ARTICLE

CURING ADMINISTRATIVE SEARCH DECAY

G.S. HANS[1]

The entry of technology companies like Uber and Airbnb into highly regulated markets such as transportation and housing means that more data on individuals than ever is being transferred from private companies to the government, under the guise of regulatory oversight. The administrative search doctrine — an exception to the Fourth Amendment warrant requirement that allows for warrantless searches for regulatory purposes — would appear at first glance to support these requests.

However, this Article argues that regulatory searches that collect data from companies are radically different in scope than historical administrative searches. These searches can collect much more sensitive data about individuals than ever before, including detailed location data, financial information, and personally identifiable information. Regulatory requirements that fall under the administrative search doctrine can easily be overbroad, allowing for collection without meaningful limitations and few restrictions on subsequent uses. Without substantial reform, the current administrative search doctrine makes little sense in the modern era.

In Part I, the Article analyzes the historical justifications for regulatory searches and describes why they are insufficiently specific for the modern era. It explores how the administrative search doctrine has evolved to allow for more expansive searches, and how the third party doctrine means that only businesses can assert the rights over the data collected by the government, even if that data concerns information about individuals. The risks of over-collection, data

[1] Clinical Fellow, University of Michigan Law School. I am grateful to Victoria Baranetsky, Eve Brensike Primus, Matt Cagle, Ryan Calo, Musetta Durkee, Susan Freiwald, Sue Glueck, Dustin Marlan, Aaron Melaas, David Moran, Paul Ohm, and Meg Young for helpful suggestions and commentary, and to participants at the University of Washington School of Law Faculty Colloquium, the University of Idaho College of Law Faculty Seminar, and the Privacy Law Scholars Conference. I have worked with some of the companies discussed in this Article, including Uber and Airbnb. I have not been compensated by any companies, and they have not reviewed any section of this Article. All errors remain my own.

breaches, and improper users are significant. Part II discusses existing critiques and proposes a modification to the administrative search doctrine, using a narrow tailoring principle, but also notes the challenges and shortcomings to a legal solution.

Part III closes by offering a policy solution using a model based on the Fair Information Practice Principles (FIPPs). This model provides better clarity to the administrative search doctrine promulgated by the courts, allowing for more effective balancing of regulatory interests alongside the privacy rights of individuals. The sensitivity of our data means that the current system cannot endure any longer.

INTRODUCTION

In 2014, the release of a dataset from the New York Taxi and Limousine Commission (TLC) triggered a chain reaction that ultimately allowed for the re-identification of individual riders and the trips these riders took.[2] The dataset was initially released pursuant to a New York State Freedom of Information Law request, and the TLC had attempted to de-identify some of the sensitive data contained within the set — including the medallion number and the hack license number, which individually identify the car and the driver respectively.[3]

However, the TLC did not do a sufficiently robust job in de-identifying the dataset. First, a computer scientist was able to reverse the cryptographic hashing, re-identifying the entire set.[4] Then, a graduate student used publicly available information — photographs of celebrities, complete with medallion numbers — to track individual trips that the celebrities took.[5] Each step built on the last, leading to individuals' private movements being tracked without their knowledge or permission. All this from a simple open data request that contained information pertaining to individuals.

While incidents like these trouble privacy advocates and civil libertarians, they may not capture the attention of lawmakers, the courts, or even the public itself. This is a problem. Too much individual data is being collected, stored, and sometimes disclosed without anyone asking or answering some very important questions. To what degree does it matter that government agencies collect data that raises privacy concerns? If there is a legal or policy issue, does the problem stem from the initial data collection, the challenges of effective de-identification, the increased digitization of American life, the public disclosure

2 J.K. Trotter, *Public NYC Taxicab Database Lets You See How Celebrities Tip*, GAWKER (Oct. 23, 2014, 12:00 PM), http://gawker.com/the-public-nyc-taxicab-database-that-accidentally-track-1646724546 [https://perma.cc/58TP-7QEB].

3 *Id.*

4 Vijay Pandurangan, On Taxis and Rainbows, MEDIUM (June 21, 2014), https://tech.vijayp.ca/of-taxis-and-rainbows-f6bc289679a1 [https://perma.cc/U7JM-URKV].

5 Trotter, *supra* note 2.

of that data, or some combination thereof? Who is, and who should be, protecting individuals from re-identification and what redress, if any, is available? This Article focuses on the role of regulatory agencies in the collection of user data from private businesses. It argues that the government should not be able to so easily collect sensitive information without a warrant, active oversight, or robust limitations.

The issues surrounding data collection and privacy in a digital economy are well-worn topics, and the struggles of engaging a population inured to corporate and government surveillance persist for scholars, policymakers, and activists.[6] But in the context of regulatory searches of businesses, getting the population to care may be a particular challenge. Regulatory agencies are mysterious to the average citizen (if they even think about them at all); businesses have to collect information in order to function, and consumers readily trade their personal information for free services. Some may even accept the possibility of re-identification as the cost of convenience for inexpensive, or even free, services in the digital age. It's unclear, however, whether individuals would so eagerly make such concessions if it were the government, and not private businesses, getting access to their personal data. To the degree the drafters of the Bill of Rights cared about the government's intrusion into individuals and their records, we too should have concerns about these practices.

The Fourth Amendment protects individuals from precisely these intrusions, and its ban on warrantless searches and seizures would *seem* to prevent the government's collection of this data from private entities. However, the Supreme Court's Fourth Amendment jurisprudence has allowed for several exceptions to the warrant requirement, including for so-called "administrative searches."[7] First formulated a half-century ago,[8] the administrative search doctrine has effectively allowed for broad searches of Americans in a variety of contexts, including schools, businesses, government employees, and national security.[9]

The justifications for administrative searches are compelling. The state has a responsibility to protect citizens, and one of its methods for doing so is to ensure compliance with laws and regulations through inspections. The administrative

---

[6] *See, e.g.*, NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE (Dave McBride ed., Oxford Univ. Press 2015) (arguing for a concept of "intellectual privacy" to protect individuals in a technological age); DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (Michael O'Malley ed., 2011) (arguing for a better protection of privacy interests in the law's privacy-security debate).

[7] *See, e.g.*, Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 255-57 (2011).

[8] Camara v. Mun. Court, 387 U.S. 523, 534 (1967).

[9] Primus, *supra* note 7, at 255-56.

search exception permits government officials to perform this duty without having to seek warrants for every inspection of business records or premises, increasing efficiency and allowing the government to promote regulatory compliance, consumer protection, and public safety.

However, the balance of government needs against individual privacy at the foundation of the administrative search doctrine has been a point of contention since its origins. This issue has become more trenchant as technology has dramatically changed the volume and detail of personal data being collected and stored in the course of everyday business. The records potentially covered under the administrative search doctrine are more robust than ever. What, then, should be the bounds of the doctrine, especially given how administrative searches increasingly touch not only on business regulation, but also upon consumers' personal data?

This Article proceeds in three parts. Part I explores the evolution of the administrative search exception and how its intersection with the third party doctrine has exacerbated the problems of current searches, and describes the issues with current administrative searches in a digital age. Part II describes the importance of re-evaluating the doctrine through scholarly criticisms, sets forth a solution by returning to its initial formulation (with an additional narrow tailoring requirement), and describes the challenges to such reforms. Finally, Part III sets out how alternative methods of governance could realize the goal of administrative search reform in the absence of judicial modification.

I. THE EVOLUTION OF ADMINISTRATIVE SEARCHES AND ITS INTERSECTION WITH THE THIRD PARTY DOCTRINE

Under the Fourth Amendment, the government is prevented from conducting searches and seizures that require a warrant absent probable cause.[10] Supreme Court jurisprudence has allowed for multiple exceptions to this requirement; the administrative search is one of them.[11] The most recent Supreme Court case to address the administrative search doctrine, *City of Los Angeles v. Patel,* described the searches as a type of special needs search,[12] different from the general governmental interest in crime control.[13]

The administrative search doctrine has a history dating back a half-century,

[10] *See* U.S. CONST. amend. IV.

[11] *See* City of Los Angeles v. Patel, 135 S. Ct. 2443, 2452 (2015).

[12] Special needs searches were first articulated in *New Jersey v. T.L.O.*, 469 U.S. 325 (1985), which created a test allowing for searches outside of the "normal need for law enforcement." *Id.* at 351. To the extent that administrative searches are considered law enforcement — though generally on the civil, rather than criminal, side — they can be considered a related, though similar, doctrine.

[13] Patel, 135 S. Ct. at 2452.

originating in the Warren Court's 1967 decisions in *Camara v. Mun. Court*[14] and *See v. City of Seattle*.[15] These decisions created an exception to the standard Fourth Amendment doctrines governing procedures surrounding governmental searches and seizures, which the Court has continued to modify through subsequent decades.

In practice, there are multiple issues with the current administrative search doctrine that stem from its muddled evolution over the last fifty years. The dynamics at play in *Patel* demonstrate some of these issues.

A. Origins: Frank, Camara, and See

As discussed *supra*, the Supreme Court first formulated the administrative search doctrine in two cases: *Camara v. Mun. Court* and *See v. City of Seattle*. This was a departure from a case decided a decade earlier, *Frank v. Maryland*.[16] In *Frank*, a Maryland public health official attempted to inspect a house owned by Frank for rats, and did not have a warrant to do so (which was permissible under the Baltimore City Code).[17] Frank argued that such a search violated his Fourth Amendment rights.[18] The Court disagreed, arguing that because the inspection power was limited and caused only a slight restriction on privacy — a restriction that was outweighed by the need for the inspection and its non-criminal application.[19] Ultimately, the Court rested its approval of the inspection scheme on the historical basis for such searches, contemporary needs, and its narrow tailoring.[20]

Frank was explicitly overruled in *Camara*, which took a much more skeptical view towards such searches.[21] *Camara* concerned a San Francisco municipal ordinance allowing for inspections of buildings to determine compliance with the city's Housing Code.[22] On multiple occasions, housing inspectors attempted to enter Camara's apartment without a warrant to conduct an inspection, which he refused each time.[23] Camara alleged that any warrantless inspection violated the Fourth and Fourteenth Amendments.[24] The Court disagreed with this argument, determining that such searches could be permissible if there were a

[14] 387 U.S. 523, 539-40 (1967).
[15] 387 U.S. 541, 546 (1967).
[16] 359 U.S. 360 (1959), *overruled by* Camara v. Mun. Court, 387 U.S. 523 (1967).
[17] *Id.* at 361–62.
[18] *Id.* at 362-63.
[19] *Id.* at 367–68.
[20] *Id.* at 373.
[21] Camara v. Mun. Court, 387 U.S. 523, 528 (1967).
[22] *Id.* at 525.
[23] *Id.* at 526-27.
[24] *Id.* at 527.

"reasonable governmental interest."[25] This approach was designed to balance the public and private interests at stake in these types of inspections.[26]

In the decision, the Court provided details on how governmental programs to inspect dwellings for compliance with fire, health, and housing codes could be constitutional, despite lacking a warrant or probable cause:

> "[P]robable cause" to issue a warrant to inspect must exist if reasonable legislative or administrative standards for conducting an area inspection are satisfied with respect to a particular dwelling. Such standards, which will vary with the municipal program being enforced, may be based upon the passage of time, the nature of the building (e.g., a multi-family apartment house), or the condition of the entire area, but they will not necessarily depend upon specific knowledge of the condition of the particular dwelling.[27]

Crucially, the *Camara* Court inserted multiple protections in order to prevent legislatures and regulators from creating scores of programs compliant with these requirements in order to create an end run around the Fourth Amendment. The Court identified "persuasive factors" to support whether inspections were reasonable, including 1) doubt "that any other canvassing technique would achieve acceptable results" and 2) that inspections "involve a relatively limited invasion of the urban citizen's privacy."[28] The government had to demonstrate, in balancing the need to search against the invasion of the search, that the program was reasonable and thus that previously defined legislative or administrative standards existed to provide an effective "warrant to inspect."[29]

See v. City of Seattle addressed a similar inspection regime as *Camara*, applying that analysis to Seattle's fire inspection rules and finding that Seattle's program did not pass muster under the *Camara* factors.[30] *See* addressed a fire inspection regime that applied to businesses, not personal dwellings; however, the court did not find much value in this distinction, arguing "The businessman, like the occupant of a residence, has a constitutional right to go about his business free from unreasonable official entries upon his private commercial property."[31] As in *Camara*, the Court supported administrative searches of premises (in this case, commercial premises), but required an administrative subpoena, "sufficiently limited in scope, relevant in purpose, and specific in

[25] *Id.* at 539.

[26] *Id.*

[27] *Id.* at 538.

[28] *Id.* at 537.

[29] *Id.* at 538.

[30] See v. City of Seattle, 387 U.S. 541, 542-46 (1967).

[31] *Id.* at 543.

directive so that compliance will not be unreasonably burdensome."[32] Additionally, the Court noted,

> while the demand to inspect may be issued by the agency, in the form of an administrative subpoena, it may not be made and enforced by the inspector in the field, and the subpoenaed party may obtain judicial review of the reasonableness of the demand prior to suffering penalties for refusing to comply.[33]

Camara and *See*, taken together, create a balancing act more precise than the thumb on the scale that *Frank* presented. Administrative agencies have the ability to conduct searches with rather broad authority; however, they must stay within the lines drawn by the Court designed to protect individuals and businesses. By explicitly requiring such searches to be authorized and governed by standards, contemplate alternatives, limit discretion in the field, and allow for pre-compliance review, the Court created an effective system that allows the government to achieve its ends while still limiting its powers and protecting individuals in conformity with the standards of the Fourth Amendment's text.

B. Administrative Search Decay

The issues with administrative searches developed in the years following the Court's formulation of the doctrine in *Camara* and *See*. *Camara* and *See* created a standard in which a series of persuasive factors were used to evaluate a search's constitutionality.[34] In her article *Disentangling Administrative Searches*, Eve Brensike Primus identifies these factors as "necessary conditions, not sufficient ones, for exempting the housing inspection program [in *Camara*] from the default rule requiring individualized suspicion."[35] In early administrative search cases, Primus singles out three factors in particular that allow what she calls "dragnet searches"[36] to remain constitutional under the Fourth Amendment.[37]

First, the search should be minimally invasive and conducted for important health and safety reasons.[38] Second, executive discretion must be limited to prevent arbitrary, discriminatory, or harassing searches.[39] In the context of administrative searches, this effectively required "legislative or regulatory

---

[32] *Id.* at 543-44.

[33] *Id.* at 544–45.

[34] *See Camara*, 387 U.S. at 537; *See*, 387 U.S. at 543-45.

[35] Primus, *supra* note 7, at 264.

[36] Professor Primus uses this term due to their broad scope over certain areas or types of activity. *Id.* at 260.

[37] *Id.* at 265-67.

[38] *Id.* at 265-66.

[39] *Id*. at 267 ("The normal method of protecting citizens against arbitrary, discriminatory, and harassing searches is to limit the discretion of executive officials . . . .").

regimes that were as effective as warrants in eliminating discretion."[40] Third, the requirement should be one of effectively last resort: "administrative searches were justified only if they were absolutely necessary."[41] As Professor Primus notes, "If the government could labor under the individualized suspicion requirement and still successfully abate hazardous conditions, then there was no good reason to expose large numbers of innocent people to unnecessary dragnets."[42]

Effectively, under the early administrative search cases, the government would need to at least implicitly demonstrate that its goals of promoting public safety or health could *only* be satisfied by a specific administrative search, rather than an alternative program that required a level of individualized suspicion. Multiple programs that did not demonstrate this requirement were struck down as impermissible under the administrative search exception.[43]

The Supreme Court continued to analyze and refine the administrative search exception in cases decided in the early 1970s. In *United States v. Biswell*, the Court first examined a federal regulatory inspection regime for Fourth Amendment compliance.[44] The Gun Control Act — the statutory regime at issue in *Biswell* — allowed for entry into premises (including storage areas) where firearms or ammunition were kept, in order to examine both weapons and required records.[45] Biswell challenged the statute as a warrantless search of the premises, but the court upheld it, as the statute included limitations on the time, place, and scope of the inspections.[46] These limitations demonstrate both the need to restrict government discretion and the desire to ensure that such searches were minimally invasive.

A subsequent case, *Donovan v. Dewey*, describes two different situations in which federally authorized regulatory programs would be permissible.[47] *Donovan* concerned a federal statute allowing for mine inspections, but the Court expounded more generally on what kinds of warrantless administrative searches were permissible.[48] First, if Congress authorized inspections but did not set out procedures that inspectors would need to follow, a warrant would be necessary to limit executive discretion.[49] Alternatively, if the Congressionally

[40] *Id.*

[41] *Id.* at 266.

[42] *Id.*

[43] *See* Wayne R. LaFave, *Computers*, *Urinals, and the Fourth Amendment: Confessions of a Patron Saint*, 94 MICH. L. REV. 2553, 2579–80 (1996) (collecting cases).

[44] 406 U.S. 311, 311-12 (1972).

[45] *Id.*

[46] *Id.* at 315.

[47] 452 U.S. 594, 599-600 (1981).

[48] *Id.* at 596-600.

[49] *Id.* at 599 (first quoting Colonnade Catering Corp. v. United States, 397 U.S. 72, 77

authorized inspection program set out a "predictable and guided federal regulatory presence" that did not allow for unchecked governmental discretion, a warrant would not be required.[50] These strong protections meant that administrative searches needed to be either very specific in targeting an individual business or residence, or created by legislatures (or, presumably, regulators) with unambiguous standards.

However, this relatively high standard for administrative searches did not last. Professor Primus argues that the first phase of administrative searches ("dragnet searches") became muddled by a new type of search.[51] The new variety, which she terms "special subpopulation searches," targeted specific people (or specific people acting in particular ways), who had reduced expectations of privacy and thus did not need to be searched under the traditional probable cause standard.[52] Such searches targeted students, government workers, probationers, and parolees.[53] These searches differed from dragnet searches because of their reduced requirement for individualized suspicion due to the nature of those "subpopulations" — a requirement that was effectively eliminated in dragnet searches, which allowed for searches of personal and business premises without *any* cause.[54] The special subpopulation searches, though, were more invasive than dragnet searches, and could potentially target individuals as well as premises or property.[55] Finally, executive discretion (and its abuse) was treated as less of an issue than before, and a reasonableness standard was employed after the fact in order to protect privacy interests.[56]

The conflation of these two types of searches has meant that protections for individuals have lowered, and that administrative searches are increasingly favored by the courts to a degree that they were not in the earlier era of *Camara* and *See*. When the reasonableness standard becomes the main barometer for whether or not an administrative search is valid, the government almost always prevails given the generally lax standards for reasonableness (which some have equated to a "rational basis" standard as found in other constitutional areas).[57] Professor Primus observes that an additional consequence is the normalization of these searches, in a world in which individualized suspicion is no longer seen

(1970); then quoting Marshall v. Barlow's Inc., 436 U.S. 307, 323 (1978)).

[50] *Id.* at 600, 604.

[51] Primus, *supra* note 7, at 259.

[52] *Id.* at 260.

[53] *Id.* at 271.

[54] *Id.*

[55] *Id.*

[56] *Id.* at 272.

[57] *See, e.g.*, Tracey Maclin, *The Central Meaning of the Fourth Amendment*, 35 WM. & MARY L. REV. 197, 199-200 (1993).

as preferable or necessary.[58]

Critics of the current doctrine have discussed why these issues are very real ones for the public.[59] The pervasiveness of searches, the offense to privacy interests, endangering individual liberty, and the possibility for pretextual actions are all reasons for concern. In the context of new technologies and increased data collection, some have argued that the cozy relationship between incumbent industries and their regulators has allowed the regulators to use administrative searches as a harassing technique.[60] Under this theory, existing firms like hotels and cab companies use their relationships with regulators to influence regulators to collect information from new entrants with data-rich records. There is little evidence that such arrangements exist, but they do emphasize the need to make sure that administrative searches are performed to pursue legitimate governmental purposes, rather than for protectionist reasons.

The decay in administrative searches — a weakening of strong protections that once existed — has very real consequences for privacy. These consequences accrue not just for businesses but also for individuals, as described *supra*. The changes in data practices means that these administrative searches are much more likely to collect sensitive data, and that the courts are more likely to uphold them than they were in the past.

C. Third Party Problems

One might assume that even if businesses cannot challenge administrative searches, there might be recourse for individuals — whose data, after all, is frequently the subject of such searches — who might have the capacity to assert Fourth Amendment rights. However, the third party doctrine, which originated in the 1970s, makes this type of claim difficult for individuals to assert.

The third party doctrine's archetypal formulation was made in *United States v. Miller*, a case involving bank records.[61] In *Miller*, two banks received subpoenas from federal law enforcement officials to turn over a customer's bank

---

[58] Primus, *supra* note 7, at 290.

[59] *See, e.g.*, Christopher Slobogin, *Government Dragnets*, 73 L. & CONTEMP. PROBS. 107, 124–26 (2010).

[60] *See, e.g.*, Bill Frezza, *The Rise of Uber Should Have Politicians, Regulators and Crony Capitalists Shaking with Fear*, FORBES (June 23, 2014, 6:31 AM), https://www.forbes.com/sites/billfrezza/2014/06/23/the-rise-of-uber-should-have-politicians-regulators-and-crony-capitalists-shaking-with-fear/#5147f93f5559 [https://perma.cc/JU6U-FAHX] (explaining that state and local governments have issued cease and desist letters, ticketed Uber drivers, impounded their cars, and attempted to pass regulations that outlaw Uber's business model).

[61] 425 U.S. 435, 436 (1976), *superseded by statute*, Right to Financial Privacy Act of 1978, 12 U.S.C §§ 3401-3422 (2012).

records, which they followed — without informing the customer.[62] The customer moved to suppress the records, claiming his Fourth Amendment rights were violated.[63]

The Supreme Court disagreed. In a now-classic description of the reasoning of the third party doctrine, it stated:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[64]

While the Court characterized this description as an extension of existing decisions, it nevertheless clarified the limits of Fourth Amendment protections. A few years later, *Smith v. Maryland* addressed the third party doctrine in the context of telephone records.[65] In *Smith*, the Court determined that individuals have no expectation of privacy in the numbers they dial, because dialers are aware that they are transmitting information to the phone companies and, therefore, have no expectation that the information that they are transmitting will remain private.[66]

As a result, individuals have little recourse in asserting Fourth Amendment rights over information transferred to a third party and collected by the government from that third party. Moreover, the third party doctrine is of particular importance in administrative search cases. Both *Miller* and *Smith* concerned situations in which individuals provided information to businesses, who are frequently the target of administrative searches.[67] Yet, it is the businesses that have the ability to challenge such searches, rather than the individuals whose data becomes incorporated into the records, files, and databases of businesses.

The third party doctrine is one of the most criticized elements of Fourth Amendment jurisprudence.[68] Orin Kerr, in his influential article *The Case for the Third-Party Doctrine*, notes that some treat it as "the *Lochner* of search and seizure law"[69] — a reference to the discredited Supreme Court case *Lochner v.*

---

[62] *Id.* at 437–38.

[63] *Id.* at 436-37.

[64] *Id.* at 443.

[65] 442 U.S. 735, 735 (1979), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848.

[66] *Id.* at 743.

[67] *See id.* at 744; *Miller*, 425 U.S. at 442.

[68] *See* Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 245-265 (2006).

[69] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563

New York,[70] treated as wrongly decided and a symbol of an overly politically minded Supreme Court.[71] Yet, despite disapprobation from the scholarly community, the Supreme Court has made few direct moves to reevaluate it.

One of the most promising signs came in the 2012 case *United States v. Jones*, a case concerning GPS tracking of an individual by the police.[72] In her concurring opinion, Justice Sotomayor observed:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[73]

Fourth Amendment devotees have read this as a sign that at least one Justice is sufficiently concerned by the interplay among individuals, companies, data, and the government to re-evaluate the third party doctrine and provide more privacy rights to citizens.[74] Those hoping for such a re-evaluation were also heartened by the Court's recent grant of certiorari to *Carpenter v. United States*, a case concerning cell phone records.[75] The degree to which the Court addresses the third party doctrine in *Carpenter*, however, is unclear, as it was not explicitly called out in the Question Presented.

(2008).

[70] 198 U.S. 45 (1905).

[71] *See, e.g.*, Richard A. Primus, *Canon, Anti-Canon, and Judicial Dissent*, 48 DUKE L. J. 243, 244-45 (1998).

[72] 565 U.S. 400, 402 (2012).

[73] *Id.* at 417–18 (Sotomayor, J., concurring) (citations omitted).

[74] *See, e.g.*, Stephen E. Henderson, *After United States v. Jones, After the Fourth Amendment Third Party Doctrine*, 14 N. CAROLINA J.L. & TECH. 431, 431-55 (2013).

[75] United States v. Carpenter, 819 F.3d 880, 885 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (June 5, 2017) (No. 16-402); *see infra* Conclusion.

D. Current Administrative Search Doctrine: City of Los Angeles v. Patel

City of Los Angeles v. Patel, the most recent Supreme Court case to address the administrative search doctrine, began as a facial challenge to a Los Angeles city ordinance that required hotels to record several types of guest information, including names, addresses, vehicle data, and payment type.[76] These records were required to be retained for 90 days in either electronic or paper form and had to be made available to a Los Angeles police officer for review; non-compliance could result in a fine or a misdemeanor punishable by up to six months in jail.[77] No opportunity for pre-compliance review was afforded.[78]

The Supreme Court's opinion focused on two discrete issues: first, it held that facial challenges to Fourth Amendment searches were not barred or disfavored.[79] Second, and more relevant for this discussion, is the court's analysis of whether the procedures around the ordinance were constitutional. Because there was no opportunity for pre-compliance review, the ordinance violated the Fourth Amendment.[80]

The Court's holding on this second issue was as important for what it did *not* rule as for what it did. The lower Ninth Circuit *en banc* decision explored the dynamics of administrative searches at greater depth. It characterized the doctrine as allowing the government to mandate businesses to maintain records and make them available to further a legitimate regulatory interest.[81] The Ninth Circuit further discussed how those inspections are required to be "sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome."[82]

The Supreme Court did not explicitly take up this inquiry in its ruling, limiting its analysis to the pre-compliance review element of administrative searches and declining to discuss other components of the ordinance.[83] However, given the current interest by the Court in analyzing the legality of contemporary

---

[76] 135 S. Ct. 2443, 2447–48 (2015).

[77] *Id*. at 2448.

[78] *Id.* at 2448–49.

[79] *Id.* at 2449.

[80] *Id.* at 2451-52.

[81] Patel v. City of Los Angeles, 738 F.3d 1058, 1064 (9th Cir. 2013) (en banc) (citing Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 45-46 (1974); McLaughlin v. Kings Island, Div. of Taft Broad. Co., 849 F.2d 990, 992-93 (6th Cir. 1988)).

[82] *Id.* (quoting See v. City of Seattle, 387 U.S. 541, 544 (1967)). Interestingly, the Ninth Circuit used the original formulation of the administrative search doctrine to describe its requirements, rather than including the mutations that the Supreme Court has introduced over the intervening years. Implicitly, the opinion endorses the parameters set out by *Camara* and *See*. *See infra* Parts II and III.

[83] *Patel*, 135 S. Ct. at 2454.

searches,[84] it is possible that a future case might provide a more suitable vehicle for reforming the administrative search doctrine. Such a reformulation would be long overdue, as the doctrine is in grave need of reform. Scholars have noted the confusing state of the law in recent years,[85] but beyond the legal problems, changes in business models and regulatory practices are not reflected in the doctrine.

E. Current Business Practices and Challenges for Administrative Searches

The ordinance at issue in *Patel* set out recordkeeping requirements for both analog and digital records,[86] but the origin of the administrative search dates to the pre-digital era.[87] At that time, when regulatory agencies conducted business inspections, the records they inspected were almost exclusively kept as hard copies — in files, books, and notes. Indeed, the subject of the searches in the first two administrative search cases included physical premises.[88] The early Supreme Court administrative search cases, like *Camara* and *See*, allowed for fire code inspections on physical premises and records inspections for firearm dealers and liquor establishments.[89]

The common thread in these seemingly disparate areas is the physicality of each search and inspection. Premises inspections are inherently tangible; they do not exist in an abstract or digitized space. Precious few businesses in the early 1970s would be storing records in a digital format; more likely, they would have physical copies and files. I observe this not to make a cyber-exceptionalism argument, but merely to point out that business practices have changed in the intervening decades.[90]

---

[84] *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2480 (2014) (holding that the police generally may not search digital information on a cell phone seized from an arrested individual without a warrant).

[85] *See, e.g.*, Primus, *supra* note 7, at 257*;* Slobogin, *supra* note 59, 107-09.

[86] *Patel*, 135 S. Ct. at 2447-48.

[87] Camara v. Mun. Court, 387 U.S. 523, 539-40 (1967).

[88] *See id.* at 525; See v. City of Seattle, 387 U.S. 541, 541 (1967).

[89] United States v. Biswell, 406 U.S. 311, 317 (1972); Colonnade Catering Corp. v. United States, 397 U.S. 72, 76-77 (1970); *See*, 387 U.S. at 546.

[90] A great deal of academic writing has focused on whether the Internet and accompanying technologies provide a new framework for legal analysis, or whether such discussions were a form of cyberexceptionalism that unnecessarily characterized digital technology as a separate realm. *See* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996); David R. Johnson & David Post, *Law and Borders — The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996). Rather than take a position on these issues, this Article merely observes how digital technology has *changed* the subject of administrative searches from being almost entirely physical to a mix of physical and digital. Some of the efficiencies of digital storage necessarily implicate how the doctrine is applied on the ground.

Records that would once have had to be laboriously taken down by hand can now be photocopied, scanned, and digitized much more swiftly. Digital records do not need to be taken from one office to another; can be retained indefinitely without taking up physical space; and are easily duplicated, transferred, or deleted. Records are more robust than before, potentially containing personal, financial, and location information.

Moreover, the growth and conglomeration of businesses means that records are now more longitudinally descriptive. Whereas once a guest might check into Hotel A in San Antonio, Hotel B in Annapolis, and Hotel C in Prague, now it is much more likely that Corporation D has bought each of these Hotels, which likely means that it holds the customer's information about movements in three different localities in one centralized database, as opposed to three different hoteliers with no connection to each other.

Finally, the growth of "disruptive" online service providers like Airbnb and Uber (commonly referred to as part of the "sharing economy," the "gig economy," or the "on-demand economy"), which operate internationally in market sectors that are classic targets of administrative searches, adds another wrinkle to the dynamic between business and regulators. Much like the conglomerates described in the preceding paragraph, these companies have massive amounts of data pertaining to their customers, in jurisdictions throughout the world.[91] These data sets can include personally identifiable information, financial data, location information, and contact information.[92]

But because they came to prominence in a smartphone era, such on-demand companies have an added bonus: their customers interact with them on a constant basis, much more than customers might with a hotelier or a limousine company. For example, if a summer storm hits just when I plan to leave my Los Angeles office, I can open Uber to plan to take a car home. But, if by the time I get to the front of the building, the skies are clear, I can merely change my mind and never actually request a car. Uber, however, could collect my location information as soon as I open the app; that information would be added to my customer record; that record could subsequently be the subject of an administrative search — even by a non-Los Angeles regulator, because Uber would not necessarily parse out a customer's records by locality. Yet in this example, *a trip was never taken*, though a regulator under the administrative search doctrine could potentially collect data pertaining to a customer record.

By contrast, if the same situation arose twenty years ago, there would be no record at all of my brief thought to take a cab home, because I would have changed my mind before leaving the building and never gotten around to hailing one on the street. Changes in technology and business practices have meant that the old days of searching premises, thick hotel ledgers, and trip receipts are gone

[91] *See, e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (2015).

[92] *Id.*

— or at least radically different. This does not mean that the administrative search doctrine holds no relevance for today's economy; indeed, its underlying justifications of promoting regulatory compliance, consumer protection, and public safety are as important as ever. However, it does mean that the balancing elements that the Supreme Court articulated in *Camara* and *See* must, at the very least, be re-examined to ensure their future vitality.

Governmental entities, for their part, disclaim any issues with how administrative searches are conducted in today's digital economy.[93] Instead, they emphasize their need to promote public safety and compliance with the laws, especially given how some companies have flaunted compliance with regulatory requirements.[94] Rarely, if ever, does the government explicitly call out the legality of administrative searches; instead, legislators, regulators, prosecutors, and elected officials choose to speak in terms of safety, and compliance. This may be because the administrative search doctrine is too obscure for the general public to be concerned about; because the government does not want its citizens to know of its broad powers to collect information from businesses; or because their focus is truly on promoting public safety and regulatory compliance, and the administrative search doctrine is merely one tool in order to achieve that goal.

---

[93] To some degree the government's position is an extension of Judge Easterbrook's "law of the horse" position — that drawing distinctions based on the nature of the company and/or digital practices is irrelevant and does not forestall the government from pursuing its mandate. This is true insofar as it goes, though it minimizes how new services and new practices can change the Fourth Amendment inquiry. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2484-85 (2014) (discussing at length how the characteristics of smartphones mean that the Fourth Amendment analysis of searches incident to arrests that involve smartphones are different than earlier cases prior to the technology's invention and adoption). The government's unwillingness to entertain potential revisions or reformulations of the administrative search doctrine could be in part due to some companies' (most notably Uber and Airbnb) history of regulatory intransigence and lack of strong internal governance. *See, e.g.*, Eric Newcomer, *Uber Paid Hackers to Delete Stolen Data on 57 Million People*, BLOOMBERG (Nov. 22, 2017, 4;58 PM), https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data [https://perma.cc/4AHC-3AG3]. The government may be unwilling to give an inch to opponents that have, at times, undermined them in administrative hearings, court proceedings, and in day-to-day operations. *See, e.g.*, Mike Isaac, *How Uber Deceives the Authorities Worldwide*, N.Y. TIMES (Mar. 3, 2017), https://www.nytimes.com/2017/03/03/technology/uber-greyball-program-evade-authorities.html.

[94] *See, e.g.*, Katie Benner, *Airbnb in Disputes with New York and San Francisco*, N.Y. TIMES (June 28, 2016), https://www.nytimes.com/2016/06/29/technology/airbnb-sues-san-francisco-over-a-law-it-had-helped-pass.html; Jeremy C. Owens, *San Francisco and L.A. Sue Uber, Claim Illegal and Misleading Actions*, THE MERCURY NEWS (Dec. 9, 2014), http://www.mercurynews.com/2014/12/09/biz-break-san-francisco-and-l-a-sue-uber-claim-misleading-and-illegal-actions/ [https://perma.cc/U7VQ-NKFD].

What is clear is who loses in this fraught dynamic: individual customers and the public at large. Individuals have little recourse to challenge searches when their records have been disclosed to a third party.[95] Additionally, the debate surrounding companies and access to data by regulators takes on an abstract quality in reporting. The capacity of the government to search records that may contain individual data often goes unreported and thus, given the obscurity of how regulatory agencies operate, the public likely has little awareness that their information may be handed over to the government as part of an oversight regime.

As discussed in the next Part, this would be less of an issue if the administrative search doctrine still had its original teeth. The relative obscurity of the practice of these searches, coupled with the changes in technology and data practices, means that administrative searches paradoxically attract little attention from the public and yet affect their information in dramatic and frequent ways. The next Part further analyzes how changes to the administrative search doctrine over time, as well as the introduction of the third party doctrine into Fourth Amendment jurisprudence, has meant that individuals are affected by searches more than ever before—but have fewer options in order to assert privacy rights in that context.

II. REVERSING ADMINISTRATIVE SEARCH DECAY AND CHALLENGES TO REVERSAL

A. Existing Criticisms of Administrative Searches

Regardless of the Court's current attitude towards administrative searches, the third party doctrine, and their interplay in the context of business records containing consumer data, scholars have repeatedly taken up the task of recasting these Fourth Amendment questions in ways that more fairly balance individual rights with government interests as compared to current case law.

Criticisms of the administrative search doctrine date back decades. Scott Sundby's critique of *Camara* in *A Return to Fourth Amendment Basics: Undoing the Mischief of* Camara *and* Terry lays the blame for the confusion at the feet of a misunderstanding of the relationship between the warrant and probable cause clauses of the Fourth Amendment.[96] Professor Sundby argues that *Camara* allowed probable cause to be governed by a reasonableness standard, rather than the converse, thus weakening individual protections by expanding "the range of acceptable government behavior beyond intrusions based on individualized suspicion to include activities in which the government

[95] *See* discussion *supra* Section I.C.

[96] Scott E. Sundby, *A Return to Fourth Amendment Basics: Undoing the Mischief of* Camara *and* Terry, 72 MINN. L. REV. 383, 383–85 (1988).

interest outweighed the individual's privacy interests."[97] In essence, the Court had put the thumb on the scale for the government when evaluating administrative searches under the *Camara* rule.[98]

Professor Sundby's solution is to recalibrate the scale. For administrative searches, he would create a "compelling government interest—least intrusive means test" in order to evaluate an administrative search's validity, which, in his view, would effectively create a strict scrutiny standard.[99] However, unlike strict scrutiny analysis in other areas, which almost always comes out against the government, Professor Sundby claims that in the Fourth Amendment context strict scrutiny would not necessarily deal a death blow to administrative searches.[100]

Professor Sundby's belief that administrative searches could survive strict scrutiny more easily than, say, race-based classifications is not buttressed by a wealth of evidence. Indeed, swinging the pendulum from one perceived extreme (in which administrative searches are too often upheld without careful examination) to another (in which they are presumptively disfavored) would do little to solve the challenge of properly formulating the doctrine. Moreover, because so many administrative searches happen in the regulatory context — which, through its operation in the administrative state, is designed to promote regulatory stability and predictability for industry, agencies and the public — radical shifts in law and policy *should* be avoided. The incrementalist model of the administrative state means that a shift towards disfavored administrative searches would greatly destabilize much of the regulatory goals and business expectations, thus weakening the ability to protect individuals and consumers — an implicit end of both the administrative state and administrative searches.

In *The Fourth Amendment in the Balance: Accurately Setting the Scales Through the Least Intrusive Alternative Analysis*, Nadine Strossen argues, similarly to Professor Sundby, for a revised approach to the balancing tests employed by the courts when analyzing Fourth Amendment rights.[101] Unlike Professor Sundby, Professor Strossen views Fourth Amendment balancing tests

---

[97] *Id.* at 394.

[98] Professor Sundby argues that the *Camara* Court's reasoning, while ostensibly limited to administrative searches, spilt over into other areas of Fourth Amendment analysis. Moreover, in his view, the lack of rhetorical limits on the concept of "administrative searches" and the government's ability to easily characterize their activities as "administrative" and thus, more likely to be upheld, means that the exception is much broader than it might appear on first blush. *Id.* at 406–11.

[99] *Id.* at 441–42.

[100] *Id.* at 444–46.

[101] 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, 1177 (1988).

as something of a *fait accompli*; her proposed reform would incorporate a least intrusive means analysis into the Fourth Amendment balancing framework.[102] Professor Strossen contends that traditional Fourth Amendment analyses systemically misidentify and inaccurately compare the interests at play between individual rights and government interests; specifically, she argues:

> The Court's tendency to focus on individual fourth amendment litigants also causes it to neglect systematic evaluation of the collective harm to individual rights resulting from searches or seizures that are similar or identical to the one that gave rise to the case. This failure leads to significant undervaluation of the cost to individual rights of mass or random searches or seizures.[103]

This is reflected in the extensive research demonstrating that the inchoate, distributed nature of broad privacy harms makes them challenging for individuals and courts to effectively analyze and value.[104] Professor Strossen also criticizes the courts for abstracting the government's interest to a level of generality that is difficult to challenge, and for credulously agreeing that the government's chosen methods for doing so are the correct and best ones.[105] Professor Strossen argues for the inclusion of a "least intrusive means" analysis into Fourth Amendment analyses in order to better reflect the relative positions of individuals and the government.[106] In her view, this would more accurately reflect the particular costs and benefits of the suite of search and seizure techniques, and thus allow for more effective balancing.[107]

In the administrative search context, this is of particular importance as it presents a common example of the problems that Professor Strossen identifies. Administrative searches typically have broad effects, implicating many businesses (and thus many individuals). Because they are generally undertaken under the guise of public safety, consumer protection, and/or regulatory oversight, it is difficult to quibble with their premises. And because such

---

[102] *Id.*

[103] *Id.* at 1196.

[104] *See, e.g.*, Alessandro Acquisti et al., *What is Privacy Worth?*, 42 J. LEGAL STUD. 249, 267-70 (2013) (utilizing a field experiment based on behavioral economics and decision research to investigate the values individuals assign to the protection of their personal data); Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 881–84 (2003) (outlining the privacy harms related to searches and the remedies for such harms).

[105] Strossen, *supra* note 101, at 1201. This is perhaps due to courts' unwillingness to too closely examine law enforcement and government decisionmaking in the context of the Fourth Amendment. *See, e.g.*, Whren v. United States, 517 U.S. 806, 813–15 (1996) (acknowledging the Supreme Court's unwillingness to assess law enforcement decision making in relation to Fourth Amendment challenges).

[106] Strossen, *supra* note 101, at 1238–53.

[107] *Id.* at 1266.

searches are undertaken pursuant to statutory authorization or administrative rules, courts may be unwilling to question the methodology of the search, lest they be accused of judicial micromanaging.

Professor Strossen's solution of including a least intrusive means analysis addresses some of the common problems with administrative searches in contemporary practice — particularly the issue of data over-collection and a lack of narrow tailoring when conducting searches. Whether the inclusion of a least intrusive means component into the balancing test most courts employ would better balance the equities in administrative searches is unclear. Despite Professor Strossen's efforts to include guidelines as to how to effectively evaluate different search alternatives, it is not clear that courts would be willing to step into the fray and make determinations about what search alternatives presented are the least intrusive. While courts frequently do so, as Professor Strossen notes, in the context of First and Fourteenth Amendment cases,[108] there have been mixed messages in doing so in Fourth Amendment cases.[109] Professor Strossen preemptively answers criticisms of the ability of courts to evaluate different alternatives,[110] but the fundamental *willingness* of courts to do so, given their traditional preference for deferring to the government in the Fourth Amendment sphere, is uncertain.

This would be particularly challenging in the administrative context, in which searches may be undertaken pursuant to statutory authorization or a regulatory rule; in theory, the methodology of those searches has been chosen after a weighing of alternatives. Professor Strossen casts this as a *benefit* — courts can look to the record in order to determine whether or not the chosen alternative was actually the least intrusive, and thus "correct" one.[111] But for whatever reason, courts have been reluctant to do so. In *Mich. Dep't of State Police v. Sitz*, for example, the Court explicitly declined to second-guess the determinations of other government officials.[112] Justice Rehnquist stated "for purposes of Fourth Amendment analysis, the choice among such reasonable alternatives remains with the governmental officials who have a unique understanding of, and a responsibility for, limited public resources, including a finite number of police officers."[113]

It is puzzling *why* courts are willing to make determinations into areas of agency action that fall outside the Fourth Amendment[114] — administrative law

[108] *Id.* at 1210–11.

[109] *Id.* at 1215–31.

[110] *Id.* at 1242–49.

[111] *Id.* at 1245–49.

[112] Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 453-54 (1990).

[113] *Id.*

[114] One theory may be that corporations are particularly interested in challenging agency actions outside of searches due to frustrations with regulation. Government searches are

is filled with such cases, from arbitrary and capricious review to *Chevron* deference — and perhaps they should be less concerned about doing so. Moving towards a better union of administrative law and the Fourth Amendment has received scholarly attention; for example, Daphna Renan, in *The Fourth Amendment as Administrative Governance*, argues for a more holistic integration of administrative governance into Fourth Amendment law.[115] It remains to be seen whether the courts will actualize this goal.

The critiques of Professor Sundby, Professor Strossen, and others have continued as the administrative search doctrine became increasingly muddled even as administrative searches became more prevalent and pervasive. Christopher Slobogin has argued that dragnet searches should be governed by narrow, nondiscriminatory legislative enactments and proportionality and exigency standards, asserting that the carte blanche authority given to the government for dragnet searches is too broad.[116] Professor Slobogin identifies many of the same concerns as other critics, but also observes that the increase in technological sophistication, national security concerns, and big data and predictive policing increases the instability in the current administrative search ecosystem.[117]

Professor Slobogin's solution to these issues incorporates a variant of political process theory (which argues that courts should intervene on legislative challenges if there has been a significant defect in the democratic process) that incorporates exigency and proportionality standards.[118] Under this proposal, courts would employ traditional political process theory, but incorporate a safeguard for situations in which political process theory defects (such as when the legislative or regulatory standards do not give targeted communities a voice or when they grant too much executive discretion).[119] The inclusion of a proportionality requirement would allow courts to intervene if the intrusiveness of a search was outweighed by the hit rate; the more intrusive a search, the higher a hit rate would need to be in order to justify it.[120] Outside of emergency situations, the exigency principle would require ex ante approval for searches

perhaps of less importance than reducing regulatory burdens and enforcement (though they can be considered a regulatory burden).

[115] Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1128-29 (2016).

[116] Slobogin, *supra* note 59, at 108–10.

[117] *See id.* at 109.

[118] *Id.* at 131, 136–43.

[119] *Id.* at 136.

[120] *Id.* at 138–41. One could argue that the proportionality requirement should analyze the intrusiveness against both the hit rate and the importance of the search. This would take into account searches that are highly important but have a lower hit rate. Thanks to David Moran for the insight here.

— not necessarily by a magistrate, but potentially by politically accountable officials as well.[121]

Professor Slobogin's marriage of political process theory to exigency and proportionality standards allows for a counterbalance of allowing traditionally pro-government legislatures and agencies to pursue searches, while limiting those searches when they are too invasive to justify their results (or if they don't receive ex ante authorization — though nearly all administrative searches will, as they are generally undertaken pursuant to statutory or regulatory guidelines).

The administrative searches that implicate data held by businesses generally target specific areas of the economy (e.g. taxis, hotels, and financial institutions), few of which give rise to political process defects given their political capital in legislation and regulation.[122] Therefore, under Professor Slobogin's framework, the key point of inquiry for an administrative search targeting a data-rich business would be the proportionality question. Judges would thus balance the invasiveness of the search against the hit rate for these types of regulatory investigations.

The challenge, though, is determining whether or not judges would determine these searches to be invasive at all. While privacy theorists in law, computer science, and policy have long raised alarm bells concerning government access to data, the potential of linking disparate databases, and backdoor sharing, courts have not been as active in finding privacy harms in those situations. Whether judges will be willing to fairly balance these concerns, even with a generous eye towards individual privacy, remains uncertain.

One could argue that if the courts fail to see a privacy issue under Professor Slobogin's framework — which works energetically to balance different equities under a cognizable balancing test — for the types of searches described *supra*, that perhaps no issue actually exists. Yet this Article's proposal of a return to the first principles for administrative searches can be seen not as seeking to influence judges to find privacy violations where few would see them, but rather to reinforce the foundational project of the administrative search exception at its initial conception.

B. Reinstating Camara and Its Progeny

The solutions described above view the administrative search doctrine through the lens of judicial failure to preserve a balance between individuals and the government. Arguably, the original formulation of the doctrine in *Camara* and its progeny does this in a way still applicable to contemporary searches.[123]

---

[121] *Id.* at 141.

[122] New entrants may not be as successful as having their views represented in the legislative and political processes as existing entrants. However, as innovators they frequently receive preferential treatment as part of the politically attractive "entrepreneurship" sector.

[123] For simplicity, this Article refers to these decisions and their formulation of the

As formulated in *Camara* and its immediate subsequent cases, administrative searches were treated as permissible if they balanced the government's interest and the intrusion on individuals and businesses, were authorized preemptively, limited executive discretion, and had to be employed in situations in which individualized suspicion could not apply.[124]

In the context of the data collection practices described *supra* Section I.E, the *Camara* factors would more effectively balance the concerns raised by overbroad administrative searches. In the 2014 TLC search described *supra*, it was certainly necessary for the TLC to gain information from taxi cabs regarding their practices in order to promote safety, ensure equal treatment of different subpopulations, and monitor for compliance of existing regulations.

But the TLC continued to increase its requests for data to include information that did not seem necessary to promote the needs that it articulated. For example, the TLC argued that it needed more information from cabs in order to prevent fatigued driving;[125] however, it wanted both pickup and dropoff location, rather than trip duration and timing, to minimize the possibility of fatigued drivers.[126] The inherent mismatch between the stated goals and the data collected would have tripped the *Camara* prong that requires effective balancing.

The TLC acted appropriately by debating changes to these rules; had they not, the requirement that searches be preemptively authorized would have been violated. Because of the broad investigatory powers that administrative searches enable in the regulatory context, coupled with their definitional lack of individualized suspicion,[127] preemptive authorization is crucial in effectively

administrative doctrine as the *Camara* factors.

[124] Primus, *supra* note 7, at 267, 270.

[125] Matthew Flamm, *City to Uber and Lyft: Hand Over Your Trip Data*, Crain's New York Business (Feb. 2 2017 4:12 PM), http://www.crainsnewyork.com/article/20170202/TRANSPORTATION/170209965/taxi-limousine-commission-approves-new-driver-fatigue-rules-and-will-require-for-hire-vehicles-including-those-using-uber-and-lyft-to-report-where-riders-are-dropped-off [https://perma.cc/FCW7-8WND].

[126] Gautam Hans, *TLC on the Wrong Trip with Ride Tracking*, N.Y. DAILY NEWS (Dec. 29, 2016, 5:00 AM), http://www.nydailynews.com/opinion/tlc-wrong-trip-ride-tracking-article-1.2926903 [hereinafter *TLC Ride Tracking*]. In previous work, I have articulated in more depth the challenges of mission creep and over-collection in the context of regulatory searches. *See* G.S. Hans, *Data in the On-Demand Economy: Privacy & Security in Government Data Mandates*, CENTER FOR DEMOCRACY & TECHNOLOGY (2015), https://cdt.org/files/2015/12/2016-02-23-On-Demand-Economy-Paper-updated2.pdf [https://perma.cc/572J-D2EF]; *TLC Ride Tracking*, *supra*. Ultimately, the TLC chose to collect intersection data, rather than precise drop-off location, in order to achieve its goals. *See* Flamm, *supra* note 125.

[127] Frequently, administrative agencies undertake searches that *can* rely upon individualized suspicion. For example, this could happen pursuant to an investigation

balancing government interests against individual privacy concerns.

Consider other statutory and regulatory authorizations that touch on these issues, and whether they would pass muster under the *Camara* factors. One illustrative example is a dispute that arose between Uber and the California Public Utilities Commission (PUC), which regulates privately owned public utilities.[128] The agency argued that Uber had failed to provide sufficient information on its drivers and users to determine compliance with obligations towards the disabled and to not discriminate against potential customers.[129] Uber countered that the PUC's investigative requests were overbroad and risked violating the privacy interests of riders and drivers.[130] The relevant provision of California state law, Section 5389 of the Public Utilities Code, reads:

> The commission, each commissioner, and each officer and person employed by the commission may, at any time have access to the land, buildings, or equipment of a charter-party carrier of passengers used in connection with the operation of its business and may inspect the accounts, books, papers, and documents of the carrier. Any inspection by the commission may include photocopying or the electrostatic or photostatic reproduction of documents . . . .[131]

Under this provision, the PUC could collect information from any other company it regulated "at any time" without any meaningful limitation on the categories of data that it would be allowed to collect.[132] From the government's perspective, however, this statutory authorization allows it to ensure compliance with laws and the flexibility to conduct inspections without tipping off the company.

The *Camara* factors would likely not treat this statutory language kindly. Its breadth is striking in allowing for searches "at any time" of the entirety of a business' records.[133] The concept of effective balancing of the government's interest against individual and business' privacy rights is wholly lacking in this

initiated either by the government or a consumer. This Article does not address those issues, in part because the more targeted nature of such searches does not necessitate a broad search a la those predominantly discussed herein.

[128] See, e.g., David Pierson, *Uber Fined $7.6 Million by California Utilities Commission*, L.A. TIMES (Jan. 14, 2016), http://www.latimes.com/business/la-fi-tn-uber-puc-20160114-story.html [https://perma.cc/NKM9-55NP] (explaining the "regulatory and competitive conflict Uber's business model repeatedly faces across the globe."); Jonathan Vanian, *California Regulator Fines Uber Millions of Dollars*, FORTUNE (July 15, 2015), http://fortune.com/2015/07/15/uber-fined-california/ [https://perma.cc/5FE5-DG6H].

[129] *Id.*

[130] *Id.*

[131] CAL. PUB. UTIL. CODE § 5389 (West 1990).

[132] *Id.*

[133] *Id.*

statutory authorization. Given the sensitivity of the data conceivably collected under this regime, there is no way this statute would pass muster under the proposed revitalization of the administrative search doctrine.

While this particular statutory language seems egregious in its one-sidedness, it is hardly the only regulatory regime that allows for such sweeping collection of information. Consider, for example, the inspection language at issue in *Patel*, described *supra* Section I.A:

> **2. Hotel Record Information.**
>
> (a) Every operator of a hotel shall keep a record in which the following information shall be entered legibly, either in electronic, ink or typewritten form prior to the room being furnished or rented to a guest:
>
> (1) As provided by the guest in response to an inquiry or by other means:
>
> (i) The name and address of each guest and the total number of guests;
>
> (ii) The make, type and license number of the guest's vehicle if the vehicle will be parked on hotel premises that are under the control of the Operator or hotel management;
>
> (iii) Identification information as required by Subsection 4 (a) and (b) of this section.
>
> (2) The day, month, year and time of arrival of each guest;
>
> (3) The number or other identifying symbol of location of the room rented or assigned each guest;
>
> (4) The date that each guest is scheduled to depart;
>
> (5) The rate charged and amount collected for rental of the room assigned to each guest;
>
> (6) The method of payment for the room; and
>
> (7) The full name of the person checking in the guest.
>
> (b) For a guest checking in via an electronic registration kiosk at the hotel, instead of the information required by Subsection 2(a), the hotel shall maintain the name, reservation information and credit card information provided by the guest, as well as the identifying symbol of the kiosk where the guest checked in and the room number assigned to the guest.
>
> **3. Maintenance of Hotel Record.** Every operator of a hotel shall comply with the following requirements for maintaining the hotel record:
>
> (a) The record shall be kept on the hotel premises in the guest reception or guest check-in area or in an office adjacent to that area. The record shall be maintained at that location on the hotel premises for a period of 90 days from and after the date of the last entry in the record and shall be made available to any officer of the Los Angeles Police Department for inspection. Whenever possible, the inspection shall be conducted at a time

> and in a manner that minimizes any interference with the operation of the business.[134]

The governmental goals are not articulated at all in this language. Under contemporaneous standards, they need not be — though the earlier version of the doctrine would have probably required some explanation. Presumably, given the language in 3(a), the intention is to promote public safety; in general, though, nearly all government regulation is designed, at least in part, to promote public safety. Thus the "justification" here does little rhetorical work.

Reading between the lines, it seems plausible that the City here is attempting to use the inspection process to limit fraud and ensure that hoteliers are complying with other provisions of the City Code. But this explanation goes completely unelaborated in the statute, where even a clause such as "For the purposes of promoting compliance and public safety . . . ." would do much to clarify the city's intentions here. Indeed, for such broad searches as the administrative search doctrine validates, both courts and the public have a right to know under what principles the government is seeking to exercise its power to oversee and regulate.

C. Introducing Narrow Tailoring

The danger of overbroad searches is addressed in part by the *Camara* factors, which balance the government needs against the public's privacy rights, but a more explicit requirement would encourage the government to better signal to courts and the public what it is attempting to accomplish through a particular administrative search. While there are challenges to incorporating a least intrusive means analysis,[135] using another tool of constitutional analysis — narrow tailoring — would be supported by the underlying *Camara* factors and be an administrable standard for courts to apply.

Narrow tailoring has been applied in equal protection and First Amendment jurisprudence under the strict scrutiny standard for evaluating a governmental program or action.[136] Generally, narrow tailoring requires that a government program choose a set of means that fits the goal so closely as to be neither over- or under-inclusive.[137] Narrow tailoring does not mean *perfect* tailoring, of course; it merely requires a generally close match between goals and means.

In the administrative search context, such a requirement would go far to both

---

[134] L.A., CAL., MUN. CODE § 41.49 (2008); City of Los Angeles v. Patel, 135 S. Ct. 2443, 2448 (2015). This language has been modified following the resolution of the *Patel* litigation. See L.A., CAL., MUN. CODE § 41.49 (2017).

[135] *See* Strossen, *supra* note 101, at 1243.

[136] *See, e.g.*, McCullen v. Coakley, 134 S. Ct. 2518, 2540 (2014) (applying strict scrutiny to speech restrictions); Grutter v. Bollinger, 539 U.S. 306, 333-34, 343 (2003) (applying strict scrutiny to race-based classification).

[137] *See McCullen*, 134 S. Ct. at 2540; *Grutter*, 539 U.S. at 333–34.

strengthen the *Camara* factors to avoid the backsliding exhibited by later administrative cases, and inculcate a standard that courts would be more willing to adjudicate than least intrusive means as suggested by Professor Strossen. Least intrusive means requires courts to make judgment calls or preferential choices, which, as discussed *supra*, they have historically been unwilling to do.[138] Narrow tailoring, by contrast, is more easily evaluated by an appellate court and remanded, if necessary, for further determination by a trial court.[139] Additionally, it is difficult to envision an administrative search that would pass the *Camara* factors and narrow tailoring, but fail least intrusive means.

Legislators and regulatory agencies seeking to avoid failing the narrow tailoring element of a revised administrative search standard would be able to satisfy it in a relatively straightforward manner. Articulating what the goals are and how the proposed program achieves those goals in a way that is not over-inclusive already undergirds many administrative search programs. The lack of public signaling, as discussed in the *Patel* analysis, is where the shortfall takes place.

The government has little incentive to explain how or why the proposed administrative search program is the best balance of interests. Yet, because of their breadth, their lack of individualized suspicion, and their justification in promoting public benefits, administrative searches are precisely the area in which that explanation is *most* valued. Creating a judicial oversight role in order to incentivize the promulgation of those explanations to the public preserves the balance of the *Camara* factors while being responsive to the dangers of overcollection of sensitive data that administrative searches in a digital era allows.

D. Critiques and Challenges to Adoption

Introducing a new factor into an evaluation of administrative searches — and using a standard that the Court has moved away from in the intervening years since its creation — will not be easy. As discussed *supra* Section I.B, the courts have been increasingly permissive in allowing administrative searches, even as the information those searches collect grows broader and more sensitive.

A small clue lurks in Justice Sotomayor's majority decision in *Patel*. While

---

[138] *See* Strossen, *supra* note 101, at 1215–31.

[139] Distinguishing between least intrusive means and narrow tailoring may not always be obvious in practice, as there is some overlap between the concepts. In this Article's formulation, "least intrusive means" requires the adjudicator to make a determination that the method in question is less intrusive as compared to other methods, whether specified or not. Narrow tailoring, by contrast, requires that the chosen method be relatively close to the stated goal, rather than overbroad. *See* cases cited *supra* note 137. It does not necessarily require an implicit or explicit comparison to another method.

the Ninth Circuit *en banc* opinion discussed the administrative search issues,[140] the Supreme Court devoted much of its analysis to the possibility of facial challenges to Fourth Amendment searches.[141] The Court expressly disclaimed any analysis of the requirements in the Los Angeles ordinance that mandated the retention of certain information,[142] though the dissents spent much time arguing in favor of the government's interests.[143] The Court's avoidance of the issue while identifying it as a *potential* issue might signal its willingness to take up the question in a future case.

Beyond reading those tea leaves, one might question whether the administrative search doctrine necessarily needs to be formulated. The *Patel* decision applied the test as formulated in *Camara* and invalidated the Los Angeles program (albeit on pre-compliance review grounds, rather than by assessing the dynamics of the search).[144] Why, then, must the test be reformulated?

Given the increased capacity of searches, as well as the increased laxity in upholding them, it is clear that the current method of analysis is insufficient in handling the challenges posed by digital collection. Moreover, the *Camara* factors were formulated prior to the instantiation of the third party doctrine which, as discussed *supra*, complicates the ability of individuals to protect their privacy when their information is held by a third party. As a result, more weight falls upon the regulated entity to safeguard the sensitive data. A test with increased attention to narrow tailoring thus responds to the changes that have arisen since *Camara*.

Any modification to the standards governing administrative searches would require a change from the Supreme Court. And at least under the current Court, changes seem unlikely to materialize in the immediate future. *Patel*, the last case to address administrative searches, was decided in 2015 by a 5–4 margin.[145] Given the current balance of the Court, it's a tough bet that any major changes to favor individual rights will happen in the near future.

III. PROACTIVE LOCAL CHANGE: USING THE FIPPS TO BALANCE PUBLIC INTERESTS AND PRIVACY

In the absence of judicial change, states and localities — which conduct many of the administrative searches that collect sensitive personal data — could still incorporate protections for administrative searches on their own. Beyond

[140] Patel v. City of Los Angeles, 738 F.3d 1058, 1063–65 (9th Cir. 2013) (en banc).

[141] City of Los Angeles v. Patel, 135 S. Ct. 2443, 2447–51 (2015).

[142] *Id.* at 2454.

[143] *Id.* at 2457–66 (Scalia & Alito, JJ., dissenting).

[144] *Id.* at 2456 (majority opinion).

[145] *Id.* at 2447-57.

avoiding issues such as the NYC TLC re-identification, the possibility of backdoor sharing, or data breaches attempted by hostile third parties, state and local governments would also promote democratic values by being more responsive to the concerns of the digital era in re-crafting administrative searches. This Part discusses the reasons that state and local governments should want to implement a standard akin to that proposed in Part II even absent judicial requirements, and then continues to formulate a possible framework for those standards.

A. The Benefits of Self-Binding Searches

With such latitude given to the government when it performs administrative searches, and general approbation coming from the courts, there seems to be little incentive for state and local governments to change their strategy when crafting administrative searches. However, multiple factors may cause those governments to re-evaluate their stances.

Perhaps most importantly, it would be more effective for government to adopt a narrow tailoring model as described above. Data has multiplied since the rise of digital technology at a staggering rate; it is nearly impossible to sort without automated systems. Overcollection of data by the government does not increase its success rate in pursuing public safety or compliance — it merely makes it more difficult to sort and analyze to determine non-compliance with laws and regulations.[146] Being more selective about what data to collect on the front end would make promoting governmental goals more efficacious on the back end. While collecting data first and asking questions later may seem appealing, it fails to increase the effectiveness of government oversight or public safety initiatives (the classic administrative search justifications), though it does bring its own costs — both financial and political.

Indeed, individual citizens are more aware of government collection than ever before. The information disclosed by Edward Snowden has increased the visibility of invasive government searches concerning individual data; individuals have high levels of concern regarding how the government collects information.[147] Unlike attorneys and policymakers, individual citizens are less

[146] *See, e.g.*, Dashiell Bennett, *The U.S. Government Has Collected More Data Than It Could Ever Possibly Read*, THE ATLANTIC (May 10, 2012), https://www.theatlantic.com/technology/archive/2012/05/us-government-has-collected-more-data-it-could-ever-possibly-read/328291/ [https://perma.cc/2TGR-EHBH] (summarizing that of a recent survey of 150 IT professional working within the U.S. government, "only 40 percent of those IT pros say that their agency is even bothering to analyze the data that they have and even fewer are using it to make strategic decisions on a regular basis.").

[147] Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RES. CTR.: INTERNET & TECH. (May 20, 2015),

likely to distinguish the national security, criminal, and regulatory goals of governmental data collection. While Snowden's disclosures primarily concerned the federal government's national security programs, the public's disapprobation of government data collection is not confined to that sphere.[148]

In order to promote democratic values, data collection via administrative searches will need to respond to this relative distrust of governmental collection. One method to achieve that goal would be to proactively explain and limit the reasons for administrative searches. Though this would not address the national security concerns that Americans would have, it would increase the buy-in from the general population for these kinds of searches, as well as communicate the need for such searches in the first place.

Further, any databases holding sensitive information — whether administered by the government or private companies — are a tempting target for data breaches. Data breaches have become major news events over the past few years, with attacks targeting both private and public sector databases. They have affected millions of Americans, with high profile breaches hitting Target,[149]

http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ [https://perma.cc/85UN-56B6] (concluding that "Americans also have exceedingly low levels of confidence in the privacy and security of the records that are maintained by a variety of institutions in the digital age.").

[148] *Id.* (explaining that "Americans expect that a wide array of organizations should have limits on the length of time that they can retain records of their activities and communications").

[149] Elizabeth A. Harris et al., *A Sneaky Path into Target Customers' Wallets*, N.Y. TIMES (Jan. 17, 2014), https://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html (outlining Target's data breach, which included the theft of confidential credit and debit card information of as many as 40 million Target customers and personal information of as many as 70 million more).

Hilton Hotels,[150] LinkedIn,[151] CareFirst,[152] Snapchat,[153] and the U.S. Office of Personnel Management,[154] among many others.[155] The more robust a database, the more valuable its contents it will be to unauthorized hackers. If governmental entities continue to amass massive data stores unnecessarily, they will become increasingly attractive targets for data breaches — especially if they hold sensitive information like financial data or location information, collected from businesses. Moreover, because data security is a costly, ongoing expense, the public sector will always be at a disadvantage in an era of limited governmental resources. The best data security plan incorporates limited data collection, in order to minimize a database's attractiveness from unauthorized third parties.

For these reasons, it makes good sense for state and local governments to institute preemptive limits on administrative searches, if only to more effectively pursue the goals of those searches, promote democratic functioning, and limit unnecessary costs and risks. Even absent a judicial requirement to more conservatively craft these searches in the mold of *Camara* and other early

---

[150] Jim Holthouser, *Hilton Worldwide Guest Update*, HILTON GLOBAL MEDIA CTR. (Nov. 24, 2015), http://newsroom.hilton.com/index.cfm/misc/guestupdate/hilton-worldwide-guest-update [https://perma.cc/WCN7-Y684] (informing patrons of any Hilton Worldwide Hotel over a seventeen week period that their credit card information may have been targeted).

[151] Daniel Victor, *LinkedIn Says Hackers Are Trying to Sell Fruits of Huge 2012 Data Breach*, N.Y. TIMES (May 18, 2016), https://www.nytimes.com/2016/05/19/business/linkedin-says-hackers-are-trying-to-sell-fruits-of-huge-2012-data-breach.html (reporting that hackers were attempting to sell 117 million emails and passwords of its users that resulted from a 2012 security breach of LinkedIn's data).

[152] Matthew Goldstein & Reed Abelson, *Up to 1.1 Million Customers Could Be Affected in Data Breach at Insurer CareFirst*, N.Y. TIMES (May 20, 2015), https://www.nytimes.com/2015/05/21/business/carefirst-discloses-data-breach-up-to-1-1-million-customers-affected.html.

[153] Nicole Perlroth & Jenna Wortham, *Snapchat Breach Exposes Weak Security*, N.Y. TIMES: BITS (Jan. 2, 2014, 7:12 PM), https://bits.blogs.nytimes.com/2014/01/02/snapchat-breach-exposes-weak-security/ [https://perma.cc/ZNF6-GADX] (describing that the usernames and telephone numbers of 4.6 million Snapchat users were released to a data breach of Snapchat).

[154] Julie H. Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES (July 9, 2015), https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html (stating that hackers stole personal information from 19.7 million individuals who were subject to a government background check).

[155] Josh Keller et al., *How Many Times Has Your Personal Information Been Exposed to Hackers?*, N.Y. TIMES, https://www.nytimes.com/interactive/2015/07/29/technology/personaltech/what-parts-of-your-information-have-been-exposed-to-hackers-quiz.html (last updated Oct. 3, 2017) (listing over 30 data breaches of different private companies).

administrative search cases and institute a narrowly tailored requirement, state and local governments could still proactively work to craft legislation, regulation, and policies that better protect privacy and promote government needs.

B. The Fair Information Practice Principles as a Model for Administrative Searches

The classic methodology for data collection and management, used by both the public and private sectors, are the Fair Information Practice Principles ("FIPPs").[156] First developed in the United States in the early 1970s, the FIPPs are a data management regime to promote privacy, transparency, and accountability.[157] Rather than require specific policies, they are used as a framework to allow different entities to come up with their own individualized data management policies, depending on the needs and context of the data collection and use.[158] Multiple entities have created a list of FIPPs with a great deal of overlap (including the Organisation for Economic Cooperation and Development, the European Union, and Canada);[159] the U.S. has done so in different iterations as well.[160] The FIPPs are not an infallible framework — some critics have argued that they are not well suited to current information practices[161] — but they are widely accepted, and have been used consistently for over forty years.[162] Despite any shortcomings, they remain popular as a data management framework.

Many (though not all) of the proposed judicial reforms discussed in Part III — limitations on executive discretion, prescriptive limits on what data can be collected, a determination that the search is the only method of promoting the government's interest, and narrow tailoring — can be achieved through applying FIPPs principles to draft legislative or regulatory language, thus achieving

---

[156] *See, e.g.,* Memorandum 2008-01 from the U.S. Dep't of Homeland Sec. on Privacy Policy Guidance, Hugo Teufel III, Chief Privacy Officer, U.S. Dep't of Homeland Sec. (Dec. 29, 2008), https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf [https://perma.cc/HF62-W2M3] [hereinafter "DHS Memorandum"].

[157] Robert Gellman, *Fair Information Practices: A Basic History*, 1–6 (Apr. 10, 2017), https://bobgellman.com/rg-docs/rg-FIPshistory.pdf [https://perma.cc/SK44-6E6U].

[158] *See id.* at 38.

[159] *See id*. at 6–19.

[160] *See id.* at 19–37.

[161] *See, e.g.*, J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 113–18 (2008) (arguing that FIPPS "neglect[s] the very real costs of processing information and making a decision.").

[162] *See generally* Gellman, *supra* note 157 (outlining the consistent use of FIPPS since the 1970s).

through policy choices some of what previously had been restricted by jurisprudence.

It is perhaps optimistic to assume that that governmental entities will be more likely to use a FIPPs-based model when they are not required to. The agency capture arguments and resistance to regulations may make FIPPs adoption as unlikely as a change in judicial assessment of administrative searches. However, despite their limitations governmental entities *are* responsive to the concerns of the public and of businesses. Moreover, they can see which way the wind is blowing with regard to data collection and management, in particular the concerns of what happens to data stockpiled by private and public entities. Given the wide adoption of FIPPs by private companies, it would be prudent for governments to incorporate FIPPs into their data practices.

The below sections briefly touch on relevant FIPPs that may be used to achieve these ends, using the 2008 U.S. Department of Homeland Security ("DHS") instantiation.[163] DHS sets out the FIPPs as:

> • Transparency: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).
>
> • Individual Participation: DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.
>
> • Purpose Specification: DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
>
> • Data Minimization: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
>
> • Use Limitation: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.
>
> • Data Quality and Integrity: DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
>
> • Security: DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use,

[163] *See* DHS Memorandum, *supra* note 156, at 3–4. As a U.S. government agency, the DHS version of the FIPPs is particularly apt for the context discussed in this Article, as its framing may be more relevant to state and local agencies collecting data (versus other versions of the FIPPs promulgated by the White House or the OECD).

destruction, modification, or unintended or inappropriate disclosure.

• Accountability and Auditing: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.[164]

1. Purpose Specification

One of the most prominent FIPPs raised in policy discussions is the purpose specification, which in the DHS framing requires specific articulation of "the authority that permits the collection of [personally identifiable information, or PII]" and of "the purposes for which the PII is intended to be used."[165] By specifically articulating the authority allowing for collection and the purposes for which it is to be used, agencies can both demonstrate that the search is the sole effective method for pursuing its regulatory and oversight goals, as well as narrow the scope of a search and reduce the likelihood of overbroad, discretionary searches.

Purpose specification is helpful in the administrative search context as it can proactively allay concerns that regulatory searches are overbroad or limitless in their application. In many instances, when governmental entities announce new programs to collect information, civil society groups and advocates raise concerns that can impede the adoption of those programs.[166] By proactively explaining and limiting the situations in which data is collected and the purposes for which it is used, agencies can minimize the risk of negative feedback from the public.

Using purpose specification will also reinstate one of the initial limits of the administrative search doctrine: the requirement that searches be limited *ex ante* by a clearly defined statutory or regulatory regime.[167] Purpose specification provides a component of that regime by setting out precisely for what purposes the data is to be collected and under what authority. Similarly, purpose specification can also be useful in ensuring narrow tailoring. By explaining what the purpose is preemptively, the drafters of the search program will also necessarily evaluate that purpose against the ends employed, making it more difficult to draft a search that does not well fit within the stated goals.

---

[164] *Id.*

[165] *Id.* at 3.

[166] *See, e.g.*, Letter from Advocacy for Principled Action in Government et al., to Jonathan R. Cantor, Acting Chief Privacy Officer, U.S. Dep't of Homeland Sec. (Oct. 18, 2017), https://cdt.org/files/2017/10/Coalition-Letter-Opposing-DHS-Social-Media-Retention-.pdf [https://perma.cc/4GDF-CXEV].

[167] *See* Primus, *supra* note 7, at 267.

2. Use Limitation

The use limitation principle states that information should only be used "for the purpose(s) specified in the notice."[168] It also states that sharing of any information should also be for "a purpose compatible with the purpose for which the PII was collected."[169] Use limitations and purpose specifications go hand-in-hand: without both, neither is sufficient on its own to protect privacy.

Use limitations are crucial to allay fears of backdoor sharing of information among government agencies.[170] This sharing transfers information from one agency to another, giving the second agency access to information it may not have (or could not have) independently obtained. In this context, a government agency could obtain massive amounts of data through its regulatory and enforcement abilities, and potentially transmit it to other governmental entities (including criminal law enforcement) that would not otherwise have the authority or ability to access.

By including use limitations in regulatory programs that collect data, legislators and policymakers can mitigate concerns about how the data is used *beyond* in its initial collection. This would move closer to the administrative search requirement that searches be circumscribed by a statutory or regulatory regime. A codified, concrete use limitation would make explicit an element of the government's management regime for data collected from regulated entities. Enacting use limitations would also help to communicate that the proposed regulation is the narrowest search that the government could execute while still achieving its desired policy goals.

3. Data Security in Transmission and Storage

In an era of rampant data breaches[171] and man-in-the-middle attacks,[172] data

---

[168] DHS Memorandum, *supra* note 156, at 4.

[169] *Id.*

[170] *See, e.g.*, Hanni Fakhoury, *DEA and NSA Team Up to Share Intelligence, Leading to Secret Use of Surveillance in Ordinary Investigations*, ELEC. FRONTIER FOUND.: DEEPLINKS BLOG (Aug. 6, 2013), https://www.eff.org/deeplinks/2013/08/dea-and-nsa-team-intelligence-laundering [https://perma.cc/Y5LD-ZZJM] (explaining the practice of "parallel construction", whereby law enforcement agents are receiving information from the DEA that was originally obtained by the NSA for national security and terrorism use only).

[171] *See, e.g.,* Allen St. John, *Equifax Data Breach: What Consumers Need to Know*, CONSUMER REPORTS, https://www.consumerreports.org/privacy/what-consumers-need-to-know-about-the-equifax-data-breach/ [https://perma.cc/8YQN-NQDT] (last updated Sept. 21, 2017) (detailing the recent 2017 Equifax data breach, which included in potentially over 143 million social security numbers of consumers being compromised).

[172] *See, e.g.,* Seth Schoen & Eva Galperin, *Iranian Man-in-the-Middle Attack Against Google Demonstrates Dangerous Weakness of Certificate Authorities*, ELEC. FRONTIER FOUND.: DEEPLINKS BLOG (Aug. 29, 2011), https://www.eff.org/deeplinks/2011/08/iranian-

security is one of the most crucial FIPPs given the risk to privacy and security. Governmental entities are hardly immune to data breaches,[173] and given the broad abilities of agencies to collect data, ensuring the security of both transmitted and stored data is paramount, as discussed *supra* Section III.A. All government agencies should make security a priority and communicate that to the public. Security is especially important for regulatory agencies that collect consumer data, as the data the agency holds pertains to individuals and may include sensitive information and PII.

The DHS instantiation of the FIPPs is fairly broad, requiring that agencies create "appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure."[174] Because of the rapid changes in security standards, proactively prescribing specific security measures or routines in legislative or regulatory language would be counterproductive — an abundance of specificity would fail to keep pace with the evolution of data security best practices. Courts have recognized this need for flexibility,[175] citing with approval the Federal Trade Commission's guidance on data security that provided a checklist of practices that form an overall security plan.[176]

While legislators and regulators should not seek to provide an overly prescriptive data security regime, they should explicitly describe the broad considerations that both companies and regulators should keep in mind when designing such a regime in order to communicate to the public that data security is being considered proactively, rather than in response to security threats or breaches. Any modern statutory regime that mandated data transmission would include data security considerations as part of its privacy framework, and by voluntarily including security as part of a proposed statute or regulation,[177] governmental entities can follow the original guidelines for administrative searches that required a detailed statutory or regulatory regime.

4. Open Government Requests and De-Identification

While not an explicit component of the FIPPs, the issues surrounding de-

man-middle-attack-against-google [https://perma.cc/8UFA-Q7NX] (detailing a 2011 man-in-the-middle attack against Google).

[173] *See, e.g.,* Davis, supra note 154.

[174] DHS Memorandum, *supra* note 156, at 4.

[175] *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 243 (3d Cir. 2015) (citing FTC v. Bunte Bros., 312 U.S. 349, 353; Atl. Ref. Co. v. FTC, 381 U.S. 357, 367 (1965)).

[176] *Id.* at 256.

[177] *See, e.g.,* Administration Discussion Draft: Consumer Privacy Bill of Rights Act, § 105 (2015), https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf [https://perma.cc/VFE4-UH5J].

identification and re-identification of consumer records, especially when those records are released in response to open government requests, are crucial for legislators and regulators to keep in mind while crafting data mandates. These issues are especially prominent when open government requests compel the release of consumer records. The NYC TLC incident explains why, in an era when open data requests can unintentionally reveal sensitive information about individuals, proactively protecting records before such requests are received is a necessity.[178] While these consequences are not directly related to the administrative search doctrine, they *are* foreseeable. Governments should therefore work proactively to prevent inadvertent disclosure of the data that they collect.

Collection limitations may mitigate the dangers of re-identification, as discussed *supra* Section III.B.1. As the theory goes, the less data collected, the less likely that an analysis of a particular data set could lead to re-identifying particular individuals. To some degree this holds true in the regulatory context, but in order to fulfill the necessary regulatory functions of oversight and consumer protection, *some* data will necessarily need to be collected — including data that could, if un-redacted, lead to re-identification.

Therefore, instituting a program designed to formalize responses to open government requests is the most effective way to reduce the risk of re-identification. The DHS FIPPs nods to this concern in the Data Minimization principle, which states in part that PII should only be retained "for as long as is necessary to fulfill the specified purpose(s)."[179] The implication in this statement is that data should be eliminated when it is no longer necessary; any subsequent open government request would therefore fail to release that data, either intentionally or inadvertently.

Beyond data minimization, regulators should also attempt to preemptively determine what data categories will be redacted in response to public records requests, even if the data is still necessary for governmental purposes. For example, address level data may be necessary for oversight purposes, but there are few obvious needs to release data with that level of granularity to the public. Releasing ZIP code level information, by contrast, would both further open government needs (by allowing for public understanding of government action and also opening the door to private sector analysis of public data) while still protecting individual privacy.

Because individuals don't have the ability to challenge searches or data releases on the grounds of inadequate privacy protection,[180] government entities are effectively the only entities that can protect individuals from re-identification in open government releases. As a result, in order to most effectively pursue its

---

[178] *See supra* Introduction.

[179] DHS Memorandum, *supra* note 156, at 4.

[180] *See supra* Section I.C.

mission of protecting the public, the government should work proactively to define what data elements are released as a result of open data requests and what elements are redacted. Agencies, legislators, and the public each have a role to play in determining what data is collected, and how that data is released.

5. Applying the FIPPs to Administrative Searches

Taking these principles, states and localities can use the guidelines above to craft search programs that would more effectively balance the government's needs against the individual and business needs to protect sensitive information. Because of the wide variety of administrative searches authorized by statutes and regulations, any framework needs to be general enough for broad applicability, while specific enough to be effective. Indeed, one benefit of applying this on the state and local level would be the experimentation that necessarily takes place in our federalist system. Broad application of administrative searches would facilitate the determination of which styles of regulation and FIPPs application best balance the competing needs that administrative searches take into consideration.

CONCLUSION

The privacy risks from administrative searches are challenging to apprehend in the abstract. It takes incidents like the TLC re-identification mishap to fully see how and why overbroad government collection for regulation and civil enforcement can lead to privacy and security risks. We cannot view the TLC episode as more than just a random anecdote; when considered alongside the prevalence of data breaches, the possibilities of illicit sharing, and the sensitivity of the data collected, the current administrative search regime cannot be considered an adequate protection of privacy interests. This skepticism, though, may be only in the minds of scholars and privacy advocates. While this Article endeavors to persuade readers of the importance of overbroad administrative searches, the complexities of Fourth Amendment law may not be of interest to the public. What, then, might persuade the population?

There *are* signs that Americans have concerns about privacy.[181] Those concerns include the broad collection of information, the lack of control over its use, and the security of that data[182] — concerns that align with the FIPPs controls over collection, use, retention, access, and security.[183] Many Americans use services like Uber, Lyft, and Airbnb that collect significant amounts of private

[181] *See, e.g.,* Madden & Rainie, *supra* note 147 ("[A]mericans continue to express the belief that there should be greater limits on government surveillance programs.").

[182] *Id.*

[183] *See* discussion *supra* Sections III.B.1-3.

information about our daily lives, our habits, and our associates.[184] Those services are frequently the targets of administrative searches.[185] Americans' concerns, therefore, could be addressed through administrative search reform.

Yet just as fixing administrative searches would not be a silver bullet for addressing privacy shortfalls, other solutions would not — absent a legal reformulation of the administrative search doctrine — fully ameliorate the problems discussed in this Article. At its core, administrative searches are facilitated by private data collection, much like government surveillance. Some data collection is necessary for the functioning of services (it is difficult to imagine ridesharing apps working without collecting user location information) — but not all.

The debate over private data collection in the current digital economy seems to have been largely settled. While arguments for collection limitations still hold weight,[186] the core of the debate has moved on from the collection prong.[187] There is simply too much data being collected, with explicit or tacit consumer consent, to leave the role of privacy protectors in the hands of private companies. Companies frequently make their profits on the monetization of their customer data; that is the implicit bargain that allows for many free online services. Even those that charge or take commissions can hardly resist the promise of big data algorithms, consumer targeting, and longitudinal comparisons — tools that all require the pervasive collection of information from individuals. Business incentives, vis-à-vis individuals, are not well enough aligned to rely on for protecting individuals against government collection, whether it be on the regulatory, criminal law enforcement, or national security fronts.

Legislative and regulatory self-control is possible, as discussed *supra* Section III, but here too one may be skeptical, for similar reasons as those that apply to private collection. Data is simply too attractive a resource to pass up, even for governments. Moreover, the potential public benefits from the application of

[184] *See* Aaron Smith, *On-demand: Ride-hailing Apps*, PEW RES. CTR.: INTERNET & TECH. (May 19, 2016), http://www.pewinternet.org/2016/05/19/on-demand-ride-hailing-apps/ [https://perma.cc/A3UG-C3RZ] (evaluating the widespread use of "on-demand ride-hailing apps" such as Uber and Lyft); Aaron Smith, *Shared: Home-sharing Services*, PEW RES. CTR.: INTERNET & TECH. (May 19, 2016), http://www.pewinternet.org/2016/05/19/shared-home-sharing-services/ [https://perma.cc/T4NJ-23D9] (evaluating the widespread use of "home-sharing services" such as Airbnb).

[185] *See supra* Section II.B.

[186] *See, e.g.*, Justin Brookman & G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, *in* Big Data & Privacy: Workshop Paper Collection 11 (2013), https://fpf.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf [https://perma.cc/PL8V-8LQA].

[187] *See, e.g.,* Benjamin Wittes, *Databuse: Digital Privacy and the Mosaic*, BROOKINGS INST. (Apr. 1, 2011), https://www.brookings.edu/wp-content/uploads/2016/06/0401_databuse_wittes.pdf [https://perma.cc/7TV7-TKHZ].

corporate data are vast. One can imagine traffic management systems improved by Lyft and Uber data, or how Airbnb's records could help a city better implement urban planning goals. There are pitfalls to amassing data for a rainy day on the government side, particularly on the security end as data breaches continue. But those pitfalls may remain too abstract to spur any self-imposed change from state and local governments, both in the legislature and in agencies. While this Article suggests how and why governments should create their own limits on administrative searches, the political and practical realities do not fill one with confidence that governments will heed that call.

That leaves us, then, with the courts. A judicial solution would be welcome — the Supreme Court would do well to clarify the administrative search morass — but the appetite for doing so is uncertain.[188] As discussed *supra*, the Court explicitly declined in *Patel* to analyze any element of the Los Angeles city ordinance other than the pre-compliance review question.[189] But the door remains open to future challenges, especially as *Patel* endorsed the possibility of facial challenges to Fourth Amendment searches.[190]

The possibility of a facial challenge to an administrative search brought by Uber, Airbnb, or another technology company subject to such searches exists. Uber has waged an extensive campaign to resist regulations that it considers obstacles to its business practices, in some instances enlisting its users as advocates.[191] Airbnb has been the subject of ballot initiatives and has filed suit against cities over its data practices and reporting requirements.[192] It is conceivable, therefore, that one of these companies might decide that an administrative search created by a state or local government is too onerous and argue that it violates the administrative search doctrine. The success of such a challenge, and the willingness of the companies to pursue litigation through appeals is unclear. Recently, Airbnb settled a lawsuit regarding platform liability for individual user actions, which it had previously seemed to be committed to

[188] Primus, *supra* note 7, at 309-12.

[189] City of Los Angeles v. Patel, 135 S. Ct. 2443, 2454 (2015).

[190] *Id.* at 2447.

[191] Alison Griswold, *Uber Won New York*, SLATE (Nov. 18, 2015), http://www.slate.com/articles/business/moneybox/2015/11/uber_won_new_york_city_it_only_took_five_years.html [https://perma.cc/D5V3-XAJM]; Issie Lapowski, *Uber's New Fake Feature in NYC Derides Regulators*, WIRED (July 16, 2015, 2:55 PM), https://www.wired.com/2015/07/uber-de-blasio/ [https://perma.cc/44LR-LXEM].

[192] Cyrus Farivar, *Airbnb: We Shouldn't Have to Help San Francisco Enforce New Rental Law*, ARS TECHNICA (June 29, 2016, 6:30 AM), https://arstechnica.com/tech-policy/2016/06/airbnb-sues-san-francisco-over-short-term-rental-law-it-helped-create/ [https://perma.cc/MU5T-7L5R]; Carolyn Said, *Prop. F: S.F. Voters Reject Measure to Restrict Airbnb Rentals*, SFGATE, http://www.sfgate.com/bayarea/article/Prop-F-Measure-to-restrict-Airbnb-rentals-6609176.php [https://perma.cc/H8AL-KLB2] (last updated Nov. 4, 2015, 6:56 AM).

pursuing.[193] While regulatory fights may be important in terms of public messaging, appellate litigation is costly in both time and money.

Separate from potential administrative search challenges is the future of the third party doctrine. As discussed *supra* Section I.C, there has been some interest from Justice Sotomayor in revisiting the third party doctrine and its justifications in the current digital economy. In 2017, the Court granted review in *Carpenter v. United States*, a case involving government access to cell site location data.[194] Carpenter argues that the third party doctrine is particularly ill suited to modern technology,[195] potentially setting the stage for its modification by the Court. Predicting Supreme Court decisions is often a fool's errand, but one can certainly see interest from the Court in revisiting the third party doctrine by the fact that the case was granted certiorari at all.

Any modification to the third party doctrine would have drastic effects through Fourth Amendment jurisprudence, and certainly for the administrative search doctrine. Because administrative searches frequently involve data collected from consumers, they are intimately entangled with the third party doctrine. Any change to the privacy expectations or standing requirements for information shared with businesses could allow for stronger protections for individual data and more restricted administrative searches.

Or, it might not. Predicting *Carpenter* is a diverting thought experiment, as is brainstorming future litigation challenging administrative searches. But when examining the current state of the administrative search doctrine, it's hard not to fantasize about a better system. The situation at present — overbroad collection, a lack of privacy protections, vague justifications, and the dangers of data misuse — is fairly depressing to contemplate when set against the Fourth Amendment and its goals. Change to the administrative search doctrine is necessary; the only remaining questions are whether it comes from the courts or from governments — and when.

---

[193] *See* Katie Benner, *Airbnb Settles Lawsuit With Its Hometown, San Francisco*, N.Y. TIMES (May 1, 2017), https://www.nytimes.com/2017/05/01/technology/airbnb-san-francisco-settle-registration-lawsuit.html; Dan Levine & Heather Somerville, *Judge Rejects Airbnb's Bid to Halt San Francisco Ordinance*, REUTERS (Nov. 8, 2016, 4:55 PM), http://www.reuters.com/article/us-airbnb-sanfrancisco-ruling-idUSKBN1332OE [https://perma.cc/GCQ2-XG4M].

[194] United States v. Carpenter, 819 F.3d 880, 885 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (June 5, 2017) (No. 16-402); *see* Amy Howe, *The Justices Return to Cellphones and the Fourth Amendment: In Plain English*, SCOTUSBLOG (July 31, 2017, 10:57 AM), http://www.scotusblog.com/2017/07/justices-return-cellphones-fourth-amendment-plain-english/ [https://perma.cc/ZYK5-2GBP].

[195] Brief for Petitioner at 14–31, Carpenter v. United States, 137 S. Ct. 2211 (2017) (No. 16–402), https://www.aclu.org/sites/default/files/field_document/16-402_ts_1.pdf [https://perma.cc/Q5QY-V54Q].