Hastings Law Journal

Volume 67 | Issue 1 Article 4

12-2015

Overcoming the Public-Private Divide in Privacy Analogies

Victoria Schwartz

Overcoming the Public-Private Divide in Privacy Analogies*

VICTORIA SCHWARTZ**

When a photographer takes unauthorized aerial photographs of a company's plant, the legal framework under which courts evaluate the case, as well as its likely outcome, depends on whether the photographer was hired by a private actor or the government. If a competitor hired the photographer, the aerial photography may constitute improper trade secret misappropriation. If, however, the government hired the photographer, the aerial photography would not violate the Fourth Amendment. This dichotomy illustrates a public-private divide in which privacy violations by the government are treated differently from privacy violations by the private sector. Despite this divide, some courts have analogized from the Fourth Amendment to the trade secret context, while the Supreme Court has rejected such an analogy in the opposite direction.

A similar but reverse phenomenon occurs in the workplace privacy context. Traditionally, whether an employee whose privacy has been invaded by an employer is likely to prevail in court depends in part on whether the employer is in the public or private sector. The longstanding wisdom is that public-sector employees receive stronger workplace privacy protections than similarly situated private-sector employees as a result of Fourth Amendment protections. Nonetheless, unlike the trade secret context, Supreme Court precedent suggests that private-sector analogies are appropriate in evaluating public workplace privacy cases.

---

* Title and Article in memory of Dan Markel who generously provided priceless written and verbal feedback including the suggestion for this title, and whose voice remains in my head whenever I am writing asking me, "Is this a Puzzle paper or a Problem paper?"

** Associate Professor of Law, Pepperdine University School of Law. J.D. 2007, Harvard Law School; B.S., B.A., 2004, Stanford University. Thank you to Gregory Boden and Zachary Price for excellent research assistance and to Caley Turner for invaluable editorial assistance. I am grateful to Paul Secunda, Lior Strahilevitz, and Adam Shinar for providing extensive feedback on earlier drafts. I would also like to thank Ryan Calo, Jack Chin, David Han, Michael Helfand, Orin Kerr, Jon Michaels, Paul Ohm, Elizabeth Pollman, Greg Reilly, and Sherod Thaxton for their thoughts and comments at various stages of the process. Many thanks also to the participants at the Ninth Annual Colloquium on Scholarship in Employment and Labor Law, 2014 Intellectual Property Scholars Conference, 2014 Works-in-Progress Intellectual Property, Prawfsfest XI, Pepperdine University School of Law Faculty Research Workshop, and Southern California Junior Law Faculty Workshop where I presented earlier versions of this Article.

Despite this apparent inconsistency, neither courts nor scholars have offered any systematic criteria for evaluating when privacy analogies across the public-private divide are appropriate. Rather, courts import or reject privacy analogies between the public and private sectors without any meaningful consideration of when such analogies make sense. This Article offers a coherent and consistent normative framework to analyze when privacy analogies are appropriate across the public-private divide. In deciding whether such privacy analogies make sense, courts ought to apply a multifactored test in which they consider the presence or absence of factors regarding the privacy-invading actor that could justify the traditional public-private distinction. These factors include power of coercion, ability to harm identity formulation or protection of democracy, access to superior technology, and presence of bureaucratic features.

Table of Contents

INTRODUCTION

An airplane flies over an industrial plant that has not yet been completed. No barriers prevent aerial viewing of the plant. Employees at the plant find the airplane suspicious and investigate. They discover that the airplane carried a photographer who had been hired to photograph the plant on behalf of an unidentified competitor. After the photographer refuses to reveal who hired him, the company sues the photographer.[1] Applying state trade secret law, a federal appellate court finds that the aerial photography could constitute improper means and allows the company to proceed with its lawsuit for misappropriation of a trade secret.[2] The court explains that although the company had taken no precautions to protect against aerial surveillance during construction of the plant, the law does not require taking "unreasonable precautions"[3] against actions "which could not have been reasonably anticipated or prevented."[4] Thus, in a sense, the court suggested that the company had a reasonable expectation of privacy from aerial photography of its plant.

Another airplane flies over a different industrial plant. Again no barriers prevent aerial viewing of the plant. Employees at the plant have been instructed to investigate any low-level flights over the plant. Upon further investigation, the employees discover that the airplane belongs to the Environmental Protection Agency ("EPA") which had requested and been refused permission to conduct a second on-site inspection of the plant at issue. Instead of obtaining an administrative search warrant, the EPA hired an aerial photographer to photograph the facility from above. The company sues the EPA.[5] Applying Fourth Amendment law and its "reasonable expectation of privacy" test,[6] the Supreme Court holds in favor of the EPA, concluding that "the taking of aerial photographs of an industrial plant complex from navigable airspace is not a search prohibited by the Fourth Amendment."[7] Notably, the Court finds the prior judicial determination that similar aerial photography by a competitor could be actionable under trade secret law to be "irrelevant"

---

1. E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1013 (5th Cir. 1970); *see infra* Part I.A.

2. *Christopher*, 431 F.2d at 1015.

3. *Id.* at 1017.

4. *Id.* at 1016.

5. Dow Chem. Co. v. United States, 476 U.S. 227, 229–30 (1986); *see infra* Part I.A.

6. Although the Court never quite explicitly says that the company does not have a reasonable expectation of privacy from aerial photography, this is apparent throughout the analysis and appears to be part of the basis for the Court's conclusion. *See Dow Chem. Co.*, 476 U.S. at 235 ("Dow further contends that any aerial photography of this 'industrial curtilage' intrudes upon its reasonable expectations of privacy. . . . [T]he Court has drawn a line as to what expectations are reasonable in the open areas beyond the curtilage of a dwelling . . . .").

7. *Id.* at 239.

to its consideration of whether the EPA's aerial photography violated the company's reasonable expectation of privacy.[8]

The aerial photography example illustrates the public-private divide in privacy law. Under the public-private divide, courts analyze privacy violations by the government under a Fourth Amendment analysis that typically includes a determination of whether the plaintiff has a reasonable expectation of privacy.[9] Courts have made abundantly clear, however, that the Fourth Amendment does not apply to the private sector.[10] Thus, depending on the particular facts of the case, courts analyze privacy violations by private actors under a variety of other possible legal frameworks including state constitutional privacy provisions,[11] federal statutes,[12] state statutes,[13] state privacy torts[14] and even state trade secret law.[15] Many of these legal frameworks contain doctrinal concepts analyzing the reasonableness of the plaintiff's expectations of privacy,[16] many of which can be similar to, but not always identical to the Fourth Amendment reasonable expectation of privacy analysis.[17]

This creates an analytical conundrum for courts. On the one hand, there exists an entrenched public-private divide in privacy law, in which the Court has repeatedly found that the Fourth Amendment does not

---

8. *Id.* at 232.

9. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

10. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 113 (1984); Chandler v. Miller, 520 U.S. 305, 323 (1997).

11. Unlike its federal counterpart, the California state constitution's privacy protections apply to the private sector. *See* Hill v. NCAA, 865 P.2d 633, 641 (Cal. 1994).

12. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681 (2013) (applying to private-sector recordkeeping); Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 (2013); *id.* § 201; *id.* § 2703 (applying to electronic submissions and known unofficially as the "Stored Communications Act"); Health Insurance Portability and Accountability Act of 1996, 29 U.S.C. § 1181 (2012) (applying to health information privacy).

13. *See, e.g.*, CAL. LAB. CODE § 435 (West 1998) (prohibiting employers from recording an employee in a restroom); CONN. GEN. STAT. § 42-471 (2009) (requiring businesses collecting social security numbers to create a privacy protection policy).

14. For a detailed overview of the privacy tort and its development, see DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 77–231 (3d ed. 2009).

15. *See, e.g.*, E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1015 (5th Cir. 1970).

16. *See, e.g.*, MASS. GEN. LAWS ch. 214, § 1B (1974) ("A person shall have a right against unreasonable . . . interference with his privacy."). *See* Gauthier v. Police Comm'r of Boston, 557 N.E.2d 1374, 1376 (Mass. 1990) (dismissing a section 1B tort claim because the plaintiff lacked a "reasonable expectation of privacy"); Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1073–74 (Cal. 2009) ("The right to privacy in the California Constitution set standards similar to the common law tort of intrusion. . . . [W]e consider (1) the nature of any intrusion upon *reasonable expectations of privacy*, and (2) the offensiveness or seriousness of the intrusion, including any justification and other relevant interests.") (emphasis added).

17. For example, although it is not formally an element of the claim, in order to succeed on an intrusion upon seclusion privacy tort, courts typically ask some variation on whether the plaintiff had a reasonable expectation of privacy. *See, e.g.*, Phillips v. Grendahl, 312 F.3d 357, 373 (8th Cir. 2002). Similarly, as explained in the aerial photography example, trade secret cases can involve a determination of whether the plaintiff used reasonable precautions in protecting the trade secret.

apply to the private sector.[18] On the other hand, the very fluid concept of a reasonable expectation of privacy is a heavily norm-driven inquiry requiring by its very nature an inquiry into the prevailing societal norms. Thus the question remains whether courts conducting a reasonable expectation of privacy analysis in a Fourth Amendment case can or should look to private-sector cases by analogy to help determine whether an expectation of privacy is reasonable. The aerial photography example suggests that the Court insists on maintaining the strict divide between the public and private sectors with regard to privacy law by rejecting analogies to private sector privacy law cases when analyzing the reasonable expectation of privacy in factually similar public sector cases.[19]

To complicate matters, in the workplace privacy context, the Court has taken a different approach to analogizing across the public-private divide in privacy law.[20] Suppose an employer wants to administer a drug test to an employee. Or, the employer wants to search the employee's desk, or place a tracking device on them, or place a video camera in the workplace. The way courts analyze these various workplace privacy invasions varies depending on whether the employer is in the private or public sector.[21] Under the traditional public-private divide, public-sector employees whose workplace privacy claims are evaluated under a Fourth Amendment framework receive stronger protection than their private-sector equivalents.[22] Unlike its staunch adherence to a strict public-private divide and refusal to analogize across that divide in the aerial photography trade secret example, the Supreme Court considers employee expectations of privacy in the private sector a relevant consideration in the Fourth Amendment analysis of public-sector workplace privacy cases.[23]

These diametrically different approaches by courts all the way up to the Supreme Court in terms of analogizing across the public-private divide result in a lack of clarity as to whether analogizing across the public-private divide is appropriate. Courts appear to freely analogize between the private sector privacy frameworks and the Fourth

---

18. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 113 (1984); Chandler v. Miller, 520 U.S. 305, 323 (1997).

19. *See infra* Part I.A. For a discussion of the public-private distinction more generally, see Erwin Chemerinsky, *Rethinking State Action*, 80 Nw. U. L. Rev. 503, 504 (1985).

20. *See infra* Part I.B. For a discussion of the public-private divide in the workplace context, see S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 Ga. L. Rev. 825, 828 (1998) ("Central to the understanding of privacy rights in the American workplace is the public/private distinction.").

21. *See* Paul M. Secunda, *Privatizing Workplace Privacy*, 88 Notre Dame L. Rev. 277, 283–302 (2012).

22. *See id.* at 278–79 (noting the conventional wisdom that public employees under the Fourth Amendment had greater expectations of privacy than their private-sector counterparts).

23. *See infra* Part I.B.

Amendment framework when it suits them and staunchly defend against such analogies when that is preferable. So can courts conducting a reasonable expectation of privacy analysis in a Fourth Amendment case look to private-sector cases by analogy to help determine whether an expectation of privacy is reasonable? Or conversely, in deciding whether a private-sector privacy violation would be "highly offensive to a reasonable person," as is required in a number of privacy torts, can or should courts look to factually similar Fourth Amendment cases by analogy for some perspective as to what is considered reasonable? Similarly, should courts look to Fourth Amendment discussions of reasonableness in order to help determine by analogy whether plaintiffs took reasonable precautions in the context of a trade secret case? Very little has been said by either courts or scholars on how to systematically decide when these types of analogies are appropriate.[24]

This Article seeks to fill that void by developing a coherent and consistent normative framework for considering when such privacy analogies are appropriate across the public-private divide. In order to do so, this Article examines the systematic structural features of government that may have traditionally necessitated a different degree of privacy protection from the government than from private citizens and companies. In doing so, it seeks to uncover the motivating principles behind the Fourth Amendment that justify treating a similar privacy-invading fact pattern differently because the government is the actor invading privacy. In other words, the Article seeks to explain the intuition that public-sector privacy invasions are more threatening, and thus more in need of protection than their private-sector counterparts.

The Article identifies four traditional features of government that could make invasions of privacy by the government more troubling than similar invasions of privacy by a private actor. First, the government has traditionally had more coercive power than the private sector.[25] Second, government invasions of privacy may harm the ability of individuals to form their own identity without interference or to act as the voice of democracy against government waste, abuse, and fraud.[26] Third, the government, at least historically, had access to privacy-invading technology that the private sector did not have.[27] Finally, the lack of accountability associated with bureaucratic features of government may cause supplementary reasons for concern.[28]

---

24. *See infra* Part I.C.
25. *See infra* Part II.A.1.
26. *See infra* Part II.A.2.
27. *See infra* Part II.A.3.
28. *See infra* Part II.A.4.

These customary differences, however, are beginning to break down in a modern world.[29] This begs the question: once Google has satellite technology, Amazon has drones, and numerous companies make use of big data, does the superior technology justification behind a strict public-private divide in privacy law still make sense? Or in the context of workplace privacy, do we consider the public-private divide differently if the private-sector employer is in the field of big data, such that it may have as much power and information over the employee as the government? Is it obvious that the harm behind the National Security Agency ("NSA") collecting large amounts of e-mail metadata is different in kind and scope to Google collecting the same data?[30] Of course all of these questions are made even more complicated by the fact that a good deal of information is shared between the private and public sectors.[31]

In light of these complications, this Article offers guidance to courts and scholars considering the use of a privacy analogy across the public-private divide. When deciding whether to analogize between the Fourth Amendment reasonable expectation of privacy analysis and its private-sector doctrinal counterparts, courts should evaluate the presence of the four identified features that traditionally made invasions of privacy by

---

29. *See infra* Part II.B.

30. The state action requirement of the federal Constitution does not in itself answer these questions. *See* U.S. CONST. amend. XIV, § 1. Of course it goes without saying that the Fourth Amendment only applies to government actors. That precedent is clearly settled and this Article does not try to change the substantive Fourth Amendment jurisprudence in any way. The established Fourth Amendment jurisprudence and the state action doctrine, however, only set the standard on the public-sector side of the comparison. The private-sector side of the comparison, currently covered by a hodgepodge of federal and state privacy and other related laws, remains open to change. For example, nothing prevents Congress from passing a law that states that private employees have the same degree of protection from workplace privacy invasions as would their public-sector counterparts. Similarly, nothing prevents a court from deciding that the appropriate standard for determining whether a company has a trade secret requires looking to whether that company would have a reasonable expectation of privacy in the Fourth Amendment context. That may or may not be a good idea, but it is open to discussion that goes beyond the claim that the Fourth Amendment does not apply to the private sector.

31. Many scholars have written on the extent to which the government and private sectors share information. *See, e.g.*, Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 7 (2008) ("[T]he line between public and private modes of surveillance and security has blurred if not vanished. Public and private enterprises are thoroughly intertwined."); Amitai Etzioni, *The Privacy Merchants: What Is to Be Done?*, 14 U. PA. J. CONST. L. 929, 951 (2012) ("[O]ne must assume that what is private is also public in two senses of these words: that one's privacy (including sensitive matters) is rapidly corroded by the private sector and that whatever it learns is also available to the government."); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1320–21 (2012) ("The FBI and other law enforcement agencies will shift from being active producers of surveillance to passive consumers, essentially outsourcing all of their surveillance activities to private third parties, ones who are not only ungoverned by the state action requirements of the Fourth Amendment, but also who have honed the ability to convince private citizens to agree to be watched."); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1095 (2002) ("[G]overnment is increasingly contracting with private-sector entities to acquire databases of personal information.").

the government more troubling than similar invasions of privacy by a private actor. The appropriateness of the analogy will require a multifactored analysis considering the extent to which the government and the private-sector actor in the relevant cases' fact patterns contain the four identified features.[32]

This Article proceeds in three parts. Part I identifies the haphazard way in which courts currently draw or refuse to draw analogies between trade secret and Fourth Amendment cases. It then engages in a similar analysis in the workplace privacy context. Part II explores the traditional differences between the public and private sectors that may justify a public-private divide in privacy law. This Part also identifies the ways in which these traditional justifications no longer make sense in the modern world. Part III uses the traditional differences identified in Part II as benchmarks in a multifactored test to be used as a coherent and consistent normative framework for courts and scholars considering use of a privacy analogy across the public-private divide. It then illustrates how that framework would work in various contexts.

I. The Traditional Public-Private Divide in Privacy Law

Traditionally, the American legal system has maintained a strict divide between the public and private sectors with regard to privacy law. A violation of privacy that occurs by a public-sector actor typically gets filtered though a Fourth Amendment analysis.[33] While the Fourth Amendment does not actually use the word "privacy,"[34] its prohibition against certain searches and seizures necessarily protects against many governmental invasions of privacy—traditionally those by the police.[35] Although scholars have contended that the Fourth Amendment should not be viewed primarily through a privacy paradigm,[36] there is little doubt

32. Admittedly, the factors identified in this Article are not novel concepts. Many of them already play a role in various aspects of judicial decisionmaking, or have been identified by scholars as important in other contexts. Furthermore, the factors likely only scratch the surface. The hope is that they will trigger a conversation that will lead to privacy analogizing by courts and scholars occurring in a coherent, rather than an ad hoc manner.

33. Public-sector privacy violations may also, depending on the specific facts, get analyzed under the First Amendment, Fourteenth Amendment, and arguably other constitutional provisions as well; however, the Fourth Amendment is the most likely basis for a claim.

34. The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

35. *See* Solove, *supra* note 31, at 1131.

36. *See, e.g.*, William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 Mich. L. Rev. 1016, 1060–77 (1995) (contending that the Fourth Amendment law's concern with privacy has led to abandoning a concern with coercion and violence); Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 Colum. L. Rev. 1751,

that privacy plays a pivotal role in the Fourth Amendment framework. This has been true at least since the Supreme Court's decision in *Katz v. United States* added the "reasonable expectation of privacy" to the Fourth Amendment analysis.[37]

The Fourth Amendment does not, however, apply to the private sector. Pursuant to the state action doctrine, the Supreme Court has "consistently construed" the Fourth Amendment "as proscribing only governmental action; it is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.'"[38] Therefore, unlike privacy violations in the public sector, privacy violations that occur in the private sector are not analyzed under a Fourth Amendment framework. Consequently, the Supreme Court has referred to the private sector as "a domain unguarded by Fourth Amendment constraints."[39] Instead, courts analyze private-sector privacy violations under a hodgepodge of other legal frameworks including state constitutional claims,[40] topic-specific federal statutes,[41] the FTC's privacy regulation,[42] state statutes,[43] state privacy torts[44] and other state common law claims such as trade secrets.[45]

1777 (1994) (defining the "constitutional value underlying the Fourth Amendment as that of 'trust' between the government and the citizenry").

37. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also* Solove, *supra* note 31, at 1118, 1121, 1128 (explaining that the Fourth Amendment's focus has been on protecting privacy against certain government actions, and that some notion of privacy has been the trigger for Fourth Amendment protection at least since the late nineteenth century).

38. United States v. Jacobsen, 466 U.S. 109, 113 (1984) (Blackmun, J., dissenting) (quoting Walter v. United States, 447 U.S. 649, 662 (1980)).

39. Chandler v. Miller, 520 U.S. 305, 323 (1997).

40. California's state constitution contains privacy protections that also apply to the private sector. *See* Hill v. NCAA, 865 P.2d 633, 641 (Cal. 1994).

41. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681 (2013) (applying to private-sector recordkeeping); Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 (2013); *id.* § 201; *id.* § 2703 (applying to electronic submissions and known unofficially as the "Stored Communications Act"); Health Insurance Portability and Accountability Act of 1996, 29 U.S.C. § 1181 (2012) (applying to health information privacy).

42. *See generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014) (describing the FTC's role in enforcing companies' privacy policies by using its unfair and deceptive trade practices authority as the functional equivalent of a body of common law); *see also* F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015) (upholding the FTC's power to regulate corporate cybersecurity failures that violate corporate privacy policies under its unfair and deceptive trade practices authority).

43. *See, e.g.*, CAL. LAB. CODE § 435 (West 1998) (prohibiting employers from recording an employee in a restroom); CONN. GEN. STAT. § 42-471 (2009) (requiring businesses collecting social security numbers to create a privacy protection policy).

44. *See* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1917 (2010) (noting that "nearly every state recognizes at least one form of the privacy torts").

45. *See infra* Part I.A.

A. Trade Secret Law and the Fourth Amendment

This traditional public-private divide in privacy law plays out in the context of certain trade secret law cases. Although trade secret doctrine involves numerous concepts that do not exist in the Fourth Amendment context, trade secret cases can involve violations of privacy in various factual scenarios. Indeed, the Supreme Court has recognized that trade secret law is necessary to protect "a most fundamental right, that of privacy."[46] Scholars have discussed the link between trade secret law and privacy,[47] and have described corporate privacy interests as part of the "fundamental nature of trade secret rights."[48] Even Justices Brandeis and Warren's seminal field-creating *Harvard Law Review* article, *The Right to Privacy,* argued that notions of privacy are embodied in trade secret law.[49]

At the doctrinal level, under the Uniform Trade Secrets Act ("UTSA"), which has been adopted by forty-seven states,[50] one of the ways in which trade secret misappropriation can occur is when someone acquires a trade secret by "improper means."[51] Although the definition of "improper means" does not explicitly list violations of privacy, some of the possibilities listed such as theft or espionage can involve privacy violations depending on the specific means by which the theft or espionage occurs.[52] Similarly, under the Restatement of Torts, a trade secret violation can occur when someone discloses or uses a trade secret that was discovered by improper means.[53] Under either standard, a trade secret plaintiff can prevail when a competitor or other individual invades the privacy of the company in the course of acquiring a trade secret by improper means.

---

46. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 487 (1974) ("A most fundamental human right, that of privacy, is threatened when industrial espionage is condoned or is made profitable; the state interest in denying profit to such illegal ventures is unchallengeable.").

47. *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.

48. Elizabeth A. Rowe, *Trade Secret Litigation and Free Speech*: *Is It Time to Restrain the Plaintiffs?*, 50 B.C. L. Rev. 1425, 1431, 1434–35 (2009).

49. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 212–13 (1890).

50. The UTSA has been adopted by every state except New York, North Carolina, and Massachusetts. Texas became the forty-seventh state to adopt the UTSA in May 2013. Massachusetts has introduced a bill to enact the UTSA, which remains pending as of this writing. *Legislative Fact Sheet – Trade Secrets Act*, Uniform L. Commission, http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade%20Secrets%20Act (last visited Dec. 18, 2015).

51. Unif. Trade Secrets Act § 1(1) (Unif. Law Comm'n 1985).

52. *Id.*

53. Restatement of Torts § 757 (Am. Law Inst. 1939). The Restatement holds a trade secret violation occurs when "[o]ne who discloses or uses another's trade secret, without a privilege to do so, is liable to the other if (a) he discovered the secret by improper means, or (b) his disclosure or use constitutes a breach of confidence reposed in him by the other in disclosing the secret to him." *Id.*

Furthermore, the trade secret and Fourth Amendment contexts can both involve extremely factually similar invasions of privacy from the perspective of the company whose privacy is being invaded.[54] Nonetheless, as the result of the traditional public-private divide in privacy law, a violation of privacy would be analyzed under entirely distinct frameworks depending on whether the privacy invasion occurred by the private sector, in which case a trade secret framework would apply, or by the government, in which case the Fourth Amendment framework would apply.

While it is abundantly clear that Fourth Amendment law does not apply to private-sector trade secret cases, there are a number of similarities between the two legal doctrines. For example, in the private-sector trade secret context, a claimed trade secret is not eligible for protection if the owner did not use reasonable efforts to ensure that the trade secret remained secret.[55] Similarly, under the "reasonable expectation of privacy test" in *Katz*, a Fourth Amendment claim only attaches if the plaintiff has a reasonable expectation of privacy over the claimed private domain. Thus, both doctrines involve consideration of the reasonableness of the asserted claim to privacy.

The traditional public-private divide serves to filter private-sector cases into a trade secret framework and public-sector cases into a Fourth Amendment framework. At the same time, in many circumstances the two types of cases may involve both similar fact patterns as well as some doctrinal similarities between the two distinct legal frameworks. As such, courts, advocates, and scholars might wonder whether it is appropriate to analogize across the public-private divide in such cases. Specifically, in deciding whether a trade secret plaintiff used reasonable efforts to ensure that a trade secret remained secret, can and should courts analogize to a factually similar case in the public Fourth Amendment context in which a court determined whether similar efforts were sufficient to create a reasonable expectation of privacy? The idea is not that Fourth Amendment precedent would be dispositive in trade secret

54. The Supreme Court has long recognized that the Fourth Amendment applies to the privacy interests of corporations. *See* Oliver v. United States, 466 U.S. 170, 178 n.8 (1984) (noting that the Fourth Amendment protection of privacy interests in business premises "is . . . based upon societal expectations that have deep roots in the history of the Amendment"); Marshall v. Barlow's, Inc., 436 U.S. 307, 312 (1978) (observing, in the OSHA administrative search context, that "it is untenable that the ban on warrantless searches was not intended to shield places of business as well as of residence"); *see also* Burwell v. Hobby Lobby Stores, Inc., No. 13-354, slip op. at 18 (U.S. June 30, 2014) (noting that "extending Fourth Amendment protection to corporations protects the privacy interests of employees and others associated with the company").

55. *See, e.g.*, Boeing Co. v. Sierracin Corp., 738 P.2d 665, 674 (Wash. 1987) ("[T]rade secrets law protects the author's very ideas if they possess some novelty and *are undisclosed or disclosed only on the basis of confidentiality.*") (emphasis added); Tennant Co. v. Advance Mach. Co., 355 N.W.2d 720, 725 (Minn. Ct. App. 1984) (noting that "the extent of measures taken to guard the secrecy of the information" is relevant to determining whether that information is a trade secret).

cases, but merely that it would help flesh out, by analogy, what sorts of efforts courts and society are prepared to recognize as reasonable.

Conversely, in deciding whether a plaintiff has a reasonable expectation of privacy in the Fourth Amendment context, can and should courts analogize to a factually similar case in the trade secret context in which a court determined that trade secret protective actions were sufficiently reasonable to satisfy that aspect of the trade secret analysis? Here again, the trade secret precedent would not be dispositive of the entire Fourth Amendment claim, but merely helpful to analyze what sorts of privacy claims courts and society are prepared to recognize as reasonable.

Currently, courts lack any clarity or guidance for when such analogizing is appropriate and have not developed a framework for evaluating when the analogy makes sense. The two factually similar cases involving aerial photography discussed briefly above and expounded upon below illustrate this problem.

In *E.I. duPont deNemours & Co. v. Christopher*, the Fifth Circuit analyzed a trade secret case involving aerial photography of an industrial plant owned by the plaintiff, DuPont.[56] The case arose out of Texas where an unknown third party, presumably one of DuPont's competitors, hired the Christophers to take aerial photographs of a DuPont plant that was still under construction.[57] DuPont had built the plant to facilitate the production of methanol by means of a "highly secret but unpatented process."[58] DuPont employees noticed the aircraft flying over the plant and launched an investigation by which they discovered that the Christophers had taken sixteen aerial photographs while circling the plant in their aircraft.[59]

DuPont filed suit alleging trade secret violation, and after the Christophers refused to disclose who had hired them during their depositions, the district court granted a motion to compel.[60] The Christophers sought an interlocutory appeal on whether DuPont had stated a claim.[61] The Christophers argued that they could not have misappropriated DuPont's claimed trade secret when they were "in public airspace, violated no government aviation standard, did not breach any confidential relation, and did not engage in any fraudulent or illegal conduct."[62] Applying the Restatement of Torts' definition of a trade secret,

56. E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1013 (5th Cir. 1970).
57. *Id.*
58. *Id.*
59. *Id.*
60. *Id.* at 1013–14.
61. *Id.* at 1014.
62. *Id.*

which the Texas Supreme Court had adopted at the time,[63] the Fifth Circuit found that illegal conduct was not necessary for misappropriation, and that the invasion of privacy that resulted from the aerial photography was sufficient.[64]

The Christophers argued that DuPont had not stated a proper claim for trade secret misappropriation because DuPont did not take reasonable precautions in its failure to cover the facility during construction and thus allowed the facility to be viewed from the air.[65] The court rejected that argument, however, holding that it would be unfair to permit espionage "when the protections required to prevent another's spying cost so much that the spirit of inventiveness is dampened."[66] The court refused to go so far as to prevent viewing of "open fields," but explained that a trade secret owner should not be forced to "guard against the unanticipated, the undetectable, or the unpreventable methods of espionage now available."[67] Because the finished plant would protect the process from view even from aerial espionage, requiring DuPont to construct a temporary barrier over the unfinished plant "would impose an enormous expense to prevent nothing more than a school boy's trick."[68] According to the court, requiring DuPont to create an "impenetrable fortress" would be an unreasonable requirement.[69] Having thus concluded that the aerial photography was improper, the court found that DuPont could sustain a cause of action for trade secret violation against the Christophers for their actions.[70]

Fourteen years later, the Supreme Court heard a case with somewhat similar facts, except that this time it was the government that violated a corporation's privacy by means of aerial photography.[71] Unlike in *Christopher*, however, where the Fifth Circuit held that aerial photographs taken of a plant could sustain a cause of action for a trade secret violation, the Court in *Dow Chem. Co. v. United States* rejected the argument that aerial photographs taken of a plant by the government

63. Texas has since adopted the UTSA. *See* 6 TEX. CIV. PRAC. & REM. § 134A.001 (2013).

64. *Christopher*, 431 F.2d at 1014. The Restatement holds a trade secret violation occurs when someone "discloses or uses another's trade secret, without a privilege to do so, is liable to the other if (a) he discovered the secret by improper means, or (b) his disclosure or use constitutes a breach of confidence reposed in him by the other in disclosing the secret to him." RESTATEMENT OF TORTS § 757 (AM. LAW INST. 1939).

65. *Christopher*, 431 F.2d at 1016.

66. *Id.*

67. *Id.*

68. *Id.*

69. *Id.* at 1017.

70. *Id.* Practically speaking, of course, this "victory" may not have accomplished very much. The Christophers were likely judgment proof, the aerial photographs had already been transferred to the unknown third party, and DuPont still did not know the identity of the third-party competitor who had hired the Christophers.

71. Dow Chem. Co. v. United States, 476 U.S. 227, 229 (1986).

violated the Fourth Amendment.[72] Dow operated a 2000-acre facility in Michigan that "consisted of numerous covered buildings with . . . equipment and piping conduits . . . exposed" between the buildings.[73] Dow had "elaborate security" around the complex that prevented public observation from the ground level.[74] Also, Dow instructed its employees to investigate any low-level flights over the facility.[75] Dow did not, however, construct any barriers to prevent aerial viewing.[76]

In 1978, the EPA conducted an on-site inspection of two power plants located on the premises with the consent of Dow.[77] The EPA requested a second inspection, which Dow rejected.[78] Rather than obtain an administrative search warrant, the EPA hired a commercial aerial photographer to take photographs of the facility with an aerial mapping camera.[79] Dow was not informed of the EPA's actions and upon learning of the aerial surveillance, filed for injunctive and declaratory relief alleging in part that the EPA violated the Fourth Amendment.[80]

The Supreme Court held that the plant was not analogous to the curtilage of a dwelling and the photographs were not a search prohibited by the Fourth Amendment.[81] Because Dow had "elaborately secured" its plant, the Court found that the space between the buildings fell somewhere between both doctrines.[82] The government has "'greater latitude to conduct warrantless inspections of commercial property'" because the reasonable expectation of privacy is significantly different than someone's home.[83] The difference here was that the aerial observation did not involve a "physical entry."[84] Because it was observable to the public, a government regulatory inspector should not need a warrant.[85]

The *Christopher* case had enough factual similarity that it might have been considered by the Court in *Dow Chemical Co.* as persuasive authority in considering the reasonable expectation of privacy aspect of the Fourth Amendment question. Both cases involved invasion of a company's privacy by means of aerial photography of a company facility. Both cases required the court to consider whether the industrial plant should be required to build a barrier preventing the facility from being

72. *Id.* at 239.
73. *Id.* at 229.
74. *Id.*
75. *Id.*
76. *Id.*
77. *Id.*
78. *Id.*
79. *Id.*
80. *Id.* at 230.
81. *Id.* at 239.
82. *Id.* at 236–37.
83. *Id.* at 237–38 (quoting Donovan v. Dewey, 452 U.S. 594, 598–99 (1981)).
84. *Id.* at 237.
85. *Id.* at 238 (citing Marshall v. Barlow's, Inc., 436 U.S. 307, 315 (1978)).

viewed from the air, and whether failure to do so meant that the company had not taken sufficient steps to protect its privacy. In *Dow Chemical Co.*, the Supreme Court apparently recognized these factual similarities between the case before them involving a Fourth Amendment claim for the EPA's aerial photography, and the Fifth Circuit precedent in *Christopher* holding that aerial photography of an industrial plant could constitute a misappropriation of a trade secret violation.

Instead of considering whether the *Christopher* case might at least be persuasive authority, however, the Court stated that the trade secret analogy was "irrelevant to the questions presented," not because the case was factually distinguishable, but rather because state tort law "does not define the limits of the Fourth Amendment."[86] In support of its claim that state tort law "does not define the limits of the Fourth Amendment," the Supreme Court cited *Oliver v. United States*[87] for the proposition that "trespass law does not necessarily define limits of [the] Fourth Amendment." The Court's shift from a position that state tort law does not have to define the limits of the Fourth Amendment to a position that state tort law is "irrelevant to the questions presented" is significant. The former formulation merely suggests that state tort law is not binding when it comes to Fourth Amendment limits, or in other words that there is a public-private divide in privacy law. The latter formulation, with its claim to irrelevance, rejects not only the binding effect of state tort law, but also any persuasive impact of state tort law or efforts to analogize across the public-private divide.[88] Viewing the public-private divide as absolute, the Court refused to answer whether the same tactics employed by a competitor would violate trade secret law.[89]

---

86. *Id.* at 232 (citing Oliver v. United States, 466 U.S. 170 (1984)). The Court used the following explanatory parenthetical in its citation of *Oliver*: "(trespass law does not necessarily define limits of Fourth Amendment)." *Id.* While the Court argues that state law has no bearing on Fourth Amendment jurisprudence, it simultaneously points out that it "does not necessarily define [the] limits," which implies that tort or property law may set a boundary on Fourth Amendment jurisprudence. *Id.*

87. 466 U.S. 170 (1984).

88. Sam Kamin describes *Dow Chemical Co.* as stating that "the fact that government conduct would have been tortious or criminal if done by a private actor is but one factor to be considered in determining whether that conduct violates a reasonable expectation of privacy." Sam Kamin, *The Private is Public: The Relevance of Private Actors in Defining the Fourth Amendment*, 46 B.C. L. REV. 83, 113–14 (2004). I disagree with that reading of the case. Nothing in *Dow Chemical Co.* suggests that the Court would be willing to consider the private-sector conduct as even "one factor to be considered." Instead, the Court's language consistently describes the private-sector precedent as "irrelevant." *Dow Chem. Co.*, 476 U.S. at 232; *see also* Florida v. Riley, 488 U.S. 445, 459 n.3 (1989) (Brennan, J., dissenting) (describing the decision in *Dow Chemical Co.* as the Court having "declined to consider trade-secret laws indicative of a reasonable expectation of privacy").

89. *Dow Chem. Co.*, 476 U.S. at 231.

The partial dissent in *Dow Chemical Co.* by Justices Powell, Brennan, Marshall, and Blackmun disagreed with the majority's dismissal of the relevance of the trade secret analogy.[90] The dissent noted that previous decisions held that a reasonable expectation of privacy exists in the Fourth Amendment context "if it is rooted in a 'source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.'"[91] Under their view, laws protecting trade secrets can be persuasive analogies to demonstrate society's beliefs regarding a reasonable expectation of privacy.

To be clear, there were a number of factual differences by which the Supreme Court decision in *Dow Chemical Co.* could have legitimately distinguished the *Christopher* precedent. The Court could have explained that the fact that DuPont was found to have taken reasonable precautions when it failed to cover its facility during the construction phase does not necessarily suggest that Dow had a reasonable expectation of privacy from aerial photography in its plant, which remained uncovered after the construction of the plant had been completed. Alternatively, the Court could have concluded that the fourteen-year gap between the two cases changed the plaintiff's reasonable expectation of privacy because aerial photography became increasingly common in the interim. Either of these approaches would have permitted the Court to consider the analogy to the trade secret case in order to determine its usefulness in evaluating the plaintiff's reasonable expectation of privacy from aerial photography. Ultimately, in doing so the Court could then have rejected the analogy as factually distinguishable. Instead, however, the Supreme Court confusingly rejected the trade secret precedent as irrelevant solely by virtue of its state tort law status, rather than because it was factually distinguishable.

Although the Supreme Court in *Dow Chemical Co.* found a factually similar trade secret case "irrelevant" to its Fourth Amendment analysis by virtue of its state tort law status, this did not put to rest the question of the appropriateness of analogies between Fourth Amendment and trade secret cases. Other courts analyzing trade secret cases have been willing to analogize in the opposite direction to relevant cases in the Fourth Amendment context. This only exacerbates the uncertainty regarding the correct treatment of privacy analogies across the private-public divide, and leaves open the question of whether it is possible that the analogies are acceptable when analogizing in one direction, but "irrelevant" when analogizing in the opposite direction.

---

90. *Id.* at 248 (Powell, J., concurring in part and dissenting in part).
91. *Id.*

For example, in *Tennant Co. v. Advance Machine Co.*, a Minnesota Court of Appeals found it appropriate to analogize to the Fourth Amendment context in deciding a trade secret case involving the privacy of trash.[92] *Tennant* involved business competitors, Tennant and Advance, who both manufactured and marketed floor cleaning equipment.[93] For two years, Advance employees went through Tennant's trash, which had been disposed of in sealed trash bags, and put in a covered dumpster behind Tennant's sales offices in California, which was only used by Tennant.[94] The dumpster diving scheme was conceived by an Advance sales representative, McIntosh.[95] He used the information he gained to send memos summarizing the content of the stolen documents to Advance's Vice President of Sales.[96]

The Minnesota Court of Appeals considered a misappropriation of trade secrets claim under the California Unfair Practices Act.[97] The court pointed out that among the relevant factors in determining whether information is a trade secret is "the extent of measures taken to guard the secrecy of the information."[98] The court explained that Tennant had "disposed of its waste in a manner that would assure secrecy except to someone particularly intent on finding out inside information" and concluded that "[t]he measures taken to guard the secrecy of the sales lists were adequate."[99]

In reaching that conclusion, the court appeared to be influenced by its earlier discussion of how the case would have been resolved under Fourth Amendment law.[100] The court noted that the law in California was settled that "an owner retains a reasonable expectation of privacy in the contents of a dumpster 'until the trash [has] lost its identity and meaning by becoming part of a large conglomeration of trash elsewhere.'"[101] The court found "no reason" to apply a different standard in a civil case because an owner "has the same expectation of privacy in property regardless of whether the invasion is carried out by a law officer or by a competitor."[102] Subsequent to the *Tennant* decision, the Supreme Court held that there is no reasonable expectation of privacy in trash put out for collection under Fourth Amendment law.[103] The key point raised by

92. *See, e.g.*, Tennant Co. v. Advance Mach. Co., 355 N.W.2d 720, 725 (Minn. Ct. App. 1984).
93. *Id.* at 722.
94. *Id.* at 722, 725.
95. *Id.* at 722.
96. *Id.*
97. *Id.* at 725.
98. *Id.*
99. *Id.*
100. *Id.*
101. *Id.* (quoting People v. Krivda, 486 P.2d 1262, 1268 (Cal. 1971)).
102. *Id.*
103. *See* California v. Greenwood, 486 U.S. 35, 40–41 (1988).

Tennant is not whether dumpster diving is acceptable, but rather whether in evaluating a dumpster-diving case in the trade secret context courts should be analogizing to discussions of the reasonable expectation of privacy in a dumpster in the applicable Fourth Amendment cases. The *Tennant* court strongly suggested that such analogizing was appropriate.

A second court reviewing a dumpster-diving trade secret case agreed that Fourth Amendment analogies are appropriate, but the actual impact of the analogy changed in light of evolving Fourth Amendment law regarding dumpster diving. In *Frank W. Winne & Son, Inc. v. Palmer*,[104] Palmer, the president of Twi-Ro-Pa,[105] instructed an employee to collect Winne's trash and to forward any office documents found therein to him.[106] The documents forwarded included invoices, customer lists, documents containing the names of factories the plaintiff used, and purchase orders that reflected the cost and pricing of Winne's orders.[107] Upon learning of the theft, Winne filed suit alleging trade secret violations and tortious interference with contractual relationships with customers.[108] After an "improper means" analysis, the court considered whether Winne had taken adequate protections to protect the trade secret because failure to do so would preclude recovery.[109]

In undertaking its analysis, the Pennsylvania court turned to Fourth Amendment cases for persuasive authority to determine if there was a reasonable expectation of privacy sufficient to protect the trade secret documents left in the trash.[110] Among others, the court discussed the Supreme Court's decision in *Greenwood* holding that there is no reasonable expectation of privacy in trash that has been placed for collection.[111] The *Palmer* court explained that it found the reasoning in those Fourth Amendment cases to be "persuasive."[112] Thus, the court demonstrated its belief that the analysis of the reasonable expectation of privacy in Fourth Amendment cases can be used as an analogy to determine similar questions in the trade secret private-sector context. Although the *Palmer* court recognized that the Fourth Amendment cases were "not commercial trade secret cases," it nonetheless found that "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

104. No. 91-2239, 1991 WL 155819 (E.D. Pa. Aug. 7, 1991).

105. Both Winne and Twi-Ro-Pa were competitors in the business of manufacturing and selling rope. *Id.* at *1.

106. *Id.*

107. *Id.*

108. *Id.*

109. *Id.* at *3.

110. *Id.* at *4.

111. *Id.* at *4 (citing California v. Greenwood, 486 U.S. 35, 40–41 (1988)).

112. *Id.*

of law, he has no reasonable expectation of privacy from prying eyes."[113] This language suggests that the court felt that Fourth Amendment law could set the floor for whether there were adequate precautions taken.

Other courts, however, have not approved of analogizing to Fourth Amendment cases in analyzing trade secret cases. Unlike the Pennsylvania court in *Palmer,* which approved of and used Fourth Amendment analogies, a California Court of Appeal criticized the use of such analogies in *Tennant*. The California appellate court explained that "Fourth Amendment principles which may be useful in resolving a criminal search and seizure dispute are of little relevance to a civil claim."[114] The court expanded that: "The question whether the state's agents violate a person's reasonable expectation of privacy by seizing items placed in the trash for purposes of the constitutional prohibition on unreasonable searches raises materially different issues" than similar actions taking place in the private sphere.[115]

To summarize, certain courts have found it permissible for trade secret cases to analogize to the Fourth Amendment reasonable expectation of privacy jurisprudence for assistance in determining whether the plaintiff used reasonable precautions to protect a trade secret. Other courts, however, have rejected precisely the same sort of analogy. Additionally, in the reverse context, the Supreme Court found a factually similar trade secret case to be "irrelevant" in determining whether a plaintiff had a reasonable expectation of privacy for purposes of conducting its Fourth Amendment analysis.[116] These inconsistent treatments of analogies across the public-private divide grow even more incoherent when the scope of the analysis shifts from the trade secret context to other areas of privacy law.

B. Workplace Privacy and the Fourth Amendment

The traditional public-private divide in privacy law also plays a role in the context of workplace privacy. Employers can and do invade the privacy of their employees in various ways including, but not limited to, drug testing, medical testing, psychological and personality testing, polygraph testing, workplace surveillance, monitoring e-mail, and GPS tracking. If the employee works for a governmental employer then courts may analyze the privacy invasion under a Fourth Amendment

113. *Id.*

114. Ananda Church of Self-Realization v. Massachusetts Bay Ins. Co., 116 Cal. Rptr. 2d 370, 377 n.3 (2002). Although the civil claim being analyzed in the case was for conversion of personal property, there is no reason to believe that the court's critique or analysis would be any different for a civil claim under trade secret law as the same logic applies.

115. *Id.* (discussing reasonable expectations of privacy in the context of a civil conversion claim).

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

framework.[117] If, however, the employee works in the private sector, a Fourth Amendment claim is not available.[118] This difference occurs because under the state action doctrine, only public-sector employees can bring constitutional claims.[119] As a result, the "[c]onventional wisdom has long held that public employees with federal constitutional protections have stronger workplace rights than their private-sector counterparts."[120] As explained below, the conventional wisdom may no longer hold true.

Without the ability to pursue Fourth Amendment claims, private-sector employees are limited to pursuing claims under either state common law privacy torts, or various scattered federal and state statutes.[121] Of the four privacy torts captured in the Restatement (Second) of Torts, the intrusion upon seclusion tort is the most applicable in private-sector workplace privacy cases.[122] Under the Restatement's formulation, the intrusion upon seclusion tort involves "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[123] Although the Restatement language does not expressly include "reasonable expectation of privacy" language, in applying this tort, courts often consider whether the employee had a "reasonable expectation of

---

117. *See* Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 665 (1989).

118. Willner v. Thornburgh, 928 F.2d 1185, 1192 (D.C. Cir. 1991) ("It is also true that private employers, unconstrained by the Fourth Amendment, may engage in practices the government as employer cannot."); Am. Fed'n of Teachers v. Kanawha Cty. Bd. of Educ., 592 F. Supp. 2d 883, 892 (S.D.W.Va. 2009) ("Private employers are free to search their employees because the Fourth Amendment 'does not apply to searches by private parties, absent governmental involvement.'") (quoting United States v. Humphrey, 208 F.3d 1190, 1203 (10th Cir. 2000)).

119. *See Am. Fed'n of Teachers*, 592 F. Supp. at 892.

120. Secunda, *supra* note 21, at 278.

121. *Id.* at 279.

122. Factual patterns that would trigger the other privacy torts—false light, public disclosure of private facts, and misappropriation of name or likeness—occur less frequently in the workplace privacy context than do facts involving employer intrusion upon seclusion. *See* Wilborn, *supra* note 20, at 842 n.66, 844 (noting that the "tort that most plaintiffs use to challenge employer monitoring and surveillance is the intrusion on seclusion tort").

123. RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977). For purposes of this discussion, this Article expressly discusses the Restatement (Second) of Torts rather than the Restatement (Third) of Employment Law. This is because whereas, forty-one states and the District of Columbia have applied some version of the intrusion upon seclusion tort, with many expressly adopting the Restatement (Second) of Torts formulation, to date no court has expressly applied the similar tort from the Restatement (Third) of Employment Law. The Restatement of Employment Law creates a "new" tort by applying the existing intrusion upon seclusion tort into the employment context to create the tort of "wrongful employer intrusion upon a protected employee privacy interest." The "new" tort consists of an application of the traditional intrusion upon seclusion tort in the employment context and does not substantively change the doctrinal analysis of the traditional tort. Therefore, the discussion here ought to apply equally to the new context once courts begin to adopt the new tort. For an extremely useful analysis of the wrongful employer intrusion tort, see Secunda, *supra* note 21, at 294–301.

privacy" in order to determine whether the employee had a privacy interest that could be intruded upon.[124]

In the public-sector employment context, the Supreme Court has clearly established that the "Fourth Amendment applies as well when the Government acts in its capacity as an employer."[125] The precise test for Fourth Amendment claims against government employers, however, remains somewhat unclear as a result of various Supreme Court cases evoking multiple possible tests.

The Court first considered employee rights to privacy in the public workplace in *O'Connor v. Ortega*[126] in 1987. The case involved the workplace privacy rights of physician and psychiatrist Dr. Magno Ortega.[127] Dr. Ortega worked as the Chief of Professional Education, training the young physicians in the psychiatric residency programs at Napa State Hospital, a government-run facility.[128] In 1981, hospital officials grew concerned regarding possible improprieties in Dr. Ortega's management of the residency program, including two charges of sexual harassment of female hospital employees, discrepancies regarding Dr. Ortega's acquisition of a computer for the program, and allegations that he had taken inappropriate disciplinary action against a resident.[129] During an investigation of these charges, hospital personnel searched Dr. Ortega's office, and seized several personal items including a Valentine's Day card, a photograph, and a book of poetry, as well as billing documentation of one of Dr. Ortega's private patients.[130] Dr. Ortega sued under 42 U.S.C. § 1983 on the grounds that the search of his office violated the Fourth Amendment.[131]

When the case reached the Supreme Court, a four-Justice plurality authored by Justice O'Connor applied a two-step analysis for public-sector workplace privacy Fourth Amendment claims.[132] First, a court must evaluate "[t]he operational realities of the workplace" in order to determine whether an employee's Fourth Amendment rights are

124. *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97, 100–01 (E.D. Pa. 1996) (applying the Restatement definition of intrusion upon seclusion and concluding that there was no "reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor" and thus "any reasonable expectation of privacy was lost"); *see also* RESTATEMENT (THIRD) OF EMP'T LAW § 7.01 cmt. g (AM. LAW INST. 2014) (observing that the concept of a 'reasonable expectation of privacy' is common to workplace privacy analyses in both the public and private sectors).

125. City of Ontario v. Quon, 560 U.S. 746, 756 (2010) (citing Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 665 (1989)).

126. 480 U.S. 709 (1987).

127. *Id.* at 712–14.

128. *Id.* at 712.

129. *Id.*

130. *Id.* at 713.

131. *Id.* at 714.

132. *Id.* at 717, 725–26.

implicated.[133] The plurality explained that at the first step, "the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis."[134] Second, where the employee has a reasonable expectation of privacy, an employer's intrusion on that expectation "should be judged by the standard of reasonableness under all the circumstances."[135] This standard involves balancing "the invasion of the employees' legitimate expectations of privacy against the government's need for supervision, control, and the efficient operation of the workplace."[136] The plurality decision evaluated the reasonableness of the employer's search by considering both whether the search was reasonable in its inception, as well as whether it was reasonable in its scope.[137]

Providing the fifth necessary vote, Justice Scalia would have skipped the plurality's first-step inquiry into "operational realities" and instead would assume that searches of the offices of government employees as well as the personal items in that office always receive a Fourth Amendment inquiry.[138] Having determined that Fourth Amendment protections are triggered, Justice Scalia would have nonetheless held "that government searches to retrieve work-related materials or to investigate violations of workplace rules" do not violate the Fourth Amendment.[139]

Although the Court failed to reach a consensus regarding what test governs the scope of a public employee's Fourth Amendment workplace privacy claims, in each of their opinions the various Justices did appear to agree that analogies to the private sector are appropriate in adjudicating these claims. In contrast to the Supreme Court's apparent rejection of analogies across the public-private divide in the trade secret context, in the workplace privacy context each of the key Court opinions in *O'Connor* suggested that such analogies to the private sector are useful and appropriate. On this point at least the Court appears united.

First, the Justice O'Connor plurality opinion in *O'Connor* suggested that it is appropriate for courts to analogize to the private sector in deciding whether a public-sector employee has a reasonable expectation of privacy in a particular case. In applying the "operational realities" test, the plurality decision explained that "[p]ublic employees' expectations of privacy in their offices, desks, and file cabinets, *like similar expectations*

133. *Id.* at 717.
134. *Id.* at 718.
135. *Id.* at 725–26.
136. *Id.* at 719–20.
137. *Id.* at 726.
138. *Id.* at 730–31 (Scalia, J., concurring).
139. *Id.* at 732.

of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation."[140]

Second, Justice Scalia's concurrence in *O'Connor* also suggests that analogies to the private sector are appropriate in deciding whether a public-sector employee has a reasonable expectation of privacy, except Scalia conducts the analysis on a sweeping basis, rather than the case-by-case approach used by the plurality. Justice Scalia "would hold that government searches to retrieve work-related materials or to investigate violations of workplace rules—*searches of the sort that are regarded as reasonable and normal in the private-employer context*—do not violate the Fourth Amendment."[141] Thus Scalia's test would require a court to decide whether a particular government search is a search of the sort that is regarded as reasonable and normal in the private-employer context. One way for a court to figure out if a search is considered reasonable and normal in the private-employer context is to analogize to the reasoning of private-sector privacy cases considering a similar type of employer search. Thus both the plurality and concurring opinions in *O'Connor* suggest that analogies to private-sector cases are appropriate.[142]

For over two decades after *O'Connor*, the Supreme Court did not clarify which of the two analyses—the Justice O'Connor plurality formulation, or Justice Scalia's concurring formulation—governed the scope of a public employee's Fourth Amendment rights. During that time, most judicial decisions and litigants assumed that the plurality decision governed, and most did not address Scalia's concurring test.[143]

In 2010, in *City of Ontario v. Quon*,[144] the Supreme Court had the opportunity to elucidate the governing test for public-sector workplace privacy claims. Instead, the Supreme Court's decision added further uncertainty to the scope of a public employee's Fourth Amendment rights in the workplace. The case involved the privacy rights of Jeff Quon, a police sergeant and Special Weapons and Tactics ("SWAT") Team member with the Ontario Police Department.[145] The City of Ontario issued pagers to Quon and his colleagues to help them respond to emergency situations.[146] A written "Computer Usage, Internet and E-

140. *Id.* at 717 (plurality opinion) (emphasis added).

141. *Id.* at 732 (Scalia, J., concurring) (emphasis added).

142. In fact, even the dissent in *O'Connor* suggested a link between the public and private sectors. *Id.* at 739 (Blackmun, J., dissenting) (contending that "the reality of work in modern time, *whether done by public or private employees*, reveals why a public employee's expectation of privacy in the workplace should be carefully safeguarded and not lightly set aside") (emphasis added).

143. *See* Pauline T. Kim, *Market Norms and Constitutional Values in the Government Workplace*, N.C. L. REV. (forthcoming) (manuscript at 23 n.115) (on file with author) (listing cases ignoring Justice Scalia, as well as those considering his opinion, but determining that the plurality controlled).

144. 560 U.S. 746 (2010).

145. *Id.* at 750.

146. *Id.* at 751.

mail Policy" ("Policy") gave the city "the right to monitor and log all network activity including e-mail and Internet use, with or without notice," and explained that "[u]sers should have no expectation of privacy or confidentiality when using these resources."[147] The Policy did not explicitly apply to text messaging, but the City explained that it would treat text messages the same as e-mails.[148]

After Quon exceeded his monthly text message character allotment, he was warned that the pagers "could be audited," but was told that there was no "intent to audit [an] employee's text messages to see if the overage [was] due to work related transmissions."[149] Instead, Quon took advantage of an available opportunity to reimburse the city for the overage fee in lieu of an audit of his messages.[150] Frustrated with this arrangement, the City decided to determine whether the existing character limit was too low, or whether the overages were for personal messages.[151] The City requested, received, and reviewed transcripts of text messages sent by Quon, "and discovered that many of the messages . . . on Quon's pager were not work related, and [that] some were sexually explicit."[152] Quon was disciplined and he filed suit against the City for various claims, including a violation of his Fourth Amendment right to privacy.[153]

In *Quon*, the Supreme Court's majority opinion reviewed the lingering *O'Connor* ambiguity on the proper analytical framework for Fourth Amendment claims against government employers.[154] Unhelpfully, however, the Court concluded it was "not necessary to resolve" which of the two approaches was correct[155] because both approaches "lead to the same result here."[156] The Court also declined to resolve whether Quon had a reasonable expectation of privacy in the text messages sent on the pager.[157] Instead, the Court assumed *arguendo* that Quon did have a reasonable expectation of privacy, and proceeded to the second step of the analysis.[158] For the second step, the Court held that the City's review of the transcripts of Quon's text messages was reasonable

147. *Id.*
148. *Id.*
149. *Id.* at 752.
150. *Id.*
151. *Id.*
152. *Id.* at 752–53.
153. *Id.* at 753–54.
154. *Id.* at 756.
155. *Id.* at 757.
156. *Id.*
157. *Id.* at 760.
158. *Id.*

under either the Justice O'Connor[159] or the Justice Scalia approach,[160] and therefore the City "did not violate Quon's Fourth Amendment rights" under either test.[161]

Although the *Quon* decision left much to be desired, the Court once again suggested that analogizing to the private sector is appropriate in analyzing the reasonable expectation of privacy portion of a public-sector Fourth Amendment workplace privacy case. Because the Court chose to assume without deciding that Quon had a reasonable expectation of privacy, it did not have to actually engage in any private-sector analogies to help determine whether Quon in fact had a reasonable expectation of privacy in his workplace pager. Nonetheless, language in the decision suggests that the Court would find such analogies useful and appropriate.

For example, in its dicta the Court noted that at least one amicus pointed out that some states have recently passed statutes requiring employers to notify employees when monitoring their electronic communications.[162] Unlike in the trade secret context, the Court did not reject this sort of reasoning as categorically irrelevant. Instead, the Court explained that "[a]t present, it is uncertain how workplace norms, and the law's treatment of them, will evolve."[163] This language suggests that the law's treatment of private-sector workplace norms remains unclear, but should those norms solidify, then the private-sector cases would be appropriate for analogy. Furthermore, the Court's phrasing that it is hard to predict the "degree to which society will be prepared to recognize those expectations as reasonable"[164] also suggests that those analogies can be appropriate because private-sector cases are one way to gauge whether society is recognizing certain expectations as reasonable.

Additionally, in the portion of the decision applying the alternative Scalia test, the Court clarified that the search of the pager transcripts "would be regarded as reasonable and normal in the private-employer context" and thus would satisfy the Scalia approach.[165] This supports a reading of the *O'Connor* case whereby under the Scalia test courts could appropriately analogize to private-sector cases in order to either support

159. *Id.* at 764 ("Because the search was motivated by a legitimate work-related purpose, and because it was not excessive in scope, the search was reasonable under the approach of the *O'Connor* plurality.").

160. *Id.* at 764–65 ("For these same reasons—that the employer had a legitimate reason for the search, and that the search was not excessively intrusive in light of that justification—the Court also concludes that the search would be 'regarded as reasonable and normal in the private-employer context' and would satisfy the approach of Justice Scalia's concurrence.").

161. *Id.* at 765.

162. *Id.* at 759.

163. *Id.* at 759–60.

164. *Id.*

165. *Id.* at 764–65.

a conclusion that a particular action is not considered reasonable and normal, or alternatively that society is prepared to recognize certain expectations as reasonable.

Despite the apparent consensus within the Supreme Court that analogies to private-sector expectations of privacy are appropriate to determine reasonable expectations of privacy in the public workplace privacy context, the Court never expressly explains why such analogies make sense in this context,[166] whereas similar analogies in the trade secret context were rejected as irrelevant.

C. Lacking a Common Normative Framework for Privacy Analogies

Just as courts have failed to offer a consistent and coherent normative framework for using privacy analogies across the public-private divide in various contexts, the scholarly literature has not yet filled the gap. Although scholars and commentators have discussed the public-private divide in privacy law in various contexts, no one has yet offered a coherent normative framework for how to determine when such privacy analogies are appropriate across various substantive areas.

Sam Kamin has written persuasively about the dangers of ignoring privacy violations by the private sector in favor of a myopic focus on state actors.[167] He offers a descriptive claim that private-sector privacy invasions are crucial because courts will examine that conduct to determine whether an individual has a reasonable expectation of privacy in the Fourth Amendment context.[168] As a consequence, "the only way for individuals to gain protection against governmental intrusions into their privacy is to actively seek to protect their private information from all prying eyes, public and private."[169] Kamin claims that courts have wrongly focused on the actual conduct of the private sector rather than the legality of that conduct.[170] As he explains, "the Court's focus is generally on what members of the public could do as a practical matter, not what they are permitted to do as a legal matter."[171] As a result of this observation he contends that "laws designed to protect individual privacy from private actors are unlikely to increase the scope of privacy from the government."[172] Kamin's contribution focuses on private-sector conduct rather than the circumstances in which courts should analogize to cases involving private-sector conduct.

---

166. *See* Kim, *supra* note 143, at 25 ("[T]he Court has not clearly spelled out why the analogy is relevant.").

167. Kamin, *supra* note 88, at 84.

168. *Id.* at 85.

169. *Id.* at 87.

170. *Id.* at 86.

171. *Id.* at 112.

172. *Id.* at 107.

Kamin does suggest, however, that the Court's use of privacy analogies to the private sector should be considered appropriate in determining the reasonable expectation of privacy analysis in public-sector cases.[173] For example, he notes that state government assertions of the privacy expectations of their citizens "ought to be relevant to a federal court's determination of whether a particular individual enjoyed a reasonable expectation of privacy."[174] Similarly, he contends that "nothing would prohibit a federal court from considering the fact that a state has protected the defendant against exactly the sort of privacy invasion engaged in by government agents in a given case."[175] Because these claims are not the main focus of his contribution, however, Kamin does not explain whether such analogies would be appropriate in every case, nor offer any framework for determining when such analogies should be used.

Margot Kaminski and Kevin Bankston advocate analogizing to the Fourth Amendment reasonable expectation of privacy standard in the subset of private-sector cases that involve statutory references to a reasonable expectation of privacy.[176] They argue that where a state statute expressly uses the exact phrase "reasonable expectation of privacy" courts should strongly presume that the legislature meant to incorporate the Fourth Amendment jurisprudence regarding that term unless there is clear evidence otherwise.[177] Where, however, the statute more obliquely references the reasonable expectation of privacy standard, they contend only that courts "may" reference the Fourth Amendment jurisprudence by analogy.[178] In that second statutory category, the framework provided by this Article could provide guidance to the Court in deciding whether to use the Fourth Amendment analogy or not.

Other scholars have written about analogizing across the public-private divide in the specific context of workplace privacy. In her earlier work, Pauline T. Kim has argued that "constitutional cases can and should provide experience in identifying those matters socially recognized to be private when determining the legitimacy of employee claims to privacy under the common law."[179] Kim explains that the constitutional cases can "provide further evidence of established privacy norms by identifying the core areas in which individual expectations of

---

173. *See id.* at 142–43.

174. *Id.*

175. *Id.* at 143.

176. Margot Kaminski & Kevin Bankston, A Unified Reasonable Expectation of Privacy? What *United States v. Jones* Means for Privacy Law Beyond the Fourth Amendment (unpublished manuscript) (on file with author).

177. *Id.* (manuscript at 14–17).

178. *Id.* (manuscript at 17–18).

179. Pauline T. Kim, *Privacy Rights, Public Policy, and the Employment Relationship*, 57 OHIO ST. L.J. 671, 706 (1996).

privacy are recognized as reasonable."[180] More recently, however, Kim's work rejects analogies in the opposite direction, arguing that "[r]elying on an analogy to private employment to interpret public employees' constitutional rights is a mistake."[181] According to Kim, the analogy is inapt "[b]ecause the government employer stands in a different relationship to the public and to the market."[182]

Similarly, Paul Secunda bemoans what he sees as "the equalization of privacy rights in the public and private sector" that has resulted from the Court's willingness to look to the private sector in determining public-sector workplace privacy cases.[183] Secunda contends that "[n]ormatively, public employees should [receive] stronger workplace privacy [protection] than their private-sector equivalents."[184] Consequently, Secunda advocates a new two-step approach for workplace searches in the public sector.[185] Because his analysis focused solely on workplace privacy issues, however, Secunda's arguments do not offer any guidance for analogizing beyond the workplace privacy context.

Other scholars have criticized the public-private distinction in the workplace privacy context, and have gone so far as to advocate eliminating the distinction altogether because it "simply does not make sense."[186] For example, Professor Betsy Malloy contends that given an aggregation of wealth and power, private employer invasions of privacy can be just as invasive and harmful as government invasions of privacy.[187] As a result, she "advocates the elimination of what has become an anachronistic inequality in the treatment of workplace privacy."[188] Wilborn would achieve that result by the enactment of a comprehensive federal statute protecting the right to privacy of all employees.[189] Other scholars have advocated abandoning the public versus private dichotomy completely by means of a new test that would find the majority of private employment behavior would constitute state action.[190] Such solutions are

180. *Id.* at 705–06.

181. Kim, *supra* note 143 at 6 (writing about both privacy and First Amendment rights).

182. *Id.* at 27.

183. Secunda, *supra* note 21, at 281.

184. *Id.* Many of his arguments in favor of this normative position that public employees should have stronger workplace privacy rights than private-sector employees are extremely persuasive. In fact, some of them get incorporated into the normative framework for when privacy analogies are appropriate. *See infra* notes 216, 238.

185. Secunda, *supra* note 21, at 282.

186. *See* Wilborn, *supra* note 20, at 831.

187. *Id.* at 830.

188. *Id.*

189. *Id.* at 832.

190. *See, e.g.*, Ronald P. Angerer II, *Moving Beyond a Brick and Mortar Understanding of State Action: The Case for a More Majestic State Action Doctrine to Protect Employee Privacy in the Workplace*, 4 CHARLOTTE L. REV. 1, 13–42 (2013) (advocating revisiting various aspects of the state action doctrine in order to limit the ability of the employer to invade employee privacy); David H.J.

unlikely to succeed as no such comprehensive federal statute has found its way through Congress, and there appears no realistic elimination of the state action doctrine on the horizon. Furthermore, such solutions would not help to answer the question of whether courts in other privacy contexts should analogize across the public-private divide.

Others have addressed the topic of analogizing across the public-private divide in the context of the Fourth Amendment and trade secrets.[191] For example, one commentator, recognizing that some courts have used a Fourth Amendment analogy in trade secret cases, points out that "the analogy is appealing in some respects."[192] In other ways, however, he finds the analogy unattractive "particularly in light of the trade secret treatment of accidental disclosure, disclosure to third parties, misrepresentation of identity, and the relevance of the costs of privacy."[193] Although this critique uses the language of "analogy," it seems to conflate a Fourth Amendment analogy, which can merely be useful for analyzing certain elements of a trade secret claim, with entirely substituting the Fourth Amendment test for the trade secret framework.[194]

Another commentator argues even more strongly that although some courts have suggested that certain standards within trade secret cases "can be derived by analogy to Fourth Amendment privacy jurisprudence," the Fourth Amendment analogy fails as a result of the differences between the underlying sources of trade secret law and Fourth Amendment law.[195] Among the various critiques of the analogy is that it "would leave courts without guidance in determining when" the analogy would apply.[196] The best way to solve that problem, suggests the argument, is to simply say that the analogy should never apply. This Article offers a different solution by presenting guidance to courts to evaluate when such analogies make sense.

Hermann III, *Privacy, the Prospective Employee, and Employment Testing: The Need to Restrict Polygraph and Personality Testing*, 47 WASH. L. REV. 73, 140–49 (1971) (explaining using the private state action approach to obtain constitutional protection for private employees).

191. Other scholars have explored the descriptive potential of other aspects of intellectual property law as a metaphor for describing Fourth Amendment law. *See* Nita A. Farahany, *Searching Secrets*, 160 U. PA. L. REV. 1239, 1244 (focusing on copyright law as a descriptive metaphor to think about Fourth Amendment cases).

192. Bruce T. Atkins, *Trading Secrets in the Information Age: Can Trade Secret Law Survive the Internet?*, 1996 U. ILL. L. REV. 1151, 1182.

193. *Id.* at 1182–83.

194. This becomes further apparent later in the analysis. *See id.* at 1183 ("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.").

195. Judge Richard Posner, Note, *Trade Secret Misappropriation: A Cost-Benefit Response to the Fourth Amendment Analogy*, 106 HARV. L. REV. 461, 462 (1992).

196. *Id.* at 472.

Other commentators have supported courts drawing an analogy to the Fourth Amendment "reasonable expectation of privacy" in determining whether a trade secret owner has used reasonable precautions in protecting her trade secret.[197] Under this view, if the owner of a trade secret has a reasonable expectation of privacy for Fourth Amendment purposes, that owner has used reasonable precautions in protecting the trade secret, and thus any violation of that reasonable expectation of privacy would constitute trade secret misappropriation.[198]

In addition to the literature addressing analogizing across the public-private divide within specific Fourth Amendment contexts, other scholars have addressed analogizing across the public-private divide outside the Fourth Amendment context. For example, Lior Strahilevitz advocates analogizing across the public-private divide in the context of information privacy.[199] More precisely, Strahilevitz supports courts analogizing to a reunified version of the common law of torts,[200] in interpreting various aspects of information privacy law beyond the Fourth Amendment, such as, for example, the Freedom of Information Act's ("FOIA") privacy provisions.[201] Specifically in the FOIA context, Strahilevitz notes that it "is natural to analogize between the common law invasion of privacy and the statutory 'unwarranted invasion of personal privacy'" language in the statute.[202] Strahilevitz acknowledges that:

> Courts must be able to recognize when an analogy breaks down, and must continue to do what the common law tradition asks of them—scrutinize precedents from peer and inferior courts carefully, follow them when appropriate, and reject them when their premises have been falsified or when their analysis does not persuade.[203]

One way to look at the project of this Article is that it offers courts a coherent and consistent way to recognize when the analogy breaks down and should be rejected, or is appropriate and should be persuasive.[204]

---

197. Peter J. Courture, *Independent Derivation and Reverse Engineering*, *in* VICTORIA CUNDIFF, TRADE SECRET PROTECTION AND LITIGATION: PROTECTING CONFIDENTIAL BUSINESS AND TECHNICAL INFORMATION 635 (PLI Patents, Copyrights, Trademarks & Literary Property Course Handbook Series No. 340, 1992).

198. *Id.*

199. *See* Lior Jacob Strahilevitz, *Reunifying Privacy Law*, 98 CALIF. L. REV. 2007, 2010–11 (2010).

200. *Id.* at 2011. For an interesting discussion of his argument that the four Prosser privacy torts should be reunified, see *id.* at 2012–15.

201. *Id.* at 2014–32.

202. *Id.* at 2020.

203. *Id.* at 2037–38.

204. Additionally, other scholars have addressed the public-private divide in contexts unrelated to privacy. *See, e.g.*, Adam Shinar, *Public Employee Speech and the Privatization of the First Amendment*, 46 CONN. L. REV. 1, 37–43 (2013) (addressing the public-private divide in the First Amendment context).

Although all this literature makes useful and important contributions to various aspects of the problem, to date neither courts nor scholars have offered a coherent and consistent normative framework for determining when courts ought to analogize across the public-private divide in various areas of privacy law. The remainder of the Article seeks to fill that void.

II. Reconsidering the Public-Private Divide in Privacy Law

This Part identifies and explores the possible justifications behind the traditional strict divide between the legal treatments of privacy violations that occur in the public sector from those that occur in the private sector. It begins by identifying various institutional features that may have historically justified distinguishing government invasions of privacy from private-sector invasions of privacy. For each justification, it then points out ways in which that traditionally governmental feature may now manifest itself in the private sector in the modern world.

A. Justifications for the Public-Private Divide in Privacy Law

The state action doctrine[205] that exists throughout constitutional law[206] means that the Constitution generally applies to governmental action, but not to private action. This is presumably based on an insight that there is something necessarily and categorically different about the government.[207] Similarly, the public-private divide in privacy law, as a specific application of the state action doctrine to the Fourth Amendment, is presumably based on an intuition that there is something necessarily and categorically different about privacy violations when they occur by the government, as opposed to those that occur by private-sector actors.[208] For Lillian BeVier that intuition is captured in the very

205. Numerous scholars have criticized the state action doctrine. *See, e.g.*, Chemerinsky, *supra* note 19, at 503–04 ("There are still no clear principles for determining whether state action exists."); Jody Freeman, *The Contracting State*, 28 Fla. St. U. L. Rev. 155 (2000) (identifying the challenges with applying the state action doctrine). This Article does not enter that debate. Suffice it to say that the state action doctrine both generally, and in the privacy context, is likely here to stay.

206. *See, e.g.*, Michael A. Helfand, *Arbitration's Counter-Narrative: The Religious Arbitration Paradigm*, 124 Yale L.J. 2994, 3035–38 (2015) (discussing the debates over whether arbitration misconduct can constitute state action and thus trigger the Fourteenth Amendment).

207. *Cf.* Shinar, *supra* note 204, at 37 (noting in the First Amendment context that the state action doctrine "rides on the intuition that there is something special about government").

208. Daniel Solove implicitly suggests this idea when he contends that the real problem with the extensive collection of personal information by the private sector is the widespread information flow from the private sector to the government. *See* Solove, *supra* note 31, at 1133–38 (describing the transfer of personal information from the private sector to the government in light of the harms of the government having that information); *see also* Lillian R. BeVier, *The Communications Assistance for Law Enforcement Act of 1994: A Surprising Sequel to the Break Up of AT&T*, 51 Stan. L. Rev. 1049, 1053 (1999) ("[O]ne must distinguish between threats to privacy that are posed by private parties and those that come from the government.").

notion and definition of "sovereign power."[209] As she explains, "[t]he threats posed by government eavesdropping or electronic surveillance are troublesome precisely because they are posed by the government, that ubiquitous repository of sovereign power whose actions by definition have implications and consequences different in kind from those of private actors."[210]

There are at least four features that traditionally distinguish the government from private actors that could support the intuition that the public sector should be treated differently from the private sector with regard to invasions of privacy. First, the government has powers of coercion that were not traditionally wielded by the private sector.[211] Second, governmental invasions of privacy can harm the abilities of individuals to make decisions about elements of their own identities by causing the individual to fear governmental reprisal based on their choices.[212] In addition to the limit this can cause on individual self-determination, this can also impact the free and open participation in democracy.[213] Third, the government historically had access to more sophisticated technology than society at large.[214] Finally, the bureaucratic nature of government can lead to various societal and individual harms.[215]

1. Government Has the Unique Power of Coercion

First, and perhaps most significantly, society may have a different expectation of privacy vis-à-vis the public sector because traditionally the government could exercise power that exceeded the power of the private sector.[216] This unique power results from a combination of coercion, state power, and the monopoly features of government. In its most extreme form, the traditional governmental police power involves the ability to take away an individual's liberty by placing them in jail, disrupting their lives and homes by searching them indiscriminately, or at the extreme even taking their lives. As Jody Freeman put it, "[e]ven in an era marked by the rise of multinational corporations . . . the claim that public power is more menacing than private power remains unmovable as a pivot point in American public law."[217]

---

209. *See id.*

210. *Id.*

211. *See infra* Part II.A.1.

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

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

214. *See infra* Part II.A.3.

215. *See infra* Part II.A.4.

216. *See* Secunda, *supra* note 21, at 303 (explaining that the state action doctrine is justified by the "power of the state in relation to the power of a private actor").

217. Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. REV. 543, 588 (2000). Adam Shinar has made a similar point in the First Amendment context, where he points out that the government "is often the only source of legitimate violence, and its status as provider of public goods

With regard to privacy law more specifically, many scholars have contended that the Fourth Amendment should best be seen as protecting individuals from government power and coercion. For example, Paul Ohm has argued that "[p]ower seems to be the amendment's essence, not merely a proxy for something deeper."[218] Similarly, Bill Stuntz contended that the Fourth Amendment should focus on coercion and violence.[219]

There is also some historical support for this government power-based justification for the public-private divide. Scholars have contended that the colonists designed the Fourth Amendment to respond to the British Crown's practice of general warrants, which allowed them to search people and their homes without suspicion.[220] Under this view, the conceptualization of the Fourth Amendment as about "security from unreasonable government intrusion" stems from the colonists' experience with the "arbitrary exercise of [British] power to invade their property."[221]

In many ways related to this idea of government power is a fear that if taken to the extreme, too many governmental invasions of privacy could allow the government to morph into the totalitarian state captured in our collective imagination by the Big Brother government in George Orwell's *1984*.[222] The Big Brother metaphor remains persuasive as one of the dangers of unfettered government access to information.[223] A totalitarian government presents a source of fear due to its ability to "achiev[e] total domination by monitoring every facet of its citizens' private lives."[224] Even in the absence of the totalitarian extreme, one version of the fear of government power is that the more society takes on totalitarian features, the greater the ability of the government to exercise social control over its citizens.[225]

Part of the source of the government's power is the extent to which the government has a monopoly in various ways. As Adam Shinar points

---

requires an element of coercion and authority that is not found in the market." Shinar, *supra* note 204, at 39.

218. Ohm, *supra* note 31, at 1338; *see also* Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1326 (2002) ("The Fourth Amendment protects power not privacy. This is not to say that the Fourth Amendment has nothing to do with privacy—the amendment clearly addresses privacy, or more precisely, the right of the people to be secure. Rather, the amendment is best understood as a means of preserving the people's authority over government—the people's sovereign right to determine how and when government may intrude into the lives and influence the behavior of its citizens.").

219. *See* William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 446 (1995).

220. *See* Morgan Cloud, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L. REV. 199, 296–97 (1993).

221. Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 351–52 (1998).

222. *See* GEORGE ORWELL, 1984 (1949).

223. *See* Solove, *supra* note 31, at 1101–02.

224. *Id.* at 1101.

225. *See id.* at 1102.

out, the government "is often the sole source of a particular service," so there is no ability to opt out.[226] Many of the government's services, such as the criminal and civil justice systems, national defense, and police, were at least traditionally public goods for which the government had a monopoly.[227] This is exacerbated by the fact that moving to a different country (or state) is challenging or sometimes impossible.[228] This monopoly power increases the coercive nature of state power as opposed to private sector power where most of the time there is more choice.

2. *Government Privacy Invasions Can Harm Individual Identity Formulation and Democracy*

A second possible justification for traditionally treating public-sector invasions of privacy as different in kind from private-sector invasions of privacy is that government privacy invasions can harm the ability of individuals to make identity-forming decisions about themselves. It can also inhibit individuals from engaging in democratic activities. This difference can also explain why society is prepared to differentiate between a reasonable expectation of privacy from the government versus a reasonable expectation of privacy from the private sector. There are various possible formulations of this justification.

First, there is the extent to which government privacy invasions can harm individual identity formulation and conversely the absence of privacy can impede the ability of individuals to express themselves and otherwise form their own identities. As other scholars have previously recognized, Fourth Amendment rights "create the environment necessary for other freedoms to flourish."[229] In the absence of adequate privacy protection "government information-gathering can severely constrain . . . individual self-determination."[230] This occurs because the excessive government invasions of privacy regarding an individual's activities can "corrupt individual decisionmaking about the elements of one's identity" by causing the individual to fear governmental repercussions based on

226. Shinar, *supra* note 204, at 39.

227. *Id.*

228. *Id.* at 40. The challenges of moving exacerbates the government's monopoly because individuals are faced with the choice between accepting the government's various invasions of their privacy or moving to somewhere where their privacy would not be invaded. If moving is extremely difficult or impossible, that means that there is no ability to opt-out of the government's privacy invasions.

229. Nadine Strossen, *The Fourth Amendment in the Balance: Accurately Setting the Scales Through the Least Intrusive Alternative Analysis*, 63 N.Y.U. L. REV. 1173, 1241 (1988); *see also* Monrad G. Paulsen, *The Exclusionary Rule and Misconduct by the Police*, 52 J. CRIM. L., CRIMINOLOGY & POLICE SCI. 255, 264 (1961) ("All the other freedoms, freedom of speech, of assembly, of religion, of political action, presuppose that arbitrary and capricious police action has been restrained. Security in one's home and person is the fundamental without which there can be no liberty.").

230. *See* Solove, *supra* note 31, at 1101–02.

individual choices.[231] This harm to self-determination[232] can occur unintentionally even if the government entities are not attempting to engage in social control or to intimidate individuals from engaging in certain activities.[233]

Relatedly, as a subset of self-determination, government invasions of privacy can harm an individual's freedom of association. The Supreme Court has recognized the "vital relationship between freedom to associate and privacy in one's associations."[234] As a result, in the First Amendment context the Court has limited the government's power to compel disclosure of group membership, an activity that would constitute an invasion of privacy, noting that "when a State attempts to make inquiries about a person's beliefs or associations" such inquiries "discourage citizens from exercising rights protected by the Constitution."[235]

Perhaps the most disturbing aspect of self-determination and interference with freedom of association is the extent to which government invasions of privacy can interfere with deliberative democracy.[236] As Shinar explains, "because of their dependence on elected officials for resources and funding, government institutions, unlike private firms, are more vulnerable to the risk of being used for improper political purposes."[237]

A variation of this theme may help justify why many scholars advocate a system in which public employees should have stronger privacy protections from their public employer than private employees do from their private employees. Just as in general governmental invasions of privacy may harm individual decision making including participation in democracy in the employment context, invasions of privacy by the public-sector employer into the privacy of the public-sector employee may harm the ability of the public employee to be the whistleblowing voice of other citizens against government waste, abuse, and fraud.[238] On the other hand, it is also possible to make the diametrically opposite argument that society ought to be willing to recognize a lower expectation of privacy from public-sector employees

231. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1657 (1999).

232. *Cf.* David S. Han, *Autobiographical Lies and the First Amendment's Protection of Self-Defining Speech*, 87 N.Y.U. L. REV. 70, 92–93 (2012) (explaining the importance of self-determination to individual personhood in the First Amendment context).

233. *See* Solove, *supra* note 31, at 1102 (noting "even if government entities are not attempting to engage in social control" the governmental invasions of privacy may still harm self-determination).

234. NAACP v. Alabama, 357 U.S. 449, 462 (1958).

235. Baird v. State Bar of Arizona, 401 U.S. 1, 6 (1971).

236. *See* Schwartz, *supra* note 231, at 1651–52 (arguing that inadequate protection of privacy can inhibit people from engaging in democratic activities).

237. Shinar, *supra* note 204, at 40.

238. Secunda, *supra* note 21, at 306–09 (noting, *inter alia*, that "employee privacy rights in the public sector are crucial so that these employees can fulfill their role of ensuring government transparency and accountability").

than private-sector employees precisely because the public sector-employees have special responsibilities and powers that have to be exercised in accordance with the public trust, such that the exercise in monitoring government is particularly strong. These sorts of arguments certainly appear relevant when considering such hot topic current issues as whether police officers should have to wear body cameras, a policy decision which necessarily invades the privacy of the police officer, but perhaps can be justified by the great responsibilities and powers given to the police. Hence, which of these arguments carries the day may depend in part on the particular type of governmental employee, and other factually specific considerations involving the degree of power given to the particular employee.

Overall, however, the increased concern that privacy invasions by the government are more likely to harm individual self-determination as well as participation in democracy may help justify the public-private divide in how society wants to think about reasonable expectations of privacy across the two sectors.

3. Government Has Access to Superior Technology

A third justification that might distinguish reasonable expectations regarding government invasions of privacy from similar invasions by the private sector is the government's superior capabilities with regard to technology. The Supreme Court has suggested that this difference between the public and private sector constitutes part of the justification for the public-private divide. In *Dow Chemical Co.*, the Court stated in dictum that "[i]t may well be, as the Government concedes, that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant."[239] The Court followed similar logic in *Kyllo v. United States*,[240] ruling that the government violates the Fourth Amendment when it uses technology that is "not in general public use" to see "details of the home that would previously have been unknowable without physical intrusion."[241]

---

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

240. 533 U.S. 27 (2001).

241. *Id*. at 40; *see also* Nadia B. Soree, *Show and Tell, Seek and Find: A Balanced Approach to Defining a Fourth Amendment Search and the Lessons of Rape Reform*, 43 SETON HALL L. REV. 127, 225–26 (2013) (describing the *Kyllo* decision as "significant because the Court signaled its understanding that when police resort to extraordinary technological measures to invade privacy, with such means being generally available only to police, individuals fail to successfully resist the intrusion, both because successful resistance is not feasible in light of the superior technological capability of the police, and because people would not be on notice of the need to resist."). Of course, often technology that is unique to government at the time later becomes available to the private sector as well. This is the case with the technology in *Kyllo* which is now available by app in the private sector. *See* Don

Various scholars have pointed out the importance of the government's technological superiority to the Fourth Amendment framework. For example, Orin Kerr has suggested that the Fourth Amendment precedent, at least in the criminal context, can be seen as implementing a goal by courts to balance governmental advances in technology with advances in technology that thwart the government's law enforcement aims.[242] Under Kerr's equilibrium-adjustment theory, courts implementing the Fourth Amendment strive to protect a technologically level playing field.[243] Similarly, Paul Ohm agrees that "[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."[244] For Ohm, this ratio can be determined by examining the metrics of crime fighting such as how long investigations take.[245] Thus, the government's access to superior technology comprises another possible difference between the public and private sectors that may justify treating reasonable expectations of privacy across the public-private divide differently.

4. Government Is Too Bureaucratic

A fourth possible reason justifying the traditional public-private divide in privacy law is that government invasions of privacy are subject to the harms that routinely arise as an inevitable consequence of bureaucratic settings.[246] According to Daniel Solove, the harms from government privacy invasions are amplified because of the bureaucratic nature of government that causes decisionmaking without sufficient accountability, the dangers that arise from "unfettered discretion," and the focus on short-term goals at the expense of a long-term view of the world.[247]

To be clear, this justification is less rooted in history than some of the earlier suggested justifications, as at the time of the Fourth Amendment, there were no organized police forces.[248] Rather, it is a

---

Clark, *Smart Phone Add-Ons Offer Thermal Imaging*, WALL ST. J. (Aug. 18, 2014, 5:13 PM), http://www.wsj.com/articles/smartphone-add-ons-offer-thermal-imaging-1408396425.

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

243. *Id.* at 480; *see also* Ric Simmons, *Why 2007 Is Not Like* 1984*: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence*, 97 J. CRIM. L. & CRIMINOLOGY 531 (2007).

244. Ohm, *supra* note 31, at 1346.

245. *Id.*

246. *See* Solove, *supra* note 31, at 1104.

247. *Id.*

248. *See* Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 82 (1988).

more modern justification in support of the traditional public-private divide. In today's modern world, law enforcement has become highly bureaucratized.[249] Solove contends that as a result of the tremendous pressures on law enforcement agencies to capture criminals, solve crimes, prevent crime, and prevent terrorism, the bureaucracy is subject to bad exercises of discretion, short cuts and obliviousness.[250]

Of course the bureaucratic nature of government may not be entirely negative. Shinar argues that the government is in fact deliberately "more 'bureaucratic' than their private sector analogues." He contends that bureaucracy is the intentional limit on the powers of government: "[w]e the people insist that they be more constrained, that there be more red tape."[251] Regardless of whether these features mean that there is an inevitable negative side effect of bureaucracy, or its very purpose, the bureaucratic nature of government may justify treating the government differently, whether as a symptom of a problem, or because bureaucracy is the very remedy itself for limiting the powers of government.

B. Reconsidering the Justifications for the Public-Private Divide

Thus far this Part has explored the intuition that there is something necessarily and categorically different about privacy violations when they occur by the government, as opposed to privacy violations by the private sector, and has offered four possibilities for differences that at least traditionally distinguished the government. This next portion seeks to reconsider those differences, and to point out that in the modern world it is not always obvious that those features belong uniquely to the government. Rather, in today's society[252] these dangers are equally possible in the private sector depending on the particular circumstances.

To be clear, the purpose of this Subpart is not to argue that the government and the private sectors are universally identical, or that the state action doctrine should be abolished. Rather, by pointing out that at times the private sector has come to have many of the features that traditionally distinguished government, this Subpart sets up the argument in Part III that courts should look for the presence of these features in deciding whether an analogy across the public-private divide is appropriate.

---

249. Solove, *supra* note 31, at 1106.

250. *Id.*

251. Shinar, *supra* note 204, at 40.

252. It is certainly possible that at the time of the Fourth Amendment that there was a categorical difference between the government and the private sector with regard to these dangers. I am not a historian, and will not weigh in on that point, but I certainly do not dispute it and am inclined to believe it was true. My point is about the realities of the modern world.

1. Private Sector Can Also Have the Power of Coercion

The first differentiating feature considered in the justification of the public-private divide is that the government traditionally has unique power that exceeds the power of the private sector. The strongest form of this power occurs when the government is acting within its capacity for police power whereby it is capable of harming actual freedom and liberty and even taking the life of individuals.

Though the police power is the strongest form of government coercion, certain private-sector entities also exert government-like police power. For example, private-sector policing groups such as security guards have received increased authority, and some can go so far as to functionally arrest or detain individuals.[253] Similarly, the private sector exercises police-like power when government agencies hire private security companies to perform work that was previously carried out by law enforcement officers.[254] Although others have contended that in these circumstances the state action doctrine should not bar application of the Fourth Amendment to the private-sector actors,[255] such an extreme change in the doctrine is unlikely to occur. This Article suggests instead that courts facing such private-sector invasions of privacy that closely resemble police-power ought to feel free to analogize to similar cases in the Fourth Amendment context as persuasive authority. These analogies would recognize that there remain some differences between the private-sector police power and the public-sector police power, such as the ability to send an individual to jail. These differences may caution against directly applying the Fourth Amendment, but nonetheless may support the use of analogies in determining the reasonable expectation of privacy of the individual from the coercive private-sector actor in the context of a private-sector case.

Of course many types of government action do not involve the government police power. Nonetheless, the government has historically had other forms of power and coercion at its disposal, including economic power. In the modern world, the private sector too, however, has the potential for a great deal of power. As Professor Malloy has argued in the workplace privacy context, "the aggregation of wealth and power . . . has given private employers the same capacity to threaten privacy as the government. Thus, the threat originally seen to emanate just from government now arises in the commercial sector—a threat

253. *See* Elizabeth E. Joh, *The Paradox of Private Policing*, 95 J. CRIM. L. & CRIMINOLOGY 49, 50 (2004).

254. David A. Sklansky, *The Private Police*, 46 UCLA L. REV. 1165, 1177 (1999).

255. *See generally* Joh, *supra* note 253 (contending that this private policing trend warrants application of Fourth Amendment protections to situations where private-sector security guards engage in such police-power behavior).

that . . . can be just as invasive and harmful as government surveillance."[256]

Similarly, the private sector is not immune from the fears that underlie the surveillance capabilities of Big Brother. Just as the totalitarian government incites dread due to its ability to achieve total societal "domination by monitoring every facet of its citizens' private lives,"[257] companies like Google are capable of monitoring every aspect of private lives as well. And it is not always obvious that individuals have the right to opt-out of such private-sector monitoring. Furthermore, just as the government's monopoly power can result in coercive elements within its services, there are numerous aspects of the private sector that also contain monopoly-like features. This can lead to an inability to entirely opt out of the system. For example, this is increasingly true in a difficult job market where the lack of meaningful alternatives and the pervasive fear of unemployment cause more dependence on the employer. This results in the removal of some constraints on employer invasions of privacy that would otherwise have existed in a more competitive market.

2. *Private Sector Can Also Harm Individual Identity Formulation and Democracy*

Just as government privacy invasions can harm individual identity formulation and deter individuals from engaging in democratic activities including whistleblowing, certain private-sector privacy invasions can cause similar harms. Prominent sociologist Amitai Etzioni has recounted the various ways in which private-sector invasions of privacy can have many of the same effects as violations committed by the government including the "'chilling' of expression and dissent."[258] Etzioni offers the examples of gays who are outed by the media, banks who call in loans of individuals they find out have cancer, and employers who refuse to hire individuals because of their political or religious views.[259] All of these possible harms from private-sector privacy invasions can result in individuals hesitating to be open with and true to aspects of their identity.

Similarly, social pressure from whatever source, governmental or private sector, can deter individuals from engaging in democratic activities. Think for example, of the recent CEO of Mozilla who was fired for engaging in a form of democratic activity, namely for making a

256. Wilborn, *supra* note 20 at 830.
257. Solove, *supra* note 31, at 1101.
258. Etzioni, *supra* note 31, at 934.
259. *Id.*

personal political donation.[260] In light of that experience and many others like it, it seems reasonable to believe that private-sector invasions of privacy—from the media, employers, social media, and so on—can influence individual behavior perhaps even more strongly than government invasions of privacy in many circumstances. This suggests that where a particular private-sector privacy invasion would be likely to impact either individual identity formation, or participation in democracy, or both, analogizing to similar governmental invasions of privacy would be more appropriate.

3. The Private Sector Has Unprecedented Access to Technology

Although traditionally the public-private divide in privacy law may have been justified by the fact that the government had access to privacy-invading technology that was unavailable to the private sector, that difference has begun to break down. In the modern world many companies have access to the sorts of privacy-invading technologies that traditionally would have been exclusively in government hands. There are countless examples of this phenomenon. As Mary Leary has persuasively noted, the modern day privacy threat is not always governmental because "private commercial entities have introduced technologies into daily life which fail to afford individuals the opportunity to demonstrate an expectation of privacy."[261] Leary points to such examples as the commercially-available satellite imaging technology of Google Earth, the Internet tracking of personal information, and the geospatial locating of cell phones, all of which are not limited to the government.[262]

For instance, traditionally only the government would have had access to satellite technology.[263] Prior to the new millennium, satellite technology was limited to the realm of the military and intelligence communities.[264] These days, satellite-based technologies, such as Google Earth, are not only available to corporations such as Google, but have become mainstream and available to the general public.[265]

---

260. *See* Tony Bradley, *Backlash Against Brendan Eich Crossed a Line*, FORBES (Apr. 5, 2014, 9:22 PM), http://www.forbes.com/sites/tonybradley/2014/04/05/backlash-against-brendan-eich-crossed-a-line/.

261. Mary G. Leary, *The Missed Opportunity of* United States v. Jones*: Commercial Erosion of Fourth Amendment Protection in a Post-Google Earth World*, 15 U. PA. J. CONST. L. 331, 333 (2012).

262. *Id.* at 332–33.

263. Ricky J. Lee & Sarah L. Steele, *Military Use of Satellite Communications, Remote Sensing, and Global Positioning Systems in the War on Terror*, 79 J. AIR L. & COM. 69, 71 (2014) (noting that "before the present millennium, military and civilian satellites were usually exclusive of each other and both tended to be government owned").

264. *Id.*

265. *See* Kevin Werbach, *Sensors and Sensibilities*, 28 CARDOZO L. REV. 2321, 2344 (2007) (noting that satellite photos "are now much more widely available to the public, thanks to services such as Google Maps").

Similar phenomena occur with all sorts of privacy-invading technologies as their use becomes more widespread in the private sector. Observers have noted the privacy-violating potential of such technological developments as Google Glasses.[266] Amazon has announced plans to make use of drones.[267] Additionally, the use of biometric technology and GPS tracking is widespread in the private sector from employers to other private companies.[268] As a result, the government no longer has unfettered access to superior technology that is unavailable in other sectors. As such, courts can no longer automatically rely on governmental technological superiority to justify treating governmental invasions of privacy entirely differently from private-sector invasions of privacy. Rather, courts ought to consider the technological prowess of a particular private sector privacy-invading actor in deciding whether to analogize to an equally technologically advanced public-sector Fourth Amendment case.

4. Private Sector Can Also Be Extremely Bureaucratic

As for the final justification for the public-private divide in privacy law, the harms that can occur as a result of the bureaucratic nature of government, the very same sort of bureaucratic-driven harms can also take place in the private sector. Scholars have recognized that the private sector often resembles the sort of bureaucracy typically used to describe the government. For example, in his influential 1984 *Harvard Law Review* article, Gerald Frug contends that corporations and government agencies share "characteristics that have traditionally identified 'bureaucracy' as a form of social organization."[269] Many scholars since have also noted the bureaucratic features of the private sector.[270] In the privacy context, Solove observes that in the private-sector information is

266. Kashmir Hill, *How Google Glasses Make a Persistent, Pervasive Surveillance State Inevitable*, FORBES (Apr. 6, 2012, 11:16 AM), http://www.forbes.com/sites/kashmirhill/2012/04/06/how-google-glasses-make-a-persistent-pervasive-surveillance-state-inevitable/.

267. *See* Gregory S. McNeal, *Six Things You Should Know About Amazon's Drones*, FORBES (July 11, 2014, 6:57 AM), http://www.forbes.com/sites/gregorymcneal/2014/07/11/six-things-you-need-to-know-about-amazons-drones/.

268. *See generally* Elizabeth M. Walker, Note, *Biometric Boom: How the Private Sector Commodifies Human Characteristics*, 25 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 831 (2015) (discussing the increased use of biometric technologies in the private sector); *see also* Laura Silverstein, *The Double Edged Sword: An Examination of the Global Positioning System, Enhanced 911, and the Internet and Their Relationships to the Lives of Domestic Violence Victims and Their Abusers*, 13 BUFF. WOMEN'S L.J. 97, 103 (2005) (noting that GPS has shifted from solely a military instrument to a common tool in the private sector).

269. Gerald Frug, *The Ideology of Bureaucracy in American Law*, 97 HARV. L. REV. 1276, 1278 (1984).

270. *See, e.g.*, Stephen M. Bainbridge, *Participatory Management Within a Theory of the Firm*, 21 J. CORP. L. 657, 661 (1996) (acknowledging that the traditional view of "the corporation as a bureaucratic hierarchy is largely correct"); Lawrence E. Mitchell, *Structural Holes, CEOs, and Informational Monopolies: The Missing Link in Corporate Governance*, 70 BROOK. L. REV. 1313, 1357 (2005).

often held not by trusted friends or family members, but by "large bureaucracies that we do not know very well or sometimes do not even know at all."[271]

Unsurprisingly then, the very harms associated with the bureaucratic features of government are also common critiques in the private sector. Above all, the private sector has often been criticized for its lack of accountability.[272] Frug contends that "corporate bureaucratic power, as it has emerged, has imposed a forceful objective restraint on the shareholders' ability to govern the corporation."[273] Thus corporate bureaucratic power limits accountability to the shareholders. In the privacy context, Solove has illustrated the lack of accountability by corporations in collecting data.[274] Many have criticized corporations for "unfettered discretion."[275]

Finally, the critique of government bureaucracies as making choices based on short-term goals without consideration of the long-term consequences of the larger social effects is also an extremely common problem in the private sector.[276] Vice Chancellor of the Delaware Court of Chancery, Leo Strine Jr. has extensively discussed the problems with corporations being managed for the short-term at the expense of the long-term.[277] Scholars have also extensively documented this potentially harmful phenomenon.[278] For example, a number of scholars have offered

---

271. Solove, *supra* note 31, at 1095.

272. Paul N. Cox, *The Public, the Private and the Corporation*, 80 MARQ. L. REV. 391, 464 (1997) (describing the standard critique of classic liberalism with respect to the corporation as failing to account for private power which is "the hierarchical authority of management and is thought, by the terms of the critique, to be unaccountable, unconstrained or arbitrary"). For the classic account of the absence of accountability, see ADOLF A. BERLE & GARDINER C. MEANS, THE MODERN CORPORATION AND PRIVATE PROPERTY (Harcourt, Brace, and World rev. ed. 1967) (1932).

273. Frug, *supra* note 269, at 1306.

274. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1429 (2001).

275. Katharine V. Jackson, *Towards a Stakeholder-Shareholder Theory of Corporate Governance: A Comparative Analysis*, 7 HASTINGS BUS. L.J. 309, 328 (2011) ("Corporations became entities of immense economic and political power that afford boards of directors and corporate executives largely unfettered discretion to govern as they see fit, subject only to market pressures and the agitations of activist shareholders."); *see also* LYNN STOUT, THE SHAREHOLDER VALUE MYTH: HOW PUTTING SHAREHOLDERS FIRST HARMS INVESTORS, CORPORATIONS, AND THE PUBLIC 110 (2012) ("[F]or most of the twentieth century directors of public companies who did not breach their loyalty duties enjoyed virtually unfettered discretion to set corporate policy.").

276. *See generally* Robert Anderson IV, *The Long and Short of Corporate Governance*, 23 GEO. MASON L. REV. (forthcoming 2015) (criticizing the emphasis on short-term shareholders in explaining the short-term governance phenomenon).

277. Leo E. Strine, Jr., *One Fundamental Corporate Governance Question We Face: Can Corporations Be Managed for the Long Term Unless Their Powerful Electorates Also Act and Think Long Term?*, 66 BUS. LAW. 1, 10–11 (2010) (explaining that because "institutional investors often have a myopic concern for short-term performance," managers have "little reason to think deeply about the effect of corporate governance proposals on long-term corporate performance").

278. *See, e.g.*, Emeka Duruigbo, *Tackling Shareholder Short-Termism and Managerial Myopia*, 100 KY. L.J. 531, 531 (2011) ("Short-termism denotes the phenomenon by which some corporate

this so-called "short-termism" as an explanation for what occurred with the collapse of Enron.[279] This bureaucracy-like focus on short-term goals at the expense of long-term goals causes the private sector to often have the same problematic relationship to privacy invasions as its public sector government counterpart. Overall, many aspects of the private sector resemble precisely the sort of bureaucracy that epitomizes government. As such, courts ought to consider the presence of such bureaucratic characteristics, and the resulting privacy concerns that come along with them, in deciding whether to analogize between the public and private sectors.

III. A Normative Framework for Privacy Analogies

This Article is about overcoming the public-private divide for the purpose of privacy analogies. The important normative question that courts and scholars continue to evade is whether it is appropriate for a court analyzing the reasonable expectation of privacy portion of a Fourth Amendment case to consider the fact that in a private-sector case a court has protected the plaintiff against precisely the sort of privacy invasion the government committed.[280] Or in reverse, whether it is appropriate for a court engaging in a doctrinally similar analysis in a private-sector privacy case to take into account a judicial decision from a Fourth Amendment case in which a court has held that a factually similar privacy invasion violated a defendant's reasonable expectation of privacy.

This Part builds on Part II by suggesting that courts deciding whether to analogize across the public-private divide should consider the applicability of the differentiating features identified in Part II that traditionally distinguished governmental invasions of privacy. This multifactored analysis should then inform the currently haphazard question of whether the analogy is appropriate.

---

managers, responding to pressure from investors or acting to bolster their own position, advert their attention and exert their energies to achieving short-term profitability, virtually eschewing longer-term considerations. . . . Short-termism promotes a tendency to overvalue short-term rewards, invariably leading to an undervaluation of long term consequences.").

279. *See, e.g.*, William W. Bratton, *Enron and the Dark Side of Shareholder Value*, 76 Tul. L. Rev. 1275, 1283 (2002) (explaining the collapse of Enron in terms of short-term decisionmaking); Jill E. Fisch, *Measuring Efficiency in Corporate Law: The Role of Shareholder Primacy*, 31 J. Corp. L. 637, 673 (2006).

280. *Cf.* Shima Baradaran, *Rebalancing the Fourth Amendment*, 102 Geo. L.J. 1, 29–32 (2013) (arguing that courts considering Fourth Amendment cases ought to consider wider information contained in statistical data, clinical evidence, and experience, rather than only intuition and common sense).

A. The Normative Framework in the Abstract

Courts should consider whether the specific governmental actor in the public-sector privacy case that is subject to the potential analogy exhibits the four features traditionally differentiating government. Courts should ask themselves: First, did the government in this situation exercise uniquely governmental coercion or hold monopoly power? Second, did the government in this case act in such a way that its invasion of privacy is likely to harm individual self-determination and/or democratic participation? Third, did the government invade privacy by using sophisticated technology that exists solely in the hands of the government? Finally, does the privacy-invading governmental actor suffer from the various bureaucratic features—namely lack of accountability, unfettered discretion, and a short-term focus—that can cause invasions of privacy to be particularly harmful?[281]

Courts should then also consider whether the particular privacy-invading actor in the private-sector privacy case that is subject to the potential analogy also exhibits those four features to a similar extent to the governmental actor. Did the private-sector actor exercise a similar degree of power and coercion to the government? Is this particular form of private-sector invasion of privacy likely to harm individual self-determination and democratic participation in a way that is comparable to the form of privacy invasion exercised by the government? Did the private-sector actor use a similar technological advantage to that used by the government? And finally, does the particular type of private actor at issue share similar bureaucratic features with their accompanying harms to its public-sector counterpart?

After asking these questions and comparing the two cases along these four factors, courts can make a better informed decision as to whether this is an appropriate case for analogizing across the public-private divide for the purpose of deciding the reasonable expectation of privacy analysis or its doctrinal equivalent. Should the factors be sufficiently comparable, then analogizing is appropriate. Should the factors be sufficiently different, then courts ought to proceed carefully before deciding to analogize across the public-private divide. As with many multifactored tests, a concept courts are quite familiar with, no single factor is dispositive, nor is this a purely quantitative question. Instead, these factors offer a framework for what sorts of questions courts ought to consider when deciding whether analogizing across the public-private divide is appropriate in a privacy law context.

To be sure, particularly in the context of evaluating reasonable expectations of privacy, courts need to be careful to keep in mind the role of both floors and ceilings in conducting the analysis. For example,

281. *See* Solove, *supra* note 31, at 1104.

assume that a certain private-sector case finds that an individual has a reasonable expectation of privacy from the private sector. Then assume that a second court faces a factually similar case, except that now it is the government, which is invading the individual's privacy. The second court applies the multifactored normative framework suggested above and concludes that the governmental actor has considerably more of the traditional factors than the private sector. This would suggest that the individual ought to have a higher expectation of privacy from the government than from the private sector. In such a circumstance, analogizing might still be appropriate because the private-sector case could constitute a floor for the court to consider. In other words, the court could conclude that the public ought to have a higher expectation of privacy from the governmental actor than from a private-sector actor. The private sector finding remains relevant, however, to show the court that at the very least the public has a certain level of protection of privacy from the private sector, such that the level of protection of privacy from the government must exceed that floor.

Now assume instead that a judicial decision in a private-sector case finds that the plaintiff does not have a reasonable expectation of privacy from the private-sector actor in that case. A second court considers a factually similar case, only now it is the government, which is invading the individual's privacy. The court engages in the multifactored normative framework and concludes that the governmental actor has more of the traditional factors than the private sector. This once again suggests that the individual has a higher expectation of privacy from the government than from a private-sector actor. In such a circumstance, the fact that the earlier case found that the individual did not have a reasonable expectation of privacy from the private-sector actor does not tell the second court much because the factors indicate that the individual ought to receive a higher expectation of privacy from the government than from the private sector.

Furthermore, it is important to note that the reasonable expectation of privacy analysis is often not outcome determinative of the entire case. It is plausible that a court may engage in the multifactored normative analysis described above to determine that a particular plaintiff had a reasonable expectation of privacy. The reasonable expectation of privacy analysis is merely one part of the Fourth Amendment analysis. The court might still determine that despite the fact that the plaintiff had a reasonable expectation of privacy, that the government's reason for invading that privacy nonetheless justifies the intrusion. This difference in the rationale for the privacy intrusion might justify a different ultimate outcome in a public-sector case than in a private-sector case, even where there is a similar reasonable expectation of privacy. The court should be able to reach a different outcome in the cases while still acknowledging

that the reasonable expectation of privacy portion of the analysis is comparable.

B. The Normative Framework Applied to a Hypothetical

To better understand how this normative framework would work in practice, this Subpart will walk through how a court would approach analogizing across the public-private divide in the context of a hypothetical scenario. Assume that the Securities and Exchange Commission ("SEC") is investigating potential insider trading and other securities violations at a medium-sized hedge fund. Traditional investigatory techniques, such as obtaining a warrant for the company's documents, might tip off individuals inside the company. So instead, the SEC decides to hire a computer systems expert and/or hacker to determine whether there was any information available from the hedge fund's computer systems that could be obtained by someone who knew what they were looking for, but without violating any laws. The SEC pays the hacker to hack into the hedge fund's computers and to investigate any wrongdoing. Although the hacker, despite being extremely good at what he does, is unable to gain access to the fund's e-mails, he is able to exploit exposures in the hedge fund's various firewalls to obtain information about all the hedge fund's trades for the SEC. Later, when the SEC brings a civil enforcement action against individuals at the hedge fund for violations of securities laws, a Fourth Amendment claim is raised based on how the SEC obtained its information.

In analyzing the Fourth Amendment claim, one of the questions the court considers is whether the hedge fund had a reasonable expectation of privacy in its trades. The government argues that the mere fact that the computer expert was able to get into the hedge fund's system suggests that the fund could not have a reasonable expectation of privacy because many computer experts could have gotten in. The government also argues that the hedge fund failed to hire a cybersecurity firm, which many hedge funds have hired to protect themselves. By not hiring such a firm, the government argues, the hedge fund should have no reasonable expectation of privacy.

In response, the hedge fund points to a similar case in the trade secret context. In that case, a computer hacker was found liable for trade secret violations under the applicable state trade secret law, for similarly exploiting weaknesses in the computer security of a hedge fund in order to obtain trading secrets.[282] In the trade secret case the hedge fund had also used a firewall and other protections, but had not hired a

282. This hypothetical is very loosely based on actual events that recently took place in the private sector. *See* Myles Udland, *A Hedge Fund Was Hacked in a Never-Before-Seen Attack*, Bus. Insider (June 19, 2014, 9:43AM), http://www.businessinsider.com/hedge-fund-hacked-in-complex-attack-2014-6.

cybersecurity firm. Nonetheless, in the context of the trade secret case, the court found that the hedge fund's trade strategy was a "trade secret" under the UTSA meaning that it "is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[283] In deciding whether to analogize to the trade secret case, or even consider it as persuasive (clearly not binding) in determining whether a hedge fund has a reasonable expectation of privacy in information that can be obtained by a computer hacker, the court ought to begin by engaging in the multifactored normative framework.

First, the court should consider the power of coercion of the government versus the private party in the two cases under consideration. In this hypothetical, the government actor at issue is the SEC. Although the securities laws prohibit conduct both criminally and civilly, the SEC is only responsible for civil enforcement and administrative actions. In a civil enforcement action, the SEC can obtain a court order enjoining an individual from further violations of securities laws, disgorgement of any money obtained from the illegal conduct, and in some circumstances impose civil penalties. Importantly, the SEC may not engage in criminal enforcement of the federal securities laws, although they can provide assistance to the U.S. Attorney and U.S. Department of Justice to do so. Therefore, although the SEC has a good deal of power of coercion in its civil enforcement role, that power of coercion is not significantly greater than the power of coercion a hacker has when stealing trade secrets. The hacker can also coerce the hedge fund to pay large amounts of money, or if they do not do so can impose a tremendous financial cost on the hedge fund. Significantly, neither the SEC nor the civil-sector hacker can put anyone in jail. If the hypothetical were modified such that the Fourth Amendment claim were being brought in the context of a criminal trial brought by the U.S. Attorney or U.S. Department of Justice, then the power of coercion factor would look very different because the government would be acting at the peak of its power of coercion, thus suggesting that higher levels of protection should be granted vis-à-vis the government. Under the existing hypothetical, however, the power of coercion in both sectors is primarily economic in nature, and therefore the public and private sectors are relatively comparable for this first factor.

Next, for the second factor, the court should consider the impact of each party's privacy invasion on individual self-determination. The target of both of these privacy invasions is a hedge fund, but corporations can have privacy interests by virtue of the individuals that make up those corporations.[284] Therefore, a court needs to consider whether the

283. UNIF. TRADE SECRETS ACT § 1(4) (UNIF. LAW COMM'N 1985).

284. Elizabeth Pollman, *A Corporate Right to Privacy*, 99 MINN. L. REV. 27, 59–64 (2014).

individuals who make up the hedge fund are likely to have their individual self-determination impacted as a result of the privacy invasion by either the public-sector or private-sector hacker. Both the public-sector hacker and the private-sector hacker obtained information about the hedge fund's trades, and not personal information about employees. Had the information hacked included such information as employee personnel files, e-mails and so on, the privacy invasion may have had more impact on individual self-determination. Under the existing hypothetical, however, the second factor does not really come into play, as there is likely minimal impact on individual self-determination from this type of privacy invasion.

Third, the court should consider the extent to which the government privacy invasion benefitted from access to superior technology. In this hypothetical it did not. The government hired a computer hacker, just like in the trade secret case. Had the government made use of uniquely government resources, such as NSA databases, or some sort of military-only cryptography, this factor would suggest great protection from the government than the private sector. As the hypothetical currently stands, this technological advantage factor is comparable for both the public and private-sector privacy invasions.

Finally, the fourth factor requires the court to evaluate the extent to which each of the parties contains the sorts of bureaucratic characteristics that can cause difficulties with privacy invasions. This factor differs between the public and private sectors in this hypothetical. The privacy-invading party in the government context, the SEC, is very much the epitome of a government bureaucracy. The SEC has five divisions and eleven regional offices throughout the United States. In addition, the SEC has a number of substantive offices.[285] Considering how many offices and branches they have, the SEC is subject to precisely the sorts of privacy concerns that exist whenever there are features of a bureaucracy. By contrast, the court in the hypothetical does not necessarily have information about who hired the hacker in the trade secret case. Therefore, there is no reason to necessarily believe that the trade secret case features the same sort of bureaucratic features as the SEC. Hence, this last feature suggests that a hedge fund should have a greater expectation of privacy from the bureaucratic government than from the private sector.

---

285. These include the Office of General Counsel; the Office of the Chief Accountant; the Office of Compliance, Inspections and Examinations; the Office of International Affairs; the Office of Investor Education and Advocacy; the Office of Economic Analysis; the Office of Information Technology, the Inspector General, who has a staff of twenty-two; and the SEC Office of the Whistleblower. *SEC Divisions Homepages*, U.S. SEC. & EXCH. COMM'N, http://www.sec.gov/divisions.shtml (last visited Dec. 18, 2015).

Putting all of the factors together, the court will conclude in this particular hypothetical that the hedge fund should have at least the same if not more of an expectation of privacy from the government than from the private sector. Therefore, to the extent that the trade secret case suggests that society has recognized a reasonable expectation of privacy in a hedge fund's trading information even if the fund did not hire a cybersecurity company, the court should feel comfortable analogizing to the trade secret case. Once again this intermediate conclusion with respect to analogizing for the reasonable expectation of privacy analysis does not necessarily mean that the two cases should ultimately have the same result. The court may determine that the fund has a reasonable expectation of privacy in its trading information, but that the government's rationale for engaging in this privacy violation justifies the privacy intrusion in a balancing analysis in a way that the private sector's corporate espionage justification would not.

Now for purposes of thoroughly understanding the multifactored normative framework, assume that the hypothetical changes such that the analogizing is happening in reverse. Under the new hypothetical, a court considering a trade secret case is trying to decide whether the trading information is in fact a trade secret, which turns on whether the hedge fund took steps that "are reasonable under the circumstances to maintain its secrecy." The court is considering analogizing to a Fourth Amendment case with the same facts as above, in which a court found that there was a Fourth Amendment violation and thus necessarily that there was a reasonable expectation of privacy. The court should first consider each of the four factors precisely as above. This time, however, the fact that the factors suggest that society might want to give an individual more of an expectation of privacy from the government than from the private sector as a result of the government's bureaucratic features means that an analogy would likely be inappropriate. Because the factors suggest that there should be more privacy protection from the government, the fact that the company received privacy protection from the government, does not help guide the court as to whether the company should also receive privacy protection vis-à-vis the private-sector hacker. A similar process would occur in any situation in which the court was considering analogizing across the public-private divide, whether in workplace privacy, trade secrets, or any other context.

CONCLUSION

Various areas of privacy law contain doctrinal similarities, including some version of consideration of an individual's reasonable expectation of privacy. The existence of the state action doctrine means that courts may not entirely conflate private-sector privacy cases with public-sector Fourth Amendment cases. Nonetheless, given the doctrinal similarities,

there are various situations in which courts naturally consider analogies between the public and the private sector case law to make sense and be appropriate.

Until now, courts have not had a coherent or consistent normative framework for deciding whether to apply such analogies across various privacy law scenarios. In the absence of such a framework, courts seem to draw analogies in a haphazard manner and without any discussion of whether and why the analogy makes sense or does not make sense in a particular case. The multifactored normative framework presented in this Article represents a starting point to move beyond that seemingly random and unarticulated system. Moving forward, courts considering analogizing between public-sector and private-sector privacy cases ought to evaluate the presence of power and coercion, the impact on self-identity and democratic participation, the existence of any technological advantages, and the bureaucratic features of the corresponding privacy-invading powers in both cases. Or, in other words, courts ought to start looking at when corporations behave like the state because they take on features that resemble those of the state.

It is certainly possible that courts and scholars may identify other differences not articulated here between the public and private sectors that would suggest that courts ought to not analogize across the public-private divide when that difference is present. I welcome such additions and debates. As long as courts and scholars are applying a coherent and consistent normative framework and articulating the reasons they believe privacy analogies are or are not appropriate in a particular context, it would be a substantial improvement over the status quo.

***