OVERCOMING THE PUBLIC-PRIVATE DIVIDE IN PRIVACY LAW*

Victoria Schwartz***

When a photographer uses an airplane to take 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 would likely constitute improper trade secret misappropriation. If, however, the government hired the photographer, the aerial photography would not violate the Fourth Amendment. This illustrates a public-private divide in which privacy violations by the government are treated entirely separately from privacy violations by the private sector. Despite this divide, some courts have analogized from the Fourth Amendment into the trade secret context, while in the opposite direction the Supreme Court has rejected such an analogy from the trade secret context into a Fourth Amendment case.

A similar but reverse phenomenon occurs in the workplace privacy context. 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. Yet, both the majority and concurring Supreme Court opinions in City of Ontario v. Quon suggest that analogies to the private sector are appropriate in evaluating questions of public workplace privacy. Yet scholars in the workplace privacy context have rejected such analogies largely on the ground that they result in a reduction of privacy.

^{*} Title and paper in memory of Dan Markel who allowed me to workshop an earlier version of this paper at Prawfsfest XI, gave me 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. For excellent research assistance I would like to thank Gregory Boden and Zachary Price. For helpful editorial assistance, I would like to thank Caley Turner. Many thanks also to the participants at the 2014 Works-in-Progress Intellectual Property and Prawfsfest XI where I presented earlier versions of this Article.

Neither courts nor scholars, however, have offered any criteria for evaluating when privacy analogies across the public-private divide are appropriate. Courts thus import or reject privacy analogies across the public and private sectors without any meaningful consideration of when such analogies make sense. This Article offers a framework to think about when privacy analogies are appropriate across the public-private divide in cases outside the criminal context. In deciding whether privacy analogies make sense, courts ought to engage in a more nuanced examination of features of the privacy-invading party that traditionally distinguished the government from the private sector such as the presence of coercion, access to superior technology, and the purpose of the privacy invasion.

INTRODUCTION

An airplane flies over an industrial plant that has not yet been completed. There are no barriers to prevent aerial viewing of the plant. Employees at the plant find the airplane suspicious and investigate. They discover that on board that airplane was a photographer who had been hired to photograph the plant on behalf of an unidentified competitor. After the photographer refuses to reveal the identity of the competitor who hired him, the company sues the photographer. 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 even though the company had taken no precautions to protect against aerial surveillance.

An airplane flies over an industrial plant. There are no barriers to prevent aerial viewing of the plant. Employees at the plant have been instructed to investigate any low level flights over the plant. Employees discover that the airplane that flew over the industrial plant belonged to the EPA who had requested and been refused permission to conduct a second on-site inspection of the plant. Instead of obtaining an administrative search warrant, the EPA hired an aerial photographer to take photographs of the facility from above. The company sues the EPA. Applying Fourth Amendment law and its accompanying "reasonable expectation of privacy" standard the Supreme Court held that the EPA had not violated the Fourth Amendment because the company had taken no precautions to protect against aerial surveillance.

These two case-based scenarios illustrate that the American legal system maintains a strict divide between the public and private sectors with regard to privacy law. Courts analyze privacy violations by the government under a Fourth Amendment analysis. Because the Fourth Amendment, however, does not apply to the private sector, courts analyze privacy violations by private actors under a variety of non-constitutional frameworks including, when applicable, state trade secret law. As the two scenarios above demonstrate, this difference can be outcome determinative.

This public-private divide in privacy law plays an important role in the workplace privacy context as well. An employer wants to drug test 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 changes depending on whether the employer is in the private or public sector. Under the existing precedent, public sector employees whose workplace privacy claims are evaluated under a Fourth Amendment framework receive stronger protection than their private sector counterparts.

Despite the clarity of this public-private divide in privacy law, there is considerably less clarity when it comes to analogizing across the public-private divide. In both the trade secret and employment contexts, courts and scholars freely analogize between the private sector privacy frameworks and the Fourth Amendment framework when it suits them to do so, and staunchly defend against such analogies when that is preferable. Very little has been said, however, on how to systemically decide when such analogies are appropriate. At most, the literature seems to favor analogies that result in more privacy, and oppose those that would lessen privacy. This Article seeks to go beyond this results-oriented approach to develop a coherent and consistent normative framework for considering when such privacy analogies are appropriate.

In order to do so, the Article examines the systematic structural differences between the government and private actors, as they relate to the underlying motivations of the Fourth Amendment. What were the features of the government that traditionally necessitated a different degree of privacy protection from the government than from private citizens? What are the motivating principles behind the Fourth Amendment that make

treatment of a very similar fact pattern begin to look extremely different once the government is the actor invading privacy?

There are a number of features that traditionally made invasions of privacy by the government more troubling than similar invasions of privacy by a private actor. Most obviously, the government traditionally had more coercive power than the private sector. Unlike a private citizen, the government could put you in jail. Relatedly, the government had the ability to obtain a warrant if they wanted to invade your privacy, whereas private citizens did not have that power. Furthermore, the government, at least historically, had access to privacy-invading technology that the private sector did not have. Therefore, some scholars contend that the Fourth Amendment protections were a way of levelling the playing field between the government and the public.

There are also features that may in certain circumstances make invasions of privacy by the government less troubling than similar invasions of privacy by the private sector. Most significantly, society may prefer the motivations behind the government's invasions of privacy and see them as socially beneficial, in a way that certain private actor invasions of privacy are not socially beneficial. For example, society may be more sympathetic to the regulatory purposes behind the EPA's invasion of privacy than to the private sector company engaging in industrial espionage.

These traditional differences, however, have begun to break down in a modern world. Once Google has satellite technology, and Amazon has drones, and everyone makes use of big data, does the superior technology justification behind a strict public-private divide in privacy law still always make sense? Or in a context of workplace privacy, do we consider the divide differently if the private sector employer is in the field of big data, such that they may have as much power and information over the employee as the government? Is it obvious that the motivation behind the NSA collecting large amounts of e-mail data is preferable to Google collecting the same data? And then 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 sector and the public sector.

Courts and scholars considering use of a privacy analogy across the public-private divide should systematically and rigorously evaluate these factors to consider the extent to which the traditional markers that justify the public-private divide apply in that context. In doing so they may discover that these differences may caution against analogizing across the two sectors for privacy law purposes in certain situations while support such analogies in other contexts. This may depend on the extent to which the government in that fact pattern contains the features that cause wariness from the government, or the private sector party resembles the government along those features. Admittedly, the factors identified in this Article are not entirely new, and probably only begin to scratch the surface. Many of them already play a role in judicial decision making, or have been identified as important in other contexts. The goal is that identifying these factors will trigger a conversation that could lead privacy analogizing by courts and scholars occurring in a coherent, rather than a haphazard and ad hoc manner. At the end of the day if courts and scholars even articulate why they feel that analogizing across the public-private divide is or is not appropriate in a particular case—more than just saying a public-private divide exists—that would be progress from the status quo.

The Article proceeds in four parts. Part I first identifies the way in which the public-private divide in privacy law plays out in the trade secret context as well as the haphazard way in which courts currently draw or refuse to draw analogies between trade secret and Fourth Amendment cases. Part I then engages in a similar analysis in the workplace privacy context. Finally, Part I points out that scholars have also not yet identified any coherent and consistent normative framework for evaluating when privacy analogies across the public-private divide make sense. Part II explores the structural and other differences between the public and private sectors that traditionally justified the public-private divide in privacy law. This section also identifies the various ways in which these traditional justifications no longer make sense in the modern world. Using the traditional justifications identified in Part II as benchmarks in a multi-factored test. Part III articulates a coherent and consistent normative framework for courts and scholars considering use of a privacy analogy across the public-private divide. The section then illustrates how that framework would work by returning to trade secret law and workplace privacy. Part IV concludes.

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 in the public sector gets filtered into a Fourth Amendment analysis. The Fourth Amendment, however, does not apply to the private sector. 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." Therefore, unlike privacy violations in the public sector, privacy violations that occur in the private sector traditionally do not get analyzed under a Fourth Amendment framework. Consequently the Supreme Court has referred to the private sector as "a domain unguarded by Fourth Amendment constraints." Instead, private sector privacy violations have been filtered into a variety of non-constitutional frameworks including privacy torts, state statutes and state common law such as trade secret law.

A. Trade Secret Law and the Fourth Amendment

This traditional public-private divide in privacy law plays out and is illustrated in the context of trade secret law. In certain factual scenarios, trade secret cases can involve violations of privacy. The Supreme Court has recognized that trade secret law is necessary to protect "a most fundamental right, that of privacy." Elizabeth A. Rowe describes corporate privacy interests as part of the "fundamental nature of trade secret rights." Other scholars have also discussed the link between trade secret law and privacy. ⁵

³ Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 478 (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.").

¹ United States v. Jacobsen, 466 U.S. 109, 113 (1984) (internal quotations omitted).

² Chandler v. Miller, 520 U.S. 305, 323 (1997).

⁴ 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).

⁵ See, e.g., Sharon K. Sandeen, *Relative Privacy: What Privacy Advocates Can Learn From Trade Secret Law*, 2006 MICH. St. L. REV. 667, 670 (2006); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1152 (2000).

Under the Uniform Trade Secrets Act ("UTSA"), which has been adopted by 47 states,⁶ one of the ways in which trade secret misappropriation can occur is when someone acquires a trade secret by "improper means." Although the definition of "improper means" does not explicitly list violations of privacy, some of the possibilities it does list such as theft or espionage can involve violations of privacy. Similarly, the Restatement of Torts finds a trade secret violation can occur when someone discloses or uses a trade secret that was discovered by improper means. 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.

Similarly, although the Fourth Amendment does not actually use the word "privacy," its prohibition against certain searches and seizures necessarily protects against many invasions of privacy by the government — traditionally the police. Although certain scholars contend that the Fourth Amendment should not be viewed primarily through a privacy paradigm, there is little doubt that ever since *Katz* added the "reasonable"

⁶ The UTSA has been adopted by every state except New York, North Carolina and Massachusetts. Texas became the 47th state to adopt the UTSA in May 2013. Massachusetts has introduced a bill to enact the UTSA, which remains pending.

⁷ UNIF. TRADE SECRETS ACT (amended 1985).

⁸ UNIF. TRADE SECRETS ACT (amended 1985).

⁹ 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" RESTATEMENT OF TORTS § 757 (1939).

¹⁰ 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.

¹¹ See Daniel Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. CAL. L. REV. 1083, 1131 (2002).

¹² See, e.g., William J. Stunz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1019 (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, 1777 (1994) (arguing that "the Fourth Amendment should be redefined as promoting 'trust' between the government and the citizenry.").

expectation of privacy" to the Fourth Amendment analysis, that privacy plays a pivotal role in the Fourth Amendment framework.¹³

1. Similar Problems with Different Results

Factually, the trade secret and Fourth Amendment contexts can both involve extremely similar invasions of privacy from the perspective of the corporation whose privacy is being invaded. Nonetheless, as the result of the traditional public-private divide in privacy law, a violation of privacy would necessarily be analyzed under entirely distinct frameworks depending on whether the privacy invasion occurs 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 clear that Fourth Amendment law does not apply to private-sector trade secret cases, and that trade secret law does not apply to public-sector Fourth Amendment cases, there are a number of similarities between the two legal doctrines. For example, 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. Similarly, under the "reasonable expectation of privacy test" in *Katz*, a Fourth Amendment claim turns on what a person exposed to the public. As Daniel Solove explains, the

¹³ Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also* Solove, *supra* note 11, 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).

Zotz v. United States 3

¹⁴ 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 (1978) (observing 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., 2014 WL 2921709 (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).

¹⁵ See, e.g., Boeing Co. v. Sierracin Corp., 738 P.2d 665, 674 (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).

"Court's new conception of privacy is one of total secrecy." As a result, "one could not have a reasonable expectation of privacy in information that was not kept secret." Thus secrecy has become a necessary component of both the trade secret and Fourth Amendment analyses.

Despite these factual and doctrinal similarities, however, there are sufficient differences between the trade secret and Fourth Amendment frameworks, such that the application of one of the two frameworks can be outcome determinative for the case. This outcome determinative disparity that can result from application of the two different frameworks is best illustrated by two factually similar cases involving aerial photography.

In DuPont, the Fifth Circuit analyzed a trade secret case involving aerial photography of an industrial plant. 18 The case arose out of Texas where an unknown third party, presumably one of DuPont's competitors, hired the defendants, Rolfe and Gary Christopher to take aerial photographs of a DuPont plant while it was still under construction. 19 DuPont built the plant in order to facilitate the production of methanol by means of a "highly secret but unpatented process."²⁰ The Christophers flew in an airplane over the unfinished plant and took sixteen photographs that were developed and delivered to the unknown third party. 21 DuPont employees noticed the aircraft flying over the plant and immediately launched an investigation by which they discovered that the Christophers had taken aerial photographs while circling the plant in their aircraft.²² Despite DuPont's efforts, the Christophers refused to disclose who had hired them, or to return the photographs without delivery.²³ DuPont filed suit alleging trade secret violation, and after the Christophers refused to disclose the third party who had hired them during their depositions, the district court granted a motion

¹⁶ Solove, *supra* note 11, at 1133.

¹⁸ 431 F.2d 1012 (5th Cir. 1970).

¹⁹ *Id.* at 1013. ²⁰ *Id.*

²¹ *Id*.

²² *Id*. ²³ *Id*.

to compel an answer.²⁴ The Christophers sought an interlocutory appeal on whether DuPont had stated a claim.²⁵

The Fifth Circuit first analyzed whether a lawful action could be considered misappropriation under the applicable Texas trade secret laws. ²⁶ 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." ²⁷ Applying the Restatement of Torts' definition of a trade secret, which the Texas Supreme Court had adopted at the time, ²⁸ the court found that illegal conduct was not necessary for misappropriation, and that the invasion of privacy that occurred from the aerial photography sufficed. ²⁹

The Christophers argued that DuPont did not take reasonable precautions because it failed to cover the facility during the construction and thus allowed the facility to be viewed from the air. The court rejected that argument, however, holding that it would be unfair to allow espionage "when the protections required to prevent another's spying cost so much that the spirit of inventiveness is dampened." 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." 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"

²⁴ *Id.* at 1014.

²⁵ *Id*.

²⁶ *Id*.

²⁷ *Id*.

²⁸ Texas has since adopted the Uniform Trade Secret Act

²⁹ 431 F.2d at 1014. 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" RESTATEMENT OF TORTS § 757 (1939).

³⁰ 431 F.2d at 1016.

³¹ *Id*.

³² *Id*.

more than a school boy's trick."33 According to the court, requiring DuPont to create an "impenetrable fortress" would be an unreasonable requirement.³⁴ 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.³⁵

Fourteen years later, the Supreme Court analyzed a case with very similar facts, except that this time it was the government who violated a corporation's privacy by means of aerial photography. 36 Unlike *DuPont*, however, where the Fifth Circuit had held that aerial photographs taken of a plant could sustain a cause of action for trade secret violation, in *Dow*, the Court rejected a contention that aerial photographs taken of a plant violated the Fourth Amendment. 37 Dow Chemicals operated a 2,000 acre facility in Michigan that consisted of numerous covered buildings with equipment and piping conduits exposed between the buildings.³⁸ Dow had "elaborate security" around the complex that prevented public observation from the ground level.³⁹ Also, Dow instructed its employees to investigate any low level flights over the facility. 40 Dow did not, however, construct any barriers to prevent aerial viewing.⁴¹

In 1978, the EPA conducted an on-site inspection of two power plants located on the premises with the consent of Dow. 42 The EPA requested a second inspection, which Dow rejected. 43 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 "from altitudes of 12,000, 3,000, and 1,200 feet." During the

³³ *Id*.

³⁴ *Id.* at 1017.

³⁵ 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.

³⁶ Dow Chem. Co. v. United States, 476 U.S. 227 (1986).

³⁷ *Id.* at 239.

³⁸ *Id.* at 229.

³⁹ *Id*.

⁴⁰ *Id*.

⁴¹ *Id*.

⁴² *Id*.

⁴³ *Id*.

flight, the plane was lawfully within navigable airspace. ⁴⁵ Dow was not informed of the EPA's actions, but filed for injunctive and declaratory relief upon learning of the aerial surveillance alleging in part that the EPA violated the Fourth Amendment. ⁴⁶

The Supreme Court held that the complex was not analogous to the curtilage of a dwelling and the photographs were not a search prohibited by the Fourth Amendment. Because Dow had "elaborately secured" its complex, the Court found that the space between the buildings fell somewhere between both doctrines. But 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. The difference here was that the aerial observation did not involve a physical entry. Because it was observable to the public, a government regulatory inspector should not need a warrant.

Therefore, while both cases involved very similar facts with both involving aerial photographs of industrial plants, the Supreme Court and Fifth Circuit come out differently based largely on the different legal frameworks triggered by the public-private divide regarding who had hired the photographers. These cases illustrate both the similar sorts of privacy violations that can occur, but also the differences in result based on the different legal frameworks.

2. Privacy Analogies

Despite the clarity that the Fourth Amendment framework does not apply to private-sector trade secret cases, and the trade secret framework does not apply to Fourth Amendment cases, in light of the possibility for similar facts as well as the similarities between the two legal frameworks, courts, legal advocates and scholars may consider whether it is appropriate to analogize across the public-private divide. In other words, when (if ever) should a court consider a Fourth Amendment case persuasive authority for a

⁴⁵ *Id*.

⁴⁶ *Id*.

⁴⁷ s*Id*. at 239.

⁴⁸ *Id.* at 236–37.

⁴⁹ *Id.* at 237–38 (quoting Donovan v. Dewey, 452 U.S. 594, 598–99 (1981)).

⁵⁰ 476 U.S. at 237.

⁵¹ *Id.* at 238 (citing Marshall v. Barlow's, Inc. 436 U.S. 307, 315 (1978)).

trade secret case, and vice versa? Currently, courts lack any clarity or guidance for when such analogizing is appropriate and do not have any framework for evaluating when such an analogy makes sense.

Some courts analyzing trade secret cases have analogized to relevant cases in the Fourth Amendment context in spite of the supposed rigid divide between the treatment of private and public cases in the privacy context. For example, in Tennant Co. v. Advance Machine Co., the Minnesota Appeals Court seemed to find it entirely appropriate to analogize to the Fourth Amendment context in deciding a trade secret case that involved the privacy of trash.⁵² Tennant involved business competitors Tennant and Advance who both manufactured and marketed floor cleaning equipment.⁵³ For two years, Advance employees went through dumpsters behind Tennant's sales offices in California, which had been disposed of in sealed trash bags, and put in a covered dumpster only used by Tennant.⁵⁴ The dumpster diving scheme had been conceived by Advance sales representative McIntosh, who used the information he gained to send memos to Advance's Vice President of Sales, in which he summarized the information contained in the stolen documents.

The Minnesota Appeals Court considered a misappropriation of trade secrets claim under the California Unfair Practices Act. 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."55 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."

In reaching that conclusion the court appeared to be influenced by its discussion earlier in the decision on how the case would have been resolved under Fourth Amendment law. The court noted that the law in California was settled that "an owner retains a reasonable expectation of

⁵² See, e.g. Tennant Co. v. Advance Mach. Co., 355 N.W.2d 720 (Minn. Ct. App. 1984). ⁵³ *Id.* at 722.

⁵⁴ *Id*.

⁵⁵ *Id.* at 725.

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." The court found "no reason" to apply a different standard in a civil case. According to the Minnesota court, 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."

Of course subsequent to the *Tennant* decision, the U.S. Supreme Court held that there is no reasonable expectation of privacy in trash put out for collection under Fourth Amendment law. ⁵⁹ But the key point raised by *Tennant* is not whether or not dumpster diving is acceptable, but whether in evaluating a dumpster diving case in the trade secret context courts should be analogizing to applicable Fourth Amendment cases. The *Tennant* court strongly suggested that such analogizing was appropriate.

A second court looking at a dumpster diving case agreed that Fourth Amendment analogies are appropriate, but it updated its analogy to reflect the updated Fourth Amendment law regarding dumpster diving. In *Frank W. Winne & Son, Inc. v. Palmer*. ⁶⁰ Winne and Son, Inc. and Twi-Ro-Pa Mills Agency, Inc. manufactured and sold rope. ⁶¹ Palmer, president of Twi-Ro-Pa, instructed an employee to collect the trash that Winne put out and forward the office documents to him. ⁶² The documents he 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. ⁶³ Upon learning of the theft, Winne filed suit alleging trade secret violations and tortious interference with contractual relationships with customers. ⁶⁴ After addressing what improper means would be, the court analyzed whether Winne had taken adequate protections

⁵⁶ *Id.* (quoting People v. Krivda, 486 P.2d 1262, 1268 (Cal. 1971)).

⁵⁷ 355 N.W.2d at 725.

⁵⁸ *Id*.

⁵⁹ See California v. Greenwood, 486 U.S. 35, 39-40 (1988).

⁶⁰ Civ-A 91-2239, 1991 WL 155819 (E.D. Pa. Aug. 7, 1991).

⁶¹ *Id.* at *1.

⁶² *Id*.

⁶³ *Id*.

⁶⁴ *Id*.

to protect the trade secret because failure to do so would preclude recovery even if the defendant used improper means. ⁶⁵

In undertaking its analysis, the 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 that were left in the trash. 66 The Pennsylvania court discussed the various Fourth Amendment cases, including the Supreme Court's decision in Greenwood holding that there is no reasonable expectation of privacy in trash that has been placed for collection. The court then explained that it found the reasoning in those Fourth Amendment cases to be persuasive, thus demonstrating its belief that Fourth Amendment cases can be persuasive authority in a trade secret private sector case. The Winne court recognized that the Fourth Amendment cases were "not commercial trade secret cases," but 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 of law, he has no reasonable expectation of privacy from prying eyes."67 This language suggests that the court felt that Fourth Amendment law could set the floor for whether there were adequate precautions taken.

Unlike the Pennsylvania court in *Winne* who approved of and used Fourth Amendment analogies, a California Court of Appeal criticized the use of Fourth Amendment 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." 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. ⁶⁹

⁶⁵ *Id.* at *3.

⁶⁶ *Id.* at *4.

⁶⁷ *Id*.

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.

⁶⁹ Ananda Church of Self-Realization v. Massachusetts Bay Ins. Co., 2002-2003 CCH INS.

Whereas some courts have analogized to the Fourth Amendment context in trade secret cases, the Supreme Court has rejected analogizing to the trade secret context in a Fourth Amendment case. In *Dow Chemical Co*, the Supreme Court undoubtedly recognized the factual similarities between the case before them involving a Fourth Amendment claim for the EPA's aerial photography, and the Fifth Circuit precedent in *DuPont* holding that aerial photography of an industrial plant could constitute a misappropriation of a trade secret violation. The *DuPont* case certainly had enough factual similarity that it might have served as persuasive authority to the Court in considering the Fourth Amendment questions at issue. 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 viewed from the air, and whether failure to do so meant that the company had not taken sufficient steps to protect its privacy.

Instead of considering whether the *DuPont* case might at least be persuasive authority, the court stated that the trade secret analogy was "irrelevant to the questions presented" because state tort law "does not define the limits of the Fourth Amendment." In support for this claim that state tort law "does not define the limits of the Fourth Amendment," the Supreme Court cited *Oliver v. United States*, ⁷¹ and noted in its parenthetical that *Oliver* stood 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 a significant one. The former formulation merely suggests that state tort law is not binding when it comes to Fourth Amendment limits, or in other words there is a public-private divide in privacy law. The latter formulation, with its claim to irrelevance, rejects not only the binding

LAW REP. §7397 (Cal. App. 3d 2002) (discussing in the context of a civil conversion claim).

⁷⁰ Dow Chem. Co. v. United States, 476 U.S. 227, 232 (citing Oliver v. United States, 466 U.S. 170 (1984) (trespass law does not necessarily define limits of the Fourth Amendment). The Court used the above parenthetical in its citation. While the Court is arguing that state law has no bearing on Fourth Amendment jurisprudence, it simultaneously points that it "does not necessarily define the limits," which implies tort or property law may set a boundary on Fourth Amendment jurisprudence.

effect of state tort law, but also any persuasive impact of state tort law or any efforts to analogize across the public-private divide. 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. 73

The dissent in *Dow* by Justices Powell, Brennan, Marshall and Blackmun, disagreed with the majority's thorough dismissal of the relevance of the trade secret analogy. The partial dissent points out that previous decisions have 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." Therefore, laws protecting trade secrets can be relevant, i.e. persuasive, in demonstrating society's expression of what constitutes a reasonable expectation of privacy.

To summarize, certain trade secret cases analogize to the Fourth Amendment precedent for assistance in determining whether there were adequate precautions to protect a trade secret and whether a defendant utilized improper means. Nonetheless, the Supreme Court firmly rejected analogizing in the opposite direction and refused to consider trade secret case precedent in considering a Fourth Amendment case. These different analyses lead to an interesting split in protection from corporate competitors and government agents. When that Fourth Amendment expectation is violated in a trade secret context, then courts engaging in the Fourth Amendment analogy are likely to find that the trade secret was acquired

⁷² Sam Kamin describes *Dow* 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 *Dow*. Nothing in *Dow* 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." *See also* Florida v. Riley, 488 U.S. 445, 60 n.3 (1989) (Brennan, J., dissenting) (describing the decision in *Dow* as the Court having "declined to consider trade-secret laws indicative of a reasonable expectation of privacy.").

⁷³ 476 U.S. at 231.

⁷⁴ *Id.* at 248 (Powell, J., concurring in part and dissenting in part) (quoting Rakas v. Illinois, 439 U.S. 128, 143–144 n.12 (1978)).

under improper means within the trade secret doctrine.⁷⁵ Courts have consistently dismissed efforts to analogize in the opposite direction, however, and have refused to consider whether a suspect would have taken reasonable efforts to secure privacy of his actions under trade secret law in the context of evaluating Fourth Amendment cases.

B. Workplace Privacy: Privacy Torts and the Fourth Amendment

[Omitted for purposes of IPSC as it goes through a similar analysis as above in the context of workplace privacy. Bottom line is that unlike with trade secret law the Supreme Court has expressly permitted analogies to the private sector in Fourth Amendment workplace privacy cases.]

C. Lacking a Normative Framework for Privacy Analogies

[Omitted for purposes of IPSC, as most of the existing scholarly literature is on the side of workplace privacy. Bottom line is that the literature largely supports privacy analogies when they increase privacy, but not when they reduce privacy. This is results oriented, and not a coherent and consistent methodology

- Sam Kamin, *The Private is Public: The Relevance of Private Actors in Defining the Fourth Amendment*, 46 B.C.L. Rev. 83 (2004)
 - Noting that state governments 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."
 - o "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."
- But see Adam Shinar, Public Employee Speech and the Privatization of the First Amendment, 46 Conn. L. Rev. 1 (2013)
 - o He <u>has</u> offered a normative articulation of the public-private divide in the context of the First Amendment.

]			
75 See id			

II. RECONSIDERING THE PUBLIC-PRIVATE DIVIDE IN PRIVACY LAW

This section identifies and explores the possible justifications behind the traditional strict divide between the treatment of privacy violations that occur in the public and private sectors. It begins by identifying various institutional features that may have justified historically 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 manifest in the private sector in the modern world. Finally, it points down the practical ways in which the public-private divide has broken down as a result of increasing transfers of information across the public-private divide.

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

The state action doctrine ⁷⁶ that exists throughout constitutional law, in which the Constitution generally applies to state action but not private action, is based on an insight that there is something necessarily and categorically different about the government. ⁷⁷ Similarly, as a specific manifestation of the state action doctrine as it is applied to the Fourth Amendment, the public-private divide in privacy law is based on a perception that there is something necessarily and categorically different about privacy violations when they occur by the government, as opposed to those that occur by the private sector. ⁷⁸

Mumarous

Numerous scholars have criticized the state action doctrine. *See, e.g.,* Erwin Chemerinsky, *Rethinking State Action,* 80 Nw. U.L. Rev. 503, 504 (1985) ("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). Cite to more. 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.

⁷⁷ C.f. Adam Shinar, *Public Employee Speech and the Privatization of the First Amendment*, 46 CONN. L. REV. 1, 37 (2013) (noting in the first amendment context that the state action doctrine "rides on the intuition that there is something special about government.")

government.")
⁷⁸ 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 generally* Solove, *supra* note 11, at 1133 (describing the transfer of personal information from the private sector to the government in light of the harms of the government having that information).

There are at least four features that traditionally distinguishes the government from a private actor that could justify treating the public sector differently than the private sector with regard to invasions of privacy. First, the government has powers of coercion that did not traditionally occur in the private sector. Second, governmental invasions of privacy can harm individual self-determination as well as democracy. Third, the government's bureaucratic nature can lead to various harms. Finally, the government historically had access to more sophisticated technology than society at large.

1. Government Has Unique Power of Coercion

First, and perhaps most significantly the government traditionally has power that in various ways exceeds the power of the private sector. This 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 entirely take away an individual's liberty by placing them in jail, or to disrupt their lives and homes by searching them indiscriminately. As Adam Shinar points out in the First Amendment context, the government "is often the only source of legitimate violence", and its status as provider of public goods requires an element of coercion and authority that is not found in the market."⁷⁹

There is some historical support for this government power-based justification for the public-private divide. Morgan Cloud has 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. Thomas Clancy argues that a 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."

Many scholars have contended that the Fourth Amendment should best be seen as protecting individuals from government power and coercion.

.

⁷⁹ Shinar, *supra* note 77, at 39.

⁸⁰ See Morgan Cloud, Pragmatism, Positivism, and Principles in Fourth Amendment Theory, 41 UCLA L. REV. 199, 296-97 (1993).

⁸¹ Thomas K. Clancy, What Does the Fourth Amendment Protect: Property, Privacy, or Security? 33 Wake Forest L. Rev. 307, 351 (1998).

For example, Paul Ohm has argued that "[p]ower seems to be the amendment's essence, not merely a proxy for something deeper." Similarly, Bill Stuntz contended that the Fourth Amendment should focus on coercion and violence. 83

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 *Nineteen Eighty-Four*. ⁸⁴ According to Daniel Solove, the Big Brother metaphor remains persuasive as one of the dangers of unfettered government access to information. ⁸⁵ A totalitarian government presents a source of fear due to its ability to achieve total domination by monitoring every facet of its citizens' private lives. ⁸⁶ 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 extent to which the government can exercise social control."

Part of the source of the government's power is the extent to which the government has a monopoly in various ways. As Shinar points out, the government "is often the sole source of a particular service," so there is no ability to opt out. ⁸⁸ Many of the government's services, such as the criminal and civil justice systems, national defense, police, were at least traditionally public goods for which the government had a monopoly. ⁸⁹ This is exacerbated by the fact that moving to a different country (or state) is challenging or sometimes impossible ⁹⁰

⁸² Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L. REV. 1309, 1338 (2012).

⁸³ William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 446 (1995).

⁸⁴ See generally, George Orwell, Nineteen Eighty-Four (1949).

⁸⁵ *See* Solove, *supra* note 11, at 1101-02.

⁸⁶ *Id.* at 1101.

⁸⁷ *Id.* at 1102.

⁸⁸ Shinar, supra note 77, at 39.

⁸⁹ Id.

⁹⁰ *Id*. at 40.

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

A second possible justification for traditionally treating government invasions of privacy as different in kind from private sector invasions of privacy is that government privacy invasions can harm individual identity formulation as well as inhibit individuals from engaging in democratic activities. As Solove explains, "government information-gathering can severely constrain . . . individual self-determination." According to Solove, this harm can occur unintentionally; "even if government entities are not attempting to engage in social control" by virtue of engaging in invasions of privacy government activities can harm self-determination. Similarly, Paul Schwartz contends that excessive government invasions of privacy regarding an individual's activities can "corrupt individual decision making about the elements of one's identity."

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." As a result, the Court has limited the government's power to compel disclosure of group membership, 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." ⁹⁵

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. Paul Schwartz argues that inadequate protection of privacy can inhibit people from engaging in democratic activities. Shinar explains that "because of their dependence on elected officials for resources and funding, government

⁹¹ See Solove, supra note 11, at 1101-02.

⁹² Solove, *supra* note 11, at 1102.

⁹³ Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1657 (1999).

⁹⁴ NAACP v. Alabama, 357 U.S. 449, 462 (1958).

⁹⁵ Baird v. State Bar, 401 U.S. 1 (1971).

institutions, unlike private firms, are more vulnerable to the risk of being used for improper political purposes." ⁹⁶

3. Government Is Too Bureaucratic

A third reason justifying the traditional public-private divide in privacy law, is that government invasions of privacy are subject to the harms that routinely arise in bureaucratic settings. ⁹⁷ According to Solove, these bureaucratic harms include decision making 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. ⁹⁸

To be clear, this justification is less rooted in originalism, as at the time of the Fourth Amendment, there were no organized police forces. ⁹⁹ Rather it is a modern justification for the traditional divide. In today's modern world law enforcement has become bureaucratized. ¹⁰⁰ 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. ¹⁰¹

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." ¹⁰²

⁹⁶ Shinar, *supra* note 77, at 40.

⁹⁷See Solove, supra note 11, at 1104.

⁹⁸ *Id*.

⁹⁹ See Silas J. Wasserstrom & Louis Michael Weidman, The Fourth Amendment as Constitutional Theory, 77 GEO. L.J. 19, 82 (1988).

¹⁰⁰ Solove, *supra* note 11, at 1106.

¹⁰¹*Id*.

Shinar, *supra* note 77, at 40.

4. Government Has Access to Superior Technology

A Fourth justification that might distinguish the government invasions of privacy from similar invasions by the private sector is the government's historic superiority with regard to technology. The Supreme Court has suggested that this is part of the justification. In *Dow* the Court stated in dicta 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." The Court followed similar logic in *Kyllo v. United States*, with its rule that the government violates the Fourth Amendment when it uses technology that is "not in general use" to see "details of the home that would previously have been unknowable without physical intrusion." 104

Various scholars have pointed out the importance of technology 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. ¹⁰⁵ In other words, under Kerr's "equilibrium-adjustment" theory courts implementing the Fourth Amendment strive to protect a technologically level playing field. ¹⁰⁶ Similarly, Paul Ohm modifies Kerr's theory and 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." ¹⁰⁷ For Ohm this ratio can be determined by examining the metrics of crime fighting such as how long do investigations take. ¹⁰⁸

¹⁰³ Dow Chem. Co. v. United States, 476 U.S. 227 (1986).

¹⁰⁴ 533 U.S. 27, 40 (2001).

¹⁰⁵ Orin Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment, 125 HARV. L. REV. 476 (2011).

¹⁰⁶ *Id*. at 480.

¹⁰⁷ Ohm, *supra* note 82, at 1346.

¹⁰⁸ *Id*.

B. Reconsidering the Justifications for the Public-Private Divide

Thus far this section 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 features that at least traditionally distinguished the government. This next part seeks to reconsider those features, and to point out that in the modern world it is not always obvious that those features belong uniquely to the government. Rather, this Section will demonstrate that in today's society ¹⁰⁹ these dangers are equally possible in the private sector. To be clear, the purpose of this section is not to argue that the government and the private sector are identical, or that the state action doctrine should be abolished. Rather, by pointing out that at times the private sector has many of the features that traditionally distinguished government, this sets up the argument in the final section that courts should look for the presence of these features in deciding whether an analogy across the public-private divide is appropriate.

1. Private Sector Can Also Have Power of Coercion

The first feature considered in defense of the public-private divide is that the government traditionally has had power than exceeds the power of the private sector.

i. Private sector police power?

See Elizabeth E. Joh, *The Paradox of Private Policing*, 95 J. Crim. L & Crimonology 49 (2004).

- Prevalence and increasing authority of private policing groups such as security guards, warrants application of Fourth Amendment protections to situations where security guards arrest/detail individuals.
- Points out security guards in Disneyland Parks p. 52-53

25

¹⁰⁹ 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.

- Still are differences of course- can't actually send you to jail/ arrest you, etc. This is a legitimate difference that may warrant against applying the Fourth Amendment itself, but may permit analogies.

See David A. Sklansky, *The Private Police*, 46 UCLA L. Rev. 1165, 1177 (1999) (discussing practice in which government agencies hire private security companies to perform work previously carried out by law enforcement officers.")

- I argue that this is unlikely to happen, but no reason in considering a private sector privacy violation claim, that courts in this circumstance should not analogize strongly to similar cases in the Fourth Amendment context.
- ii. Other forms of coercion- economic coercion?
 - 2. Private Sector Actions Can Also Harm Individual Identity Formulation and Democracy

See sociologist Amitai Etzioni, *The Privacy Merchants: What is to be Done?* 14 U. Pa. J. Const. L. 929, 934 (2012) (noting that the violation of privacy by private agents has some similar effects to violations committed by government agents—effects that lead to discrimination and chilling of expression and dissent."

Examples he gives:

- Gays who are outed by the media
- Banks call in loans of those they find out have cancer
- Employers refuse to hire people because of political or religious views.

- 3. Private Sector Can Be Extremely Bureaucratic
- The dangers that Solove identifies from bureaucratic settings: "decisions without adequate accountability, dangerous pockets of unfettered discretion, and choices based on short-term goals without consideration of the long-term consequences of the larger social effects" are all problems that occur with corporations as well. Common criticisms of corporations, especially consideration of short-term goals
- As Solove himself points out even in the private sector information is 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."
 - 4. Private Sector Has Unprecedented Access to Technology That Once Used to be Solely for Government
- Google has satellite technology
- Amazon drones
- Everyone has access to big data
- Biometric technology
- GPS tracking
 - C. Practical Breakdowns in the Public-Private Divide
- Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 Minn. L. Rev. 1 (2008)
 - P4: "much of the surveillance in the National Surveillance State will be conducted and analyzed by private parties."
 - o P7: "the line between public and private modes of surveillance and security has blurred if not vanished. Public and private enterprises are thoroughly intertwined."
 - o P8: "Government and businesses are increasingly partners in surveillance, data mining, and information analysis."
 - o P20: private parties "can freely collect, collate, and sell personal information back to the government free of Fourth

- Amendment restrictions, effectively allowing an end-run around the Constitution."
- Amitai Etzioni, *The Privacy Merchants: What is to be Done?*, 14 U. Pa. J. Const. L. 929 (2012)
 - P. 951: "one must assume that what is private is also public in two sense 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.)
- Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1103 (2002)
 - "the government's extensive ability to glean information about one's associations from third party records without any Fourth Amendment limitations seems to present an end-run around [Fourth Amendment] principles")
 - o "government is increasingly contracting with private sector entities to acquire databases of personal information."
 - o "All of this suggests that businesses and government have become allies." P. 1101
- Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 Miss. L. Rev. 1309 (2012)
 - o 1320-21: "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."
- S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 Ga. L. Rev. 825, 826 (1998)

III. NORMATIVE FRAMEWORK FOR PRIVACY ANALOGIES

This paper considers a modest proposal in order to overcome the public-private divide that would not require extremely difficult legislative intervention. It suggests that in deciding whether to analogize across the public-private divide and treat cases across the divide as persuasive, courts should consider the extent to which the cases are similar with regard to the traditional markers that distinguished government invasions of privacy. This multi-factored analysis should then inform the currently haphazard decision of whether the analogy is appropriate.

The question that is being asked is merely whether it is appropriate for a court in the Fourth Amendment case to consider the fact that in the private sector a state has protected the defendant against precisely the sort of privacy invasion the government committed. 110

- A. Applying the Normative Framework to Trade Secret Analogies
- B. Applying the Normative Framework to Workplace Privacy Analogies

¹¹⁰ C.f. Shima Baradaran, Rebalancing the Fourth Amendment, 102 GEO. L.J. 1 (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).