No. 13-1175

In the Supreme Court of the United States

CITY OF LOS ANGELES, CALIFORNIA, PETITIONER

v.

NARANJIBHAI PATEL, ET AL.

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

BRIEF FOR GOOGLE INC. AS AMICUS CURIAE SUPPORTING RESPONDENTS

ERIC D. MILLER
Counsel of Record
ALBERT GIDARI, JR.
NICOLA C. MENALDO
PERKINS COIE LLP
1201 Third Ave., Suite 4900
Seattle, WA 98101
(206) 359-8000
emiller@perkinscoie.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases:

Cases—Continued: Page

Cases—Continued: Page

Constitution, statutes, and regulation:

Other authorities: Page

In the Supreme Court of the United States

No. 13-1175

CITY OF LOS ANGELES, CALIFORNIA, PETITIONER

v.

NARANJIBHAI PATEL, ET AL.

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

BRIEF FOR GOOGLE INC. AS AMICUS CURIAE SUPPORTING RESPONDENTS

INTEREST OF AMICUS CURIAE*

Google Inc. is a diversified technology company whose mission is to organize the world's information and make it universally accessible and useful. Google

* No counsel for a party authored this brief in whole or in part, and no person other than amicus or its counsel has made a monetary contribution intended to fund the preparation or submission of the brief. The parties have entered blanket consents to the filing of amicus briefs, and copies of their letters of consent are on file with the Clerk.

offers a variety of web-based products and services—including Search, Gmail, Google+, Maps, YouTube, and Blogger—that are used by people throughout the United States and around the world.

This case concerns the circumstances under which the government can compel a commercial entity to collect and retain personal information about its customers and turn that information over to police without an opportunity for pre-enforcement judicial review. Like most Internet-based service providers, Google collects information about its customers in order to offer its services. Google has a strong interest in protecting its customers' privacy and in preserving its ability to challenge unlawful government requests for information. Under the reasoning advanced by petitioner, the government could rely on a combination of the third-party doctrine and the administrative-search doctrine to compel a business—including, perhaps, an Internet-based service provider—to collect and retain information from its customers and then produce it without any opportunity for pre-compliance judicial review or notice to the affected customers. While this Court has approved administrative searches in a narrow class of cases, the Court should reject petitioner's reasoning, which would permit a scheme of broad-ranging warrantless searches to survive constitutional scrutiny based on little more than the government's interest in identifying the few users of a regulated service who might be engaged in criminal activity. Google files this brief to defend its users and to protect its own privacy rights in the information it collects by preserving its ability to oppose warrantless searches of its records.

SUMMARY OF ARGUMENT

This case involves a Los Angeles ordinance that requires hotel operators to collect personal information about their customers and to produce that information to the police upon request, without a warrant or any other opportunity for pre-execution judicial review. L.A., Cal., Mun. Code (LAMC) § 41.49 (2008). The court of appeals correctly held that the statute violates the Fourth Amendment.

The compelled disclosure of business records containing customers' personal information is a "search" under the Fourth Amendment because it interferes with constitutionally protected privacy interests of businesses and their customers. Accordingly, the warrant requirement applies unless the search qualifies for one of the Court's specifically delineated exceptions. Petitioner argues that Section 41.49 can be upheld under *New York* v. *Burger*, 482 U.S. 691 (1987), in which this Court held that a warrantless inspection scheme may be permissible in certain closely regulated industries. That is incorrect.

The *Burger* exception to the warrant requirement applies only to industries that are subject to such intensive regulation that businesses operating in those industries have a diminished expectation of privacy. Although petitioner identifies a hodgepodge of regulations governing hotels, it has not shown anything comparable to the kinds of regulations at issue in the cases in which this Court has upheld warrantless searches. Accepting petitioner's position would require a significant expansion of *Burger* that could affect many other industries. Internet and telecommunications services, for example, are also subject to

broad regulation, but that in no way diminishes the privacy interests of users of those services.

Nor can petitioner show that hotels lack an expectation of privacy in their customers' personal information. Petitioner denigrates that privacy interest, arguing that the information at issue is about the customers, not the hotels. But petitioner fails to appreciate that a business has a significant—and constitutionally protected—interest in protecting the privacy of information entrusted to it by its customers. Users of Google's services, for example, have their own privacy interests, but Google itself has a privacy interest in information about the identity of its users collected through registration for its services.

Even if *Burger* were applicable here, the searches conducted under Section 41.49 are unreasonable because they do not further any regulatory interest but instead serve only the general interest in crime control. In addition, petitioner has failed to show that warrantless searches are necessary to further the regulatory regime, and the administrative scheme of which they are a part does not include constitutionally adequate limits on officers' exercise of discretion in the field.

Finally, petitioner argues that facial challenges are impermissible in the Fourth Amendment context. But while facial challenges are disfavored, this Court has never held that they are categorically forbidden under the Fourth Amendment, and it should not do so here. Statutes like Section 41.49 cause an immediate, concrete injury to the businesses that are subject to them because they undermine customers' expectation that their personal information will be secure from disclo-

sure. The Court should not eliminate the ability of businesses to bring facial challenges against such statutes in appropriate circumstances.

ARGUMENT

A. Inspections under Section 41.49 are searches that are subject to the Fourth Amendment

Petitioner does not question that the inspections authorized by Section 41.49 constitute searches under the Fourth Amendment, and with good reason. The Fourth Amendment protects the right of the people to be secure in their "persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. Amend. IV. Under the Fourth Amendment, a "search" takes place "when government officers violate a person's 'reasonable expectation of privacy'" or when the government engages in a physical trespass upon the areas enumerated in the Amendment in order to obtain information. *United States* v. *Jones*, 132 S. Ct. 945, 950 (2012) (quoting *Katz* v. *United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)). The Ninth Circuit panel suggested (Pet. App. 39-44) that inspections under Section 41.49 do not infringe either a reasonable expectation of privacy or a possessory interest on the part of hotel owners, but that is incorrect.

Recognizing that the owner of a business, "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," this Court has held that businesses have a reasonable expectation of privacy in both their premises and their business records. *See* v. *City of Seattle*, 387 U.S. 541,

543 (1967); see *Dow Chem. Co.* v. *United States*, 476 U.S. 227, 236 (1986) ("Dow plainly has a reasonable, legitimate, and objective expectation of privacy within the interior of its covered buildings, and it is equally clear that expectation is one society is prepared to observe."); *Hale* v. *Henkel*, 201 U.S. 43, 76 (1906) (holding that an order for production of corporate papers constituted an unreasonable search). An entry on a hotel's premises to inspect a hotel's records of customer information infringes both of those interests.

In addition, a non-consensual inspection of hotel guest records is a common-law trespass. That is so whether the inspection involves flipping pages in a book, requiring a hotel operator to enter his credentials and log in to a password-protected computer, or simply turning a computer screen to view it from the other side of a desk. See Restatement (Second) of Torts § 217, at 417 (1965) (defining trespass to chattel as "intentionally * * * intermeddling with a chattel in the possession of another"); cf. *Arizona* v. *Hicks*, 480 U.S. 321, 324-325 (1987) (lifting turntable to examine serial numbers on bottom constitutes a search). Because hotel operators have a possessory interest in their business records, and an inspection under Section 41.49 trespasses upon that interest, the inspection constitutes a "search."

B. The Fourth Amendment generally requires pre-execution judicial review of searches like those conducted under Section 41.49

Petitioner argues that warrantless searches conducted under Section 41.49 comport with the Fourth Amendment because they are part of a "reasonable

administrative inspection scheme." Pet. Br. 29 (capitalization omitted); accord U.S. Br. 25. The asserted reasonableness of the searches, however, is not sufficient to make the searches consistent with the Fourth Amendment. This Court has adopted a presumption that searches must be authorized by warrants, and a warrantless search can be constitutional "only if it falls within a specific exception to the warrant requirement." *Riley* v. *California*, 134 S. Ct. 2473, 2482 (2014). The Court has applied the warrant requirement in the context of administrative searches of businesses such as those at issue here. *Camara* v. *Municipal Court*, 387 U.S. 523, 534 (1967); *See*, 387 U.S. at 546.

In *See*, the Court recognized an exception to the warrant requirement for administrative searches conducted under a scheme that limits the "discretion of the enforcement officer in the field" and that provides the target of the search with an opportunity to "obtain judicial review of the reasonableness of the demand prior to suffering penalties for refusing to comply." 387 U.S. at 545. Section 41.49 satisfies neither of those requirements. It requires that the hotel's guest records be "made available to *any* officer of the Los Angeles Police Department for inspection" without specifying any limits on which officers may demand to see the records, let alone how often they may do so and for what purpose. LAMC § 41.49(3)(a) (emphasis added). And the statute provides no opportunity for pre-execution judicial review. Compare LAMC § 41.49(3)(a), with *See*, 387 U.S. at 545 ("[T]he subpoenaed party may obtain judicial review of the reasona-

bleness of the demand prior to suffering penalties for refusing to comply.").

Recognizing that the searches here cannot be defended under *See*, petitioner relies instead on this Court's decision in *Burger*, which permitted an exception to the warrant requirement for situations of "'special need'" in "closely regulated" industries where "the privacy interests of the owner are weakened and the government interests in regulating particular businesses are concomitantly heightened." 482 U.S. at 702 (quoting *New Jersey* v. *T.L.O.*, 469 U.S. 325, 353 (1985) (Blackmun, J., concurring in the judgment)). Even in that context, a warrantless search is reasonable only if it meets three criteria: (1) "there must be a 'substantial' government interest that informs the regulatory scheme pursuant to which the inspection is made"; (2) "warrantless inspections must be 'necessary to further [the] regulatory scheme'"; and (3) the statutory scheme, "'in terms of the certainty and regularity of its application, [must] provid[e] a constitutionally adequate substitute for a warrant.'" *Id.* at 702-703 (quoting *Donovan* v. *Dewey*, 452 U.S. 594, 600, 603 (1981)) (brackets in original).

As shown below, *Burger*'s threshold requirement of a "closely regulated industry" is not satisfied here, but even if it were, the searches at issue would not be consistent with *Burger*.

C. The *Burger* exception for "closely regulated" industries is inapplicable here

Petitioner argues (Pet. Br. 31-36) that the hotel industry in Los Angeles is "closely regulated" for purposes of *Burger*. That is incorrect. Hotels have none

of the features that characterize the other industries this Court has described as "closely regulated," and extending *Burger* to them would weaken Fourth Amendment protections for a wide range of businesses.

1. This Court has identified only a few industries that are sufficiently pervasively regulated that businesses operating in them may be subjected to warrantless search regimes. The common feature of those industries is that they have "such a history of government oversight that no reasonable expectation of privacy could exist for a proprietor over the stock of such an enterprise." *Marshall* v. *Barlow's, Inc.*, 436 U.S. 307, 313 (1978) (citation omitted). As the Court explained in *Burger*, "the doctrine is essentially defined by 'the pervasiveness and regularity of the federal regulation' and the effect of such regulation upon an owner's expectation of privacy." 482 U.S. at 701 (quoting *Dewey*, 452 U.S. at 606).

"[T]he closely regulated industry of the type" at issue in those cases, the Court has explained, "is the exception," not the rule. *Barlow's*, 436 U.S. at 313; see *Huber* v. *New Jersey Dep't of Envtl. Prot.*, 131 S. Ct. 1308, 1308 (2011) (Alito, J., respecting the denial of certiorari) (describing *Burger* as "a limited exception to the Fourth Amendment's warrant requirement"). Indeed, this Court has identified only four types of businesses that qualify: licensed vendors of alcoholic beverages, *Colonnade Catering Corp.* v. *United States*, 397 U.S. 72 (1970); licensed firearms dealers, *United States* v. *Biswell*, 406 U.S. 311 (1972); mines and quarries, *Dewey*, *supra*; and automobile junkyards, *Burger*, *supra*. Each of those businesses poses

a potential danger to the public. See, *e.g.*, *Burger*, 482 U.S. at 709 ("Automobile junkyards and vehicle dismantlers provide the major market for stolen vehicles and vehicle parts."); *Dewey*, 452 U.S. at 602 (describing the mining industry as "among the most hazardous in the country"). More importantly, the pattern of regulation in each industry is such that a business could not reasonably expect privacy in its facilities or its records. See, *e.g.*, *Biswell*, 406 U.S. at 316 ("When a dealer chooses to engage in this pervasively regulated business and to accept a federal license, he does so with the knowledge that his business records, firearms, and ammunition will be subject to effective inspection.").

The Court has emphasized the narrowness of the exception by holding that simply being subject to the Occupational Safety and Health Act of 1970, 29 U.S.C. 651 *et seq.*—as most workplaces are—is not sufficient. *Barlow's*, 436 U.S. at 313-314. The "closely regulated" industries doctrine thus does not extend to businesses merely because they are subject to general economic or social legislation.

2. While hotels are subject to some regulations, petitioner has not come close to showing that the hotel industry resembles the industries that this Court has held to be subject to *Burger*. In arguing that hotels are closely regulated, petitioner relies principally (Pet. Br. 32) on Section 41.49 itself, noting that it requires hotels to record information and make it available to the police, that it carries penalties for violations, and that it informs hotels that the required records will be subject to periodic inspections. That argument, of course, is entirely circular. The same reasoning would

apply equally to any statute prescribing warrantless inspections, and it would make such a statute self-justifying. This Court has never accepted the existence of such a statute, by itself, as evidence that an industry is closely regulated.

Nor does the mandatory recording of the information do anything to diminish the hotel's privacy interest. Respondents have not challenged the provision of the statute that requires them to collect customer information. But requiring that a business collect and retain information from its customers does not make that information government property or otherwise interfere with a business's possessory interest in its own records. A contrary rule would mean that the government could circumvent the Fourth Amendment with respect to information a business already collects for its own purposes by mandating that it collect that information on behalf of the government. See, *e.g.*, *McLaughlin* v. *Kings Island*, 849 F.2d 990, 995 (6th Cir. 1988) ("[T]he concept of 'required records' is not synonymous with the absence of a privacy interest."); *Brock* v. *Emerson Elec. Co.*, 834 F.2d 994, 996 (11th Cir. 1987) (concluding that a business had a privacy interest in records that OSHA required it to compile).

Petitioner observes (Pet. Br. 32) that hotels must have a license and must display a registration certificate on the premises. But in Los Angeles, as in many other places, the same is true of all businesses. See LAMC § 21.09(a) (requiring that all entities doing business in Los Angeles obtain a Business Tax Registration Certificate, which must be "posted in a conspicuous place upon the premises at or from which the

business is conducted"). Petitioner does identify (Pet. Br. 33-34) a few regulatory requirements that appear to be hotel-specific. But many of them are health regulations—for example, the requirement that bed linens be changed between guests—that are similar to those imposed on other businesses. See, *e.g.*, Cal. Health & Safety Code § 114095 (West 2012) (cleaning requirements for restaurant utensils); Cal. Code Regs. tit. 16, § 979 (disinfection requirements for equipment used by cosmetologists). And the others—for example, the obligation not to refuse a guest without cause, and the prohibition on charging more than the posted rate—are characteristic of regulations imposed on public utilities, common carriers, and other places of public accommodation. See, *e.g.*, Cal. Civ. Code § 51(b) (West 2007 & Supp. 2015) (imposing nondiscrimination obligations on "all business establishments of every kind whatsoever"); Cal. Pub. Util. Code § 489(a) (West 2004) (requiring public utilities to file tariffs with the California Public Utilities Commission). If such general regulations were sufficient to invoke *Burger*, it is difficult to see what type of business would not qualify. See *Barlow's*, 436 U.S. at 314.

3. Significantly, none of the regulations identified by petitioner has any direct relationship to the information covered by Section 41.49. That is, the fact that hotels are subject to health regulations and obligations not to turn away customers does nothing to reduce a hotel owner's expectation of privacy in the sensitive customer information at issue here.

The hotel guest records required by Section 41.49 include guests' names and home addresses, as well as the names of anyone with whom a guest will be shar-

ing a hotel room. LAMC § 41.49(1). The records may also include license plate numbers, car make and model information, payment details, and individuals' driver's license or other identification numbers and expiration dates. *Ibid.*; LAMC § 41.49(4). That information is far more sensitive than that at issue in this Court's other cases involving closely regulated industries. The statute in *Burger*, for example, required junkyards to maintain records of vehicles and parts of vehicles coming into their possession, but it did not require them to collect or produce customer information like that at issue here. 482 U.S. at 694 n.1. In any event, information about vehicle sales is less likely to be regarded as private than information about where, when—and with whom—one has stayed at a hotel.

Businesses typically do not freely disclose sensitive, personally identifiable information about their customers to the general public. Customer personal information is a valuable, competitively sensitive resource that can help a business understand its customers and tailor services to their needs. Making that information available to the public would diminish its value and allow competitors to entice customers away from a business.

More importantly, the privacy of such information is important to a business's customers, and a business has an interest in protecting that information in order to retain the trust of its customers. That interest is "one that society is prepared to recognize as 'reasonable.'" *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Many commercial entities promise to limit disclosures of their customers' private information. See, *e.g.*,

Google Inc., *Privacy Policy*, http://www.google.com/policies/privacy/ (last visited Jan. 29, 2015) (explaining that "[w]e do not share personal information with companies, organizations and individuals outside of Google" except in certain enumerated circumstances). Indeed, in many circumstances, the law *requires* that a business safeguard customer information from disclosure and that it comply with representations it has made about the purposes for which such information will be collected, used, stored, or shared.

Both state and federal law reflect an understanding that personal information of the kind that hotels are required to collect under Section 41.49 is private and not to be disclosed to the general public. For example, California, like nearly every other State, requires that commercial entities provide notice to individuals in the event that a third party obtains unauthorized access to individuals' personal information. Cal. Civ. Code § 1798.82 (West 2009 & Supp. 2015). The definition of personal information includes a person's name when combined with driver's license information, which is information that Section 41.49 requires that hotels collect from some of their guests. Cal. Civ. Code § 1798.82(h)(1)(B) (West 2009 & Supp. 2015); cf. Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 *et seq.* (recognizing the privacy interest in driver's license information).

Similarly, federal law requires that businesses protect customers' personal information from unauthorized disclosure and that they comply with representations they have made to consumers about how they will use that personal information. In an assertion of its statutory authority to prohibit deceptive and unfair

trade practices, the Federal Trade Commission has brought more than 50 cases against companies that were alleged to have engaged in practices that put consumers' personal information at risk. Federal Trade Commission, *2014 Privacy and Data Security Update*, http://tinyurl.com/FTC-update; see 15 U.S.C. 45. The FTC has brought such an action against a hotel chain that it said had engaged in unfair and deceptive practices by allegedly failing to maintain reasonable and appropriate security for its guests' sensitive personal information, which included "names, addresses, email addresses, telephone numbers, payment card account numbers, expiration dates, and security codes." First Amended Complaint at 7, *FTC* v. *Wyndham Worldwide Corp.*, Dkt. No. 28, 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012).

4. Both petitioner and the United States fail to appreciate a hotel's interest in protecting its customers' information from unwarranted government inspection. As the United States puts it (U.S. Br. 29), hotels "have little privacy interest in the required information" because "[g]uests themselves have no reasonable expectation of privacy in the information recorded by the hotel operator." That reasoning relies on the third-party doctrine, which assumes that a person has no Fourth Amendment protected interest in information exposed to a third party. *Smith* v. *Maryland*, 442 U.S. 735, 743-744 (1979); *United States* v. *Miller*, 425 U.S. 435, 442-443 (1976). As Justice Sotomayor has suggested, however, that interpretation of the Fourth Amendment should be reconsidered because in government surveillance cases it "is ill suited to the digital age, in which people reveal a great deal of infor-

mation about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring); see *ibid.* (expressing "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 even if guests lack a constitutionally protected privacy interest in information they have been compelled to disclose to a hotel, it does not follow, as petitioner argues, that the *hotel* lacks such an interest. Pet. Br. 52 ("A register of guests' names, addresses, and home license plate numbers is not highly personal information *about the hotel*."). To the contrary, if guests are unable to assert their own privacy interests, that serves to heighten the hotel's interest because only the hotel has the ability to bring a legal challenge to protect the information from government intrusion.

The implications of petitioner's reasoning are sweeping. Under petitioner's theory, if the government wishes to collect sensitive information about the customers of a business, it need only compel the business to collect that information from the customers. Then, as a result of the third-party doctrine, the customers will cease to have a reasonable expectation of privacy in that information; and according to petitioner, the business will have no privacy interest in that information either. The government could use that analysis to justify warrantless collection of information from the customers of many types of businesses, including electronic communications service providers. Criminals may use email to facilitate crimes

just as people may use hotels to engage in prostitution, but both Google and its users have an interest in protecting the identify of users of the service (and Google would also argue against compelled registration of email users).

Neither the courts nor Congress have accepted petitioner's reasoning. See Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (prohibiting providers from disclosing certain customer communications and records to law enforcement, except when the disclosure is authorized by a subpoena, a court order, or a warrant). A business's interest in protecting its customer information is appropriately viewed as a privacy interest, and it is one that can be invoked by a business to oppose a search of that information. In the circumstances of this case, that interest is significant, and it is undiminished by the regulations that petitioner and the United States have identified. The *Burger* exception to the requirement of pre-execution judicial review is inapplicable here.

D. Searches conducted under Section 41.49 are not consistent with *Burger*

1. Even in a closely regulated industry, *Burger* allows a regime of warrantless searches only when "there [is] a substantial government interest that informs the regulatory scheme pursuant to which the inspection is made." 482 U.S. at 702 (internal quotation marks omitted). That interest must be a "special need[]" that is something other than "the normal need for law enforcement." *Ashcroft* v. *al-Kidd*, 131 S. Ct. 2074, 2081 (2011) (quoting *Vernonia Sch. Dist. 47J* v. *Acton*, 515 U.S. 646, 653 (1995)); see *Skinner* v. *Rail-*

way Labor Execs. Ass'n, 489 U.S. 602, 619-620 (1989) (identifying *Burger* as an example of a special-needs case). As the Court explained in *Ferguson* v. *City of Charleston*, the Court in *Burger* "relied on the 'plain administrative purposes' of the scheme to reject the contention that the statute was in fact 'designed to gather evidence to enable convictions under the penal laws,'" and it upheld the inspection scheme only because "[t]he discovery of evidence of other violations would have been merely incidental to the purposes of the administrative search." 532 U.S. 67, 83 n.21 (2001) (quoting *Burger*, 482 U.S. at 715).

The principal government interest cited by petitioner (Pet. Br. 37) is that of ensuring that hotel operators maintain registers that accurately identify their guests in order to deter criminal activities that allegedly proliferate in an environment of anonymity. That is simply a law-enforcement interest under another name. The desire to eliminate anonymity does not give rise to a legitimate interest in coopting commercial businesses to operate as recordkeepers for future law enforcement investigations. Other industries and services, including telecommunications and Internet services, enable anonymous commercial activity. Some users exploit that anonymity for criminal purposes; the vast majority use it for legitimate, socially valuable purposes. See *McIntyre* v. *Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995) (discussing the value of anonymous speech). At all events, the supposed government interest in eliminating anonymity would not justify a scheme of warrantless searches of Internet businesses, and it can no more justify the scheme at issue here.

The United States argues (U.S. Br. 27) that "[i]nspection of the records enables police to determine swiftly whether a person is staying at a particular hotel" because "police can demand to inspect the register without having to seek a court order, issue a subpoena, or face litigation delays before compliance." In some cases, such searches could be justified on the basis of exigent circumstances. In the absence of genuine exigency, however, they cannot be justified under *Burger* on the ground that they would facilitate "general crime control." *City of Indianapolis* v. *Edmond*, 531 U.S. 32, 43 (2000).

2. Petitioner also has not shown that the warrantless inspections permitted by Section 41.49 are "necessary to further [the] regulatory scheme." *Burger*, 482 U.S. at 702 (quoting *Dewey*, 452 U.S. at 600) (brackets in original). All of the cases in which this Court has applied the *Burger* exception to the warrant requirement have involved industries that either are permeated with criminal activity or offer services or products that are inherently dangerous. See, *e.g.*, *id.* at 709 (explaining the relationship between junkyards and automobile theft). Petitioner cites the problems attendant to hourly motels in certain areas of Los Angeles (Pet. Br. 5-6), but it provides no evidence as to what proportion of all hotels suffer from those problems, and it offers no rationale for why hotels that do not offer hourly rates should require the intrusive spot checks contemplated under the ordinance. That criminal activity takes place at a subset of a type of business does not justify warrantless searches of the entire industry. The statute is far broader than necessary to accomplish the government's purpose.

3. Section 41.49 also fails to satisfy *Burger*'s requirement of appropriate safeguards as to "time, place, and scope * * * to place appropriate restraints upon the discretion of the inspecting officers." 482 U.S. at 711 (internal quotation marks and citation omitted). As respondent observes (Resp. Br. 41), the statute imposes no meaningful constraint on officers' discretion as to which hotels to search and how often to do so. Petitioner argues (Pet. Br. 39-40) that the element of surprise is important to ensure that hotel operators do not have an opportunity to falsify their records. Even if that were true, petitioner does not explain why surprise could not be achieved in the context of a regime that limited the discretion of individual officers as to who and where to search. The failure to provide any such limits creates the possibility of arbitrary or discriminatory enforcement and makes the statute inconsistent with *Burger*.

E. The court of appeals properly entertained a facial challenge to Section 41.49

A facial challenge to a statute is permitted when "no set of circumstances exists under which the Act would be valid," *United States* v. *Salerno*, 481 U.S. 739, 745 (1987), or the act lacks a "plainly legitimate sweep," *United States* v. *Stevens*, 559 U.S. 460, 473 (2010) (quoting *Washington State Grange* v. *Washington State Republican Party*, 552 U.S. 442, 449 n.6 (2008)). Those standards are demanding, but the court of appeals correctly determined that they are satisfied here.

1. Petitioner relies (Pet. Br. 23-24) on *Sibron* v. *New York*, 392 U.S. 40 (1968), for the proposition that

facial challenges are categorically prohibited in the Fourth Amendment context. Its reliance on that case is misplaced.

In *Sibron*, the Court stated that the "constitutional validity of a warrantless search is pre-eminently the sort of question which can only be decided in the concrete factual context of the individual case." *Id.* at 59. That statement does not mean that a Fourth Amendment facial challenge is never permitted, and in fact the Court has entertained such challenges both before and after *Sibron*. See, *e.g.*, *Berger* v. *New York*, 388 U.S. 41, 55 (1967) ("[T]he statute is deficient on its face[.]"); *Barlow's*, 436 U.S. at 325 (declaring inspection statute "unconstitutional insofar as it purports to authorize inspections without warrant or its equivalent"); see also *Skinner*, 489 U.S. at 614 (considering a "facial challenge" to "breath and urine tests required by private railroads").

Sibron involved a statute that permitted police to stop a person upon reasonable suspicion of criminal activity, and to search that person for dangerous weapons if the officer suspected he was in danger. 392 U.S. at 43-44. The Court determined that the statute was unconstitutional as applied to one of the criminal defendants in the case, but not the other, and stated that it would not invalidate the statute as a whole because "warrantless searches" of the type at issue were "pre-eminently" the kinds of searches that could only be decided within the context of their specific factual circumstances. *Id.* at 59. In so holding, the Court expressly distinguished *Berger*, which held that a New York law that established a procedure for issuing search warrants for electronic eavesdropping failed to

incorporate the safeguards required under the Constitution. *Ibid.* The constitutional validity of the statute at issue in *Sibron*, the Court explained, was "quite different from the question of the adequacy of the procedural safeguards written into a statute which purports to authorize the issuance of search warrants in certain circumstances." *Ibid.* That discussion makes clear that a facial challenge such as this one, which turns in part on whether there are sufficient procedural safeguards in Section 41.49, is still permissible.

2. A prohibition on facial Fourth Amendment challenges would be particularly inappropriate in the context of searches of third-party information. A statute that authorizes warrantless searches of a business's customer information leads consumers to believe that they should not trust that type of business with sensitive information. The mere existence of such a statute thus injures businesses that are subject to it, even before it is enforced against them. As an example, the 2013 revelations by Edward Snowden about warrantless Internet searches appear to have affected consumers' willingness to conduct activities online. See Amrita Jayakumar, *Americans say they're shopping less online. Blame the NSA*, Wash. Post (Apr. 2, 2014), http://tinyurl.com/wp14-04-02 (in a survey, 26% of people said they are engaging in less online shopping and banking since the revelation of the government's widespread surveillance programs); Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. Times (Mar. 21, 2014), http://tinyurl.com/nyt14-03-21 (reporting that losses to the cloud-computing industry following the Snowden revelations could range from $35 billion to $180 billion).

In the Fourth Amendment context, therefore, unconstitutional legislation can cause an immediate injury to regulated parties that is apparent without "specula[ing] about 'hypothetical' or 'imaginary' cases." *Washington State Grange*, 552 U.S. at 450. The concreteness and immediacy of that injury make it appropriate to permit the affected businesses to challenge the law on its face. Cf. *Broadrick* v. *Oklahoma*, 413 U.S. 601, 611 (1973) (explaining that the prohibition on suits challenging the application of a law to others is relaxed "where individuals not parties to a particular suit stand to lose by its outcome and yet have no effective avenue of preserving their rights themselves").

3. On the merits, Section 41.49 is facially invalid because it is unconstitutional in all of its applications. As explained above, the validity of warrantless searches depends on whether they are conducted under a statutory scheme that satisfies the requirements of *Burger*. Because Section 41.49 is deficient, all of the searches conducted under it are invalid. Petitioner's suggestions to the contrary (Pet. Br. 19-20)—for example, that the police might obtain a warrant for the required information, that an exigency might justify the inspection, or that the hotel owner might disclose the information to the public without the compulsion of the statute—are not examples of situations in which the statute would be valid; they are examples of situations in which the statute might not need to be used. As such, they are insufficient to demonstrate that the law has valid applications.

CONCLUSION

The judgment of the court of appeals should be affirmed.

Respectfully submitted.

ERIC D. MILLER
Counsel of Record
ALBERT GIDARI, JR.
NICOLA C. MENALDO
PERKINS COIE LLP
1201 Third Ave., Suite 4900
Seattle, WA 98101
(206) 359-8000
emiller@perkinscoie.com

JANUARY 2015