

NetChoice *Promoting Convenience, Choice, and Commerce on The Net*

Carl Szabo, Vice President and General Counsel
1401 K St NW, Suite 502
Washington, DC 20005
202-420-7485
www.netchoice.org



May 15, 2019

Rep. Michael Coyne Turzai, Speaker
House of Representatives
Harrisburg, Pennsylvania

RE: **Opposition to HB 787 – Exposing Pennsylvaniaian privacy**

Dear Speaker Turzai and members of the House,

We ask that you not move forward with HB 787.

Government efforts, like those in HB 787, to force Short-term Rental (STR) platforms to disclose data to the government are unconstitutional on several privacy protecting fronts, including the 4th Amendment and the Stored Communications Act.

We outline the legal problems with such an approach below and welcome further conversation on the matter. We do, however, agree with reasonable requirements for STR hosts and regularly advocate for such requirements.

Benefits to your constituents of short-term rentals

STR services provide necessary income to many of your constituents. Over 52 percent of hosts nationwide live in low-to-moderate income households. More than 48 percent of the income hosts earn through certain short-term rental services is used to cover household expenses.

Consider, for example, families coming from across the country for graduation ceremonies at University of Pennsylvania. STR services allow constituents to earn income by sharing their homes.

The presence of STR services also brings new money into areas under-served by hotels. Historically, travelers are not likely to encounter businesses in these under-served parts of Pennsylvania.

Conversely, guests who stay in under-served areas via STR services, bring income to nearby restaurants, grocery stores, and businesses.

HB 787's forced disclosure of STR platform records illegally exposes the privacy of Pennsylvania residents to government employees and potentially law enforcement

The 4th Amendment of the US Constitution protects Pennsylvania citizens from unlawful search and seizure and is a core privacy protection.

But HB 787's forced disclosure of STR platform records ignores this privacy protection and instead requires platforms to disclose records and information about hosts to government employees and

potentially law enforcement. And this disclosure does not require the state’s employees to first obtain a warrant.

This could not only expose the operating procedures and income of businesses but also expose the privacy of Pennsylvania residents using the platform and people staying in Pennsylvania homes.

New York City attempted this same effort and was swiftly enjoined from taking effect.

In the court’s decision against the New York City’s ordinance, the court said:

The Court, therefore, holds that the Ordinance implicates the Fourth Amendment. It puts in place a search and seizure regime that implicates protected privacy interests of the “booking services” whose user records must be produced monthly to the OSE. The Court now considers whether this regime satisfies the Fourth Amendment.

...

[T]he scale of the production that the Ordinance compels each booking service to make is breathtaking.¹

In outlining the dangers of disclosure requirements like this, the court worried:

By the City’s logic, a City Council presumably could also compel (1) all online auction services monthly to produce all records of sales by New York City residents, on the premise that such records could assist in finding sellers who evaded capital gain taxes on sales of collectibles; (2) all medical providers monthly to produce all patient records for care rendered in New York City, on the premise that such records could assist in finding instances in which users engaged in up-coding and other health-care fraud; and (3) all credit card companies monthly to produce all records of expenditures in New York restaurants, on the premise that such records could assist in identifying instances in which commercial income was not reported to tax authorities.²

Pennsylvania even just as unconstitutional as New York City’s ordinance.

Required disclosure of STR platform’s stored names and addresses of Pennsylvania residents to government employees and potentially law enforcement.

The US Supreme Court and the Hotel industry say that mandated disclosure is unconstitutional

When the city of Los Angeles demanded a hotel’s proprietary business records, the hotel industry fought back in court – ultimately winning at the US Supreme Court in a decision written by Justice Sotomayor in *Los Angeles v Patel*, 135 S. Ct. 2443 (2015).

In its opinion the US Supreme Court said:

The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” It further provides that “no Warrants shall issue, but upon probable cause.” Based on this constitutional text, the Court has repeatedly held that “searches conducted out- side the judicial process, without prior approval by [a] judge or [a] magistrate

¹ *Airbnb v. City of New York, HomeAway v. City of New York*, 18 Civ. 7712 (S.D.N.Y. Jan. 3, 2019).

² *Id.*

[judge], are per se unreasonable . . . subject only to a few specifically established and well- delineated exceptions.”³

The Respondent hotel operator said in its brief:

The Fourth Amendment generally requires a warrant to address the Founders’ fundamental “concern about giving police officers unbridled discretion to rummage at will among a person’s private effects.” *Arizona v. Gant*, 556 U.S. 332, 345 (2009). The warrant requirement “interpose[s] a neutral magistrate between the citizen and the law enforcement officer.” *Nat’l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 667 (1989). In addition, by requiring that the warrant “particularly describe[] the place to be searched, and the persons or things to be seized,” the Fourth Amendment seeks to safeguard against “exploratory rummaging in [that] person’s belongings,” including her papers. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971) (plurality). In combination, these requirements ensure that the decision whether, and how, to invade a person’s privacy is not made by officers in the field “engaged in the often competitive enterprise of ferreting out crime.” *Johnson v. United States*, 333 U.S. 10, 14 (1948); *see also United States v. U.S. Dist. Court*, 407 U.S. 297, 317 (1972).

In an amicus brief from the Asian American Hotel Operators Association, the hotel industry argued:

“The City should not be able to destroy the hoteliers’ property or interest in this information merely by requiring that some of it be collected.”

To protect this court ruling, we could see the hotel industry opposing such requirements on STR platforms to disclose business records. And if such a requirement is passed, Pennsylvania would likely see a similar court outcome.

HB 787’s forced disclosure of records by a STR platform violates federal privacy laws

The Federal Stored Communications Act (SCA) was designed to prevent the voluntary or compelled disclosure of stored communications to the government. This precluded disclosure to federal, state, city, and other municipal governments.

The SCA states:

(a) Prohibitions. — Except as provided in subsection (b) or (c)—

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—⁴

[unless complying with the following provisions for disclosure to a governmental entity]

Contents of Wire or Electronic Communications in a Remote Computing Service.—

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in

³ *Los Angeles v Patel*, 135 S. Ct. 2443 (2015).

⁴ 18 U.S.C. § 2702(a)

the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.⁵

As is clear from the SCA, either a warrant, administrative subpoena, or court order is required prior to compelled disclosure of stored communications by a “remote computing service.” Note also, that the 6th Cir in *United States v. Warshak*⁶ ruled that a warrant is required for government mandated disclosure of contents – not an administrative subpoena.

And for purposes of the SCA, names of hosts, lengths of stays, addresses, or any other information generated by users of the service and stored by HomeAway or Airbnb is covered by SCA.

The Congressional records for SCA state the purpose of the SCA is specifically to prevent governmentally forced disclosures such as mandating disclosure of host or visitor records kept by an STR platform. In particular, the SCA’s congressional record states:

“In the absence of market discipline, there is no presumption that the government will strike an appropriate balance between disclosure and confidentiality. And the enormous power of the government makes the potential consequences of its snooping far more ominous than those of . . . a private individual or firm.’ Posner, *Privacy in the Supreme Court*, 1979 Sup. Ct. Rev. 173, 176 (1979).

...

if Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Additional legal protection is necessary to ensure the continued vitality of the Fourth Amendment.”⁷

Clearly the express language of the SCA and the legislative intent preclude any forced disclosure of records kept by an STR platform.

Privacy invasion of Pennsylvania residents from the HB 787’s forced disclosure of STR platform records

Legal arguments aside, mandating STR platforms disclose data to the government grants virtually any Pennsylvania public employee access to private information of Pennsylvania residents. As you can imagine, this provides an easily abused resource of information about your constituents and guests staying in the state.

We’ve seen high compliance rates when localities create reasonable registration and regulation for STRs. A thoughtful approach to home-sharing by creating a registration process would benefit all Pennsylvania

⁵ 18 U.S.C. § 2703(b).

⁶ *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

⁷ Congressional Record of Electronic Communications Act, Pub.L. 99–508 (1986).

residents. We welcome the opportunity to work with you on reasonable regulations that allow all to prosper.

Sincerely,

Carl Szabo

Vice President and General Counsel, NetChoice

NetChoice is a trade association of e-Commerce and online businesses. www.netchoice.org