth Amendment Yard Work: Curtilage's Mow-Line Rule*, 56 STAN. L. REV. 943, 944–45 (2004).

[169] Oliver, 466 U.S. at 180 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886).

"easily understood from our daily experience."[170] More recently, the role of trespass and the primacy of the protection of curtilage played a central part in *Florida v. Jardines*.[171] There, Justice Scalia, writing for the majority, 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."[172]

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, 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.

Trespass therefore presents an interesting contrast between trade secret law and the Fourth Amendment. Under trade secret, whether a trespass counts as an improper means is a relatively easy question. Under the Fourth Amendment, some trespasses count more than others. This distinction within the Fourth Amendment impacts the next area that we will address: trash searches.

3. Dumpster-Diving

The age-old adage that one man's trash is another man's treasure holds true in the realm of corporate espionage. "Dumpster diving is one of the easiest and safest ways of gathering confidential information, and yield secrets ranging from corporate executives' travel itineraries to description of company merger plans."[173] Corporations generate huge amounts

---

[170] *Id.*, 182 n.11.

[171] Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013).

[172] *Id.* at 1417.

[173] Harry Wingo, *Dumpster Diving and the Ethical Blindspot of Trade Secret Law*, 16 YALE L. & POL'Y REV. 195, 200 (1997).

of sensitive paper and, when these companies are careless, enterprising investigators can fish this valuable corporate information from the rubbish bin.[174] As a result, many privacy-minded corporations have employed document management strategies that include shredding sensitive documents, often on-site.[175]

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.[176] 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.*[177] Winne, a rope manufacturer, ordered an employee to collect the trash of rival Palmer, and the proprietary information found in the trash was used to expand Winne's sales territory.[178] Previous cases had recognized a privacy interest in trash so long as its origin was identifiable,[179] but *Greenwood* conceived of trash as open to the public from the moment it was placed in a receptacle accessible to the public.[180] 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."[181] 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.[182]

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.[183] While Greenpeace had voluntarily dismissed its trade secret claim earlier in the litigation to allow for the appeal to the DC Circuit, the appellate court did address Greenpeace's interest in its trash

---

[174] *See generally id.*, 199–202 (describing the degree of care corporations use to securely dispose of sensitive information).

[175] *Id.*

[176] 486 U.S. 35 (1988).

[177] 1991 WL 155819, at *1 (E.D. Pa. Aug. 7, 1991).

[178] *Id.* at *1.

[179] *See, e.g.*, Tennant Co. v. Advance Mach. Co., 355 N.W.2d 720, 725 (Minn. Ct. App. 1984).

[180] *Palmer*, 1991 WL 155819 at *3.

[181] *Id.* at *4.

[182] *Id.*

[183] 97 A.3d 1053, 1057–58 (D.C. Ct. App. 2014).

in the context of corporate espionage and its claim of conversion.[184] Here, the court held that Greenpeace had forfeited its 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."[185] Other cases provide evidence of the practice of trade secret misappropriation through dumpster-diving and other trash thievery.[186]

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. Some courts framed this result in terms of abandonment: if you are trying to get rid of a piece of personal property, how can you still have a privacy interest in it? Accordingly, a number of courts have held that a search of trash is permissible under the Fourth Amendment even if conducting the search requires trespassing on private land.[187] These cases have often distinguished between land that is 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.[188] In *United States v. Hall*, for example, a search of a company's dumpster was upheld even though accessing the

---

[184] *Id.*

[185] *Id.*, 1063 (internal quotations omitted) (citing *Danai v. Canal Square Assocs.,* 862 A.2d 395 (D.C. Ct. App. 2004).

[186] 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. 2005 WL 327536 (E.D. Penn. 2005). In *AlphaMed Pharmaceuticals Corp. v. Arriva, Pharmaceuticals, Inc.*, AlphaMed accused Arriva of pulling trade secret documents from its trash. 2005 WL 5960935 (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." 2003 U.S. Dist. LEXIS 842, *13 (N.D. Tex. May 19, 2003).

[187] 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).

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

dumpster required walking forty feet onto private property.[189] There the court fixated on the lack of signs, barricades, and similar obstacles to public access.[190] This represents another exception to the general rule that trespasses are Fourth Amendment searches.

As noted in Part I.B, however, two recent Supreme Court cases have reaffirmed the role of trespass in the Fourth Amendment analysis and call these earlier decisions somewhat 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.[191] It may violate the Fourth Amendment when a government agent trespasses on property to obtain information even if the trespass is small.[192] 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.[193]

Lower courts are somewhat divided on the implications of these new cases, which question the broader use of implied consent that was employed in the 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. For example, the Kentucky Supreme Court drew on the *Jones* case to hold that that removal of trash from the curtilage of a property *does* violate the Fourth Amendment under *Greenwood*.[194] Thus a dumpster sufficiently close to a house or corporate office would be protected. The Fourth Circuit in *United States v. Jackson* technically agreed with this conclusion, but defined a property's curtilage so narrowly that most trash searches would be permissible.[195]

---

[189] United States v. Hall, 47 F.3d 1091, 1094–95 (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).

[190] *Id.* at 1096.

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

[193] Florida v. Jardines, 133 S. Ct. 1409, 1414, 185 L. Ed. 2d 495 (2013)

[194] Com. v. Ousley, 393 S.W.3d 15, 33 (Ky. 2013).

[195] United States v. Jackson, 728 F.3d 367, 373–75 (4th Cir. 2013) (suggesting that post-*Jardines*, a trash pull from inside the curtilage of a home would be a Fourth Amendment violation, but construing curtilage narrowly to allow the search of a trash can that was not yet put to the

This is also the one area that we will discuss that is substantially affected by state constitutions. In the wake of *Greenwood*, several state supreme courts interpreted their state constitutions as protecting against trash searches, going further than the federal Fourth Amendment.[196]

Overall, then, we largely have convergence between trade secret law and the Fourth Amendment on this question. Trade secret, drawing on *Greenwood* and the Fourth Amendment, treats trash as public. 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. The Fourth Amendment is also generally friendly toward trash searches, but this tendency is similarly complicated if the police need to enter a property to collect the trash.

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, 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 would be 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% v. 42.6% for trade secret; 50.2% v. 71.3% for a police search). While more than 70% of respondents supported police searches of public trash, the most clearly permissible scenario of the four vignettes, support for the other three was more variable, ranging from just over a fifth of respondents for corporate searches of trash on private land to just over half for police searches of the same. In sum, it is never okay to trespass on private land to search trash under trade secret, but it is a

curb for collection because it was in a common area). *See also*, United States v. Castleman, 795 F.3d 904, 913 (8th Cir. 2015), *cert. denied*, 136 S. Ct. 912, 193 L. Ed. 2d 802 (2016) (officers could search trash bags found in an "open field" without a warrant").

[196] *See, e.g.,* State v. Goss, 150 N.H. 46, 49, 834 A.2d 316, 319 (2003) (holding that the New Hampshire constitution does protect against trash searches, going further than *Greenwood*). State v. Hempele, 120 N.J. 182, 223, 576 A.2d 793, 814 (1990) (holding 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).

closer case when no trespass is required. Conversely, it is always okay for law enforcement to search trash if no trespass is required, but is a borderline case when a trespass does occur. In our view, this ambiguity is an appropriate match with the fact-dependent and occasionally contradictory lower court decisions discussed above.

B. False Friends and Pretexts

Though the domain of independent legal wrongs is one of convergence between the Fourth Amendment and trade secret law, this domain is one of extreme divergence. In the trade secret domain, the ethical acceptability of soliciting information under false pretenses is fiercely disputed. Many ethical guidelines advise against such tactics,[197] and both the UTSA and federal Defend Trade Secrets Act explicitly list "misrepresentation" as an improper means.[198] In one somewhat dated survey of competitive intelligence professionals, however, between 30% and 45% of respondents said their company uses misrepresentations to gather information, and twice as many thought other firms would do so.[199] 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. Similarly, 63.2% 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.

The boundaries of deceit and misdirection acceptable under trade secret are challenging to define. Businesses sometimes negotiate in bad faith as a pretext to misappropriate 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.[200] While the inventor worked in good faith on the joint venture, Seismograph worked on its own system and planned to forego partnership with the

---

[197] Paine, *supra* note 116, at 426. This practice is discouraged by both SCIP and Fuld + Co. SCIP, *Code of Ethics, supra* note 119; Fuld + Co, *Code of Ethics, supra* note 21.

[198] Uniform Trade Secrets Act, §1.1. 18 U.S.C. § 1839(6).

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

[200] *Id.* at 348.

inventor.[201] Seismograph neglected to inform the inventor of its plans after hearing competitors were interested in his work.[202] Seismograph even "conjured up a fake demonstration" before cancelling it by way of a fraudulent excuse.[203] Based on this subterfuge, the court announced, "The importance of the equitable issues in this case transcends the interests of the parties . . . . The robber baron morality of another day is no longer acceptable. Courts are insisting on increasingly higher standards of commercial integrity."[204] The court employed its equitable authority to right Seismograph's fraudulent conduct.[205]

Such misrepresentations also occur at the individual level. In one particularly colorful case, a corporate executive at Exxon Office Services used a yet-to-start new hire, named Halpern, to arrange a demonstration of a competitor's product.[206] Halpern contacted the competitor under the name of his soon to-be-ex employer and was able to get extensive information from the other company by posing as a potential customer.[207] 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.[208]

Despite the occasional lecture and sanction from the judiciary, corporate trickery surrounding negotiations persists. The Pennsylvania Superior Court, for example, granted 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.[209] Corporations also take advantage of existing relationships as a pre-text for acquiring confidential information. In *EchoMail, Inc., v. American Express Co.*, EchoMail alleged that its customer American Express conducted an "architecture review" of the product American Express used as a pretext for IBM, EchoMail's direct competitor, to obtain confidential and

---

[201] *Id.* at 348–49.
[202] *Id.* at 348.
[203] *Id.* at 355.
[204] *Id.* at 354.
[205] *Id.* at 354–55.
[206] Cont'l Data Sys., Inc. v. Exxon Corp., 638 F. Supp. 432, 435 (E.D. Pa. 1986)
[207] *Id.*
[208] Id. at 443.
[209] Den-Tal-Ez v. Seimans Capital Corp., 389 Pa. Super. 219, 566 .2d 1214 (Pa. Super. 1989).

proprietary technology.[210] Similarly, in the bankruptcy proceeding *In re InSITE Services Corp.*, InSITE alleged that one of its customers misappropriated trade secrets under the pretext of conducting an "audit" of InSITE's internal processes.[211] In other circumstances, employees may have conflicting loyalties or ulterior motives leading to the misappropriation for trade secrets.[212] For example, in *Advanced Fluid Systems, Inc. v. Huber,* 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 access and forward sensitive digital information on upcoming projects and commercial strategy.[213]

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.[214] 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 interviews."[215] Further, it adds, "depending on the jurisdiction, misrepresentation may be illegal."[216] Nevertheless, stories of such activities abound.[217]

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."

---

[210] 529 F. Supp. 2d 140, 145 (D. Mass. 2007).

[211] 287 B.R. 79, 89 (S.D.N.Y. 2002).

[212] *See* 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.

[213] 28 F. Supp. 3d 306, 313–15 (M.D. Pa. 2014).

[214] SCIP, *Code of Ethics, supra* note 119.

[215] *Id.*

[216] *Id.*

[217] *See also* 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).

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,[218] 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.[219] The Court held that the Fourth Amendment does not "protect[] a wrongdoer's misplaced belief that a person whom he voluntarily confides his wrongdoing will not reveal it."[220] The Supreme Court further elaborated this principle in *United States v. White*, stating "[O]ne 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."[221] 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.[222] The risk of revealing information to a party or committing incriminating acts in the presence of another who might reveal that information to the police or who might themselves be an undercover agent spans a wide range of scenarios, from disclosing incriminating information on internet chat rooms,[223] to serving alcohol to under-age undercover agents,[224] to selling obscene materials to an undercover officer,[225] and to revealing a marijuana grow operation to a customer-turned-police-

---

[218] *See, e.g.*, 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. INFO. TECH & PRIVACY L. 191, 198–203 (2015) (discussing the case-law establishing records collection and its application by the U.S. Government to electronic data).

[219] 87 S. Ct. 408, 412–13 (1966).

[220] *Id.* at 413.

[221] 91 S. Ct. 1122, 1126 (1971).

[222] 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).

[223] *See* U.S. 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).

[224] *See* Winkel v. Reserve Officer of City of Beloit, Kan., 773 F. Supp. 1487, 1489 (D. Kan. 1991).

[225] *See* Maryland v. Macon, 472 U.S. 462, 469–70 (1985).

informant.[226]

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 they 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, respondents found the use of both tactics to be more of a violation of a reasonable expectation of privacy in the context of trade secret. 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. This is consistent with earlier work by Slobogin and Schumacher.[227] Tracking disapproval by competitive intelligence scholarship and some courts, there is 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 are observable from a public place. For example, 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

---

[226] U.S. v. Ward, 703 F.2d 1058, 1059 (8th Cir. 1983).
[227] *See* note 125 and accompanying text.

"[v]isual surveillance from public places . . . or adjoining [the private property in question] would have sufficed to reveal all of these facts to the police."[228] 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."[229]

Yet, as we describe below, it is not clear that this is 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.[230]

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 ascertained or derived from publicly available information."[231] 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 when one has been surveilled. Though the techniques of law enforcement surveillance are generally revealed during later criminal proceedings, trade secret thieves have little incentive to disclose their successes to their victims. Therefore, we have little 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. Drone

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.[232] The Fifth Circuit held that a claim of trade secret misappropriation does not require a trespass or other illegal conduct, writing:

---

[228] 460 U.S. 276, 282 (1983).

[229] *Id.* The Supreme Court goes on to quote a *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. 274 U.S. 559 (1927).

[230] *See* Part III.C.2–3.

[231] Uniform Trade Secrets Act, § 1.4 (1).

[232] 431 F.2d 1012, 1013 (5th Cir. 1970).

> Our 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 espionage which could not have been reasonably anticipated or prevented.[233]

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" may have changed from the Fifth Circuit's analysis of more than four decades ago. Drone usage has filtered into many aspects of public life, from recreational uses to entrepreneurial activity.[234] 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.[235] This technology could also allow commercial competitors to photograph trade secrets of their rivals. While a case using drones as an improper means has not yet reached the courts, as the number of drones in private hands dramatically increases, the likelihood that one will be used to uncover a trade secret will likewise increase and then courts will 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 an understood fact of life, the Supreme Court was willing to hold in *California v. Ciraolo* that aerial observation does not present a

---

[233] *Id.* at 1016.

[234] *See, e.g.,* Carol Pogash, *Santa Delivered the Drone. But Not the Safety and Skill to Fly Them*. N.Y. TIMES. (Jan 8., 2017) (describing the challenges of drone ownership for everyday consumers) https://www.nytimes.com/2017/01/08/business/drone-safety-risk-popular.html?_r=0; Aili McConnon, *Drones Pique the Interest of Entrepreneurs*, N.Y. TIMES (May 25, 2016) (discussing the use of drones in agriculture, aerial photography, and construction) https://www.nytimes.com/2016/05/26/business/smallbusiness/drones-pique-the-interest-of-entrepreneurs.html. ; Timothy T. Takahashi, *Drones and Privacy,* 15 COLUM. SCI. & TECH. L. REV. 72, 81–91 (2012) (providing a detailed explanation of what a drone is and what it can do).

[235] *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 complaints by members of the public).

Fourth Amendment problem.[236] "Any member of the public flying in this airspace who glanced down could have seen everything that these officers observed. . . we 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."[237] 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.

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. 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.[238] 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. The Court also emphasized that "no intimate details connected with the use of the home or curtilage were observed, and there was no undue noise, and no wind, dust, or threat of injury."[239] Perhaps a drone could be distinguished from a plane or helicopter on these grounds were it flying very low, but that again does not seem a particularly promising avenue of attack; a drone fifty feet in the air is unlikely to cause much physical disruption to people below.

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.[240] A fixed-wing plane could not have legally flown at that altitude, but a helicopter could. A person in a state or locality that banned drone flight, or drone flight at a

---

[236] California v. Ciraolo, 476 U.S. 207, 213 (1986).

[237] *Id.* at 213–14.

[238] Florida v. Riley, 488 U.S. 445, 450–51 (1989)

[239] *Id.* at 452.

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

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%) v. 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 also suggests that it might be time to reconsider the Fourth Amendment case law on aerial surveillance.

2. Camera Across Street

Does the 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 the uses of 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."[241] 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 standards of the Strategic and Competitive Intelligence Professionals 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.[242]

---

[241] Paine, *supra* note 116, at 428.
[242] SCIP, *Code of Ethics, supra* note 119.

While state law may 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."[243] In *Ages Group, L.P. v. Raytheon Aircraft Co.*, a defendant corporation argued successfully that video surveillance from within an automobile of a commercial competitor conducted from a car did not constitute criminal surveillance under Alabama law because it was conducted from a public street.[244] Surveillance from a public place appears not to be per se illegal, and no case law provides guidance on what surveillance from a public place might constitute improper means. We can then tentatively conclude that videotaping of public places does not constitute improper means.

This presents a harder case under Fourth Amendment law, though the majority rule is clear. Most courts have held that such surveillance is not a search. In one typical case, ATF agents had placed a camera on a utility pole across from the defendant's property. As the Sixth Circuit observed, 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 Houston's farm in person, the fact that they instead used a camera to conduct the surveillance does not make the surveillance unconstitutional."[245] 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

---

[243] Code of Ala. § 13A-11-32 (2017). 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."

[244] 22 F. Supp. 2d. 1310, 1321 (M. D. Ala. 1998).

[245] United States v. Houston, 813 F.3d 282, 287–88 (6th Cir.), *cert. denied*, 137 S. Ct. 567, 196 L. Ed. 2d 448 (2016). *See also* United States v. Jackson, 213 F.3d 1269, 1281 (10th Cir.) (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. United States v. Cantu, No. 16-2191, 2017 WL 1244826, at *2 (10th Cir. Apr. 5, 2017 (same)). United States v. Brooks, 911 F. Supp. 2d 836, 839 (D. Ariz. 2012). *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).

Fourth Amendment regulation of long-term camera surveillance.[246] Courts are not universally unsympathetic to this intuition.[247] 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."[248] The South Dakota Supreme Court recently held that pole camera surveillance of a front yard for two months was a Fourth Amendment violation.[249] Nevertheless, the majority rule is that warrants are not required for these kinds of cameras.

This creates an interesting question from the standpoint 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 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.

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

---

[246] *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, 539 (2017). *See also* Jonathan Witmer-Rich, *Metaphysical Fourth Amendment Question: How Long Could a Tiny ATF Agent Sit Atop a Telephone Pole?*, PRAWFSBLOG (Feb. 8, 2016) http://prawfsblawg.blogs.com/prawfsblawg/2016/02/ten-week-camera-surveillance-and-reasonable-expectation-of-privacy.html

[247] *See, e.g.*, United States v. Cuevas-Sanchez, 821 F.2d 248, 251 (5th Cir. 1987) ("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, United States v. Vargas, No. CR-13-6025-EFS, at 20 (E.D. Wash. Dec. 15, 2014).

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

[249] State v. Jones, 2017 S.D. 59, ¶ 43 (Sept. 20, 2017).

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 revealing much more?

There are 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 relied upon in the previous hypothetical, *Ages Group*. 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.[250] However, that case does not discuss the use of a telephoto lens as an aggravating factor in determining whether visual surveillance was an improper means. A similar passing mention of vision-enhancing technology occurs 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.[251] However, the court in that case found that the information at issue was not a trade secret because it was readily ascertainable by other means 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.[252]

Courts sympathetic to the "corporate morality" justification exemplified by *E.I. DuPont deNemours v. Christopher* could find the use of high-powered lens to reveal the interior of offices or laboratories to be representative of "espionage which could not have been reasonably anticipated or prevented."[253] It could be argued that requiring any private business or information to be

[250] *Ages Group*, *supra* note 244 at 1316.
[251] 2011 Ohio App. LEXIS 5655, *6 (Ct. App. Ohio 2011).
[252] *Id.* at *13–14.
[253] 431 F.2d 1012, 1013 (5th Cir. 1970).

completely obscured from outside observation because of the possibility that text only readable from a few feet away by the naked eye could be obtained from thousands of feet away through sophisticated technology would "cost so much that the spirit of inventiveness is dampened."[254] 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. Taking the use of enhanced visual observation to its logical extreme, one could imagine using a high-powered lens[255] to capture video of a computer screen through the window of a skyscraper from several blocks away and employing optical character recognition technology[256] to generate a fairly accurate copy of any written material that appears. This level of intrusion 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 suspect's rights. A police officer strolling down the street is not required to avert their eyes from an unobstructed window; the police are generally free to observe whatever may be seen from a place where they are entitled to be.[257] 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."[258] But open curtains do not result in a total end to the Fourth Amendment analysis. In the apparently rare

---

[254] *Id*.

[255] *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 photography 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 eighty-three 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 .

[256] Optical character recognition (OCR) converts digital images into machine-readable text files. 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/ .

[257] Florida v. Riley, 488 U.S. 445, 449 (1989).

[258] 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).

case that this has been discussed, courts have sometimes found that use of a telescopic lens does implicate the Fourth Amendment.[259]

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. 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."[260] 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 observation. Similarly in *Florida v. Jardines*, the Court stated 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.[261]

This is again a case where the Fourth Amendment analogy is of great interest. Were one restricted to citing the trade secret case law, they would have a difficult time assessing whether technology-aided observation is an improper means. If one knows how they are permitted to analogize to the Fourth Amendment cases, the task is far easier. We believe that trade secret should permit fewer means of surveillance than does the Fourth Amendment, so we would view the discussed means of surveillance as improper under trade secret.

The vignette included in the survey specified only that a high-powered lens was used to take photographs through a window; we included no information about what information was captured.

---

[259] United States v. Smith, 978 F.2d 171, 180 (5th Cir. 1992); 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.").

[260] Kyllo v. United States, 533 U.S. 27, 34 (2001) (internal citation omitted).

[261] 133 S. Ct. 1409, 1414 (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").

Following the general trend, respondents reported on average that the lens through the window was more of a violation of privacy expectations in the trade secret context than the law enforcement context. Respondents found the lens through the window was more of a violation of privacy in both contexts than any of the other vignettes except wiretap and trespass to curtilage. However, 42.4% found the lens through the window should be permitted for law enforcement uses, while just 16.7% thought it should be permitted in the trade secret context. These results suggest that courts could match popular opinion by finding 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.

CONCLUSION

These results establish several important propositions for trade secret law. First, the hierarchy of searches in the trade secret context is very similar to the hierarchy of searches in the Fourth Amendment context. This is the sine qua non for allowing analogies between the two areas; that which is more a violation of privacy expectations in one context will also be more of a violation in the other.

Within the trade secret context, we find substantial support for the independent legal wrong approach to improper means. People most strongly condemned searches that violated other laws, such as trespass or wiretapping. Dumpster diving on both public and private land was also condemned, 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. Hedge funds now sometimes employ satellite imagery to track industrial trends,[262] and presumably use of them to uncover a trade secret would also face skepticism from the average jury member.

Public norms also support our proposition of a Fourth Amendment floor for trade secret. People drew an extremely

[262] Bradley Hope, *Investors Can Get an Eye in the Sky*, WALL ST. JOURNAL, C.1., Aug. 14, 2016 https://www.wsj.com/articles/satellites-hedge-funds-eye-in-the-sky-1471207062.

strong distinction in favor of allowing more law enforcement searches than commercial ones. 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 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've 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 those samples would change our key finding.

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 consistency we observe in the hierarchy of searches in our empirical data suggests that we are right to think there is at least something to this commonality in gravity of the intrusion point.

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. 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.

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.

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 the 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:

Government

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

Government

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)

Government

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 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 ABC Corp's private property, but outside the building.

4. False Friend

Government

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

Government
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

Government
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

Government
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

Government
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

Government
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

Government

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.