# IDENTICAL FACTS, OPPOSITE RULINGS: *CHOICE HOTELS*, *HICKORY FARMS*, AND THE ADVENT OF WEBSITE "PEN REGISTERS"

*Michael M. Epstein, J.D., Ph.D.*[*]



## INTRODUCTION: HOW TWO RULINGS, WEEKS APART, ILLUSTRATE A DIVIDE IN PRIVACY LAW

On April 3, 2024, Judge Cherol J. Nellon of the Los Angeles Superior Court ruled that a plaintiff could sue Choice Hotels International, a hotel chain, for using tracking software on its website without the plaintiff's consent.[1] Weeks earlier, on March 13, 2024, a different Los Angeles Superior Court Judge, Stephen P.

* Professor of Law and Supervising Editor of the Journal of International Media & Entertainment Law, Southwestern Law School. Director, Amicus Project at Southwestern Law School. Director, Entertainment and Media Law Concentration, Southwestern Law School. My thanks to Alexandra E. Kerecman for her research assistance.

[1]Min. Order at 3, *Levings v. Choice Hotels Int'l, Inc.*, No. 23STCV28359 (Cal. Super. Ct., Los Angeles Co.).

Pfahler, dismissed an almost identical claim against a website operated by Hickory Farms LLC, a food retailer.[2] In both cases, plaintiffs alleged that the websites' use of tracking software without first obtaining their consent violated California Penal Code § 628.51, which bans the use of "pen registers," a privacy law that dates to the landline telephone age.[3]

In issuing these opposite rulings, the two judges disagreed about a fundamental issue at the intersection of privacy and technology: should a privacy protection codified to address wrongdoing in one medium be extended to a functionally equivalent wrongdoing in a different medium? In *Choice Hotels*, the court thought that the answer to this question may be yes. In *Hickory Farms*, the bench came to the opposite conclusion. This article reviews the two rulings in an effort to determine which judge has the better of the two arguments.

## I. THE CALIFORNIA PEN REGISTER STATUTE

The California Penal Code chapter relevant to *Choice Hotels* and *Hickory Farms* defines a pen register as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication."[4] However, the penal code clarifies that a pen register is not:

> a device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider, or a device or process used by a provider or customer of a wire communication service for cost accounting or other similar purposes in the ordinary course of its business.[5]

---

[2] Min. Order at 3, 5, *Licea v. Hickory Farms LLC*, No. 23STCV26148 (Cal. Super. Ct., Los Angeles Co.).

[3] Levings Compl. 2; First Am. Compl. at 2, *Licea v. Hickory Farms LLC*, No. 23STCV26148 (Cal. Super. Ct., Los Angeles Co.).

[4] CAL. PENAL CODE § 638.50(b) (Deering 2024).

[5] *Id.*

Pen registers, initially developed for telephone communications, have now extended their utility to internet communications. This longstanding historical association with landline telephony is understandable given the more recent advent of the internet. The U.S. Supreme Court in 1977 defined a pen register as "a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released."[6] These mechanical devices logged the electrical impulses on paper tape, disconnecting as soon as the number was dialed, without relaying information such as the contents of the call or even if the call was answered.[7]

The Supreme Court ruled that there is no expectation of privacy regarding the numbers dialed on a telephone recorded by a pen register.[8] The rationale included the notion that consumers understand they must voluntarily provide the telephone number they wish to dial to the telephone company to place a call.[9] Additionally, the Court noted that telephone users are aware that telephone companies record dialed numbers, as evidenced by itemized bills, especially for long-distance calls.[10]

In 1986, Congress passed the Electronic Communications Privacy Act (ECPA) to restrict the use of pen registers and wiretapping devices, mandating court orders for their usage.[11] Courts were to grant these orders if law enforcement officials demonstrated that the information collected would likely be relevant to a criminal investigation.[12] The ECPA did not require courts to conduct an independent investigation before granting

---

[6] United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977) (appearing to adopt a definition stemming from the 7th Circuit Court of Appeals in United States v. Dote, 371 F.2d 176, 178 (7th Cir. 1966)).

[7] Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949, 982-83 (1996) (quoting *Dote*, 371 F.2d at 178).

[8] Smith v. Maryland, 442 U.S. 735, 741-44 (1979).

[9] *Id.*

[10] *Id.*

[11] Freiwald, *supra* note 7, at 969, 972.

[12] *Id.* at 972 (explaining that Congress made this decision to abide by the Supreme Court's ruling in Smith v. Maryland); Rich Haglund, *Applying Pen Register and Trap and Trace Devices to Internet Communications: As Technology Changes, is Congress or the Supreme Court Best-Suited to Protect Fourth Amendment Expectations of Privacy?*, 5 VAND. J. ENT. L. & PRAC. 137, 140 (2003).

such orders.[13] The USA PATRIOT Act of 2001 amended the ECPA's definition of pen register to encompass both wire and electronic communications.[14] According to the Department of Justice in 2005, pen registers can collect non-content electronic communication information, such as IP addresses, email senders, and recipients.[15]

However, the evolution of electronic communication technology has blurred the lines between content and non-content information, merging them within metadata. This convergence, such as a URL containing specific webpage details or user actions, complicates the legality of using pen registers without violating privacy laws.[16] The courts are only beginning to address these nuanced issues.

## II. THE CASES: LEVINGS V. CHOICE HOTELS INT'L, INC. AND LICEA V. HICKORY FARMS LLC

### *A. Levings v. Choice Hotels Int'l, Inc.*

Plaintiff Levings, a California "consumer privacy advocate," filed suit on November 20, 2023, alleging that the defendant caused economic and intangible damages by installing a pen register on the plaintiff's laptop after visiting the defendant's website earlier in the year.[17] The defendant, Choice Hotels International, a Delaware-based corporation, operates a website facilitating hotel bookings in LA County and nationwide.[18] California's Civil Procedure and Penal Codes permit the plaintiff to sue the out-of-state defendant under the long-arm statute because of the impact of the alleged misconduct on California residents.[19]

The plaintiff did not detail how the pen register was downloaded, only that it occurred after visiting the defendant's website.[20] The pen register allegedly enabled the defendant to

---

[13] *See* Freiwald, *supra* note 7, at 986-89.

[14] Haglund, *supra* note 12, at 140.

[15] Steven M. Bellovin et al., *It's too Complicated: How the Internet Upends* Katz, Smith, *and Electronic Surveillance Law*, 30 HARV. J. L. & TECH. 1, 62-63 (2016).

[16] *Id.* at 73-75.

[17] Levings Compl. 2.

[18] *Id.* at 3.

[19] *Id.* at 2.

[20] *Id.* at 4-6.

engage in identity resolution, gathering private information such as the plaintiff's full name, address, voter registration status, employment information, and familial relations.[21] The plaintiff claims that this constituted a violation of California Penal Code Sections 502(j) and 638.51.[22]

Section 502(j) stipulates that accessing a computer from another jurisdiction is equivalent to accessing it within each jurisdiction.[23] Section 638.51(a) prohibits installing or using a pen register or trap and trace device without a court order.[24] The plaintiff emphasized the protection of private information under California law and cited a Ninth Circuit case permitting suits against Facebook for tracking users' browsing history on third-party websites.[25] The plaintiff sought damages and cessation of the pen register's use, and threatened to amend the complaint to include more plaintiffs if the defendant did not comply.[26]

On February 16, 2024, the defendant demurred, arguing for dismissal without leave to amend on two grounds: (1) insufficient factual support for the claim, asserting that the plaintiff's complaint lacked specific allegations of how the pen register was installed, and (2) the plaintiff consented to the pen register's installation by voluntarily visiting the website.[27] The defendant cited Section 638.51(b), which allows pen register installation with user consent.[28]

Judge Nellon denied the demurrer on April 3, 2024, allowing the case to move forward.[29]

---

[21] *Id.* at 5.

[22] *Id.* at 2, 6.

[23] CAL. PENAL CODE § 502(j) (Deering 2024).

[24] CAL. PENAL CODE § 638.51(a) (Deering 2024).

[25] Levings Compl. 3. *See* Davis v. Facebook, Inc. (In re Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 599 (9th Cir. 2020).

[26] *Id.* at 6.

[27] Def.'s Notice of Dem. and Dem. to Compl.; Mem. of P. & A. in Supp. Thereof at 6, 9-10, *Levings v. Choice Hotels Int'l, Inc.*, No. 23STCV28359 (Cal. Super. Ct., Los Angeles Co.).

[28] CAL. PENAL CODE § 638.51(b) (Deering 2024).

[29] Min. Order at 3, *Levings v. Choice Hotels Int'l, Inc.*, No. 23STCV28359 (Cal. Super. Ct., Los Angeles Co.).

### *B. Licea v. Hickory Farms LLC*

Filed on December 4, 2023, the plaintiff, also a "consumer privacy advocate," alleged economic and intangible damages from the defendant's installation of pen register and trap and trace software on the plaintiff's device after visiting the defendant's website.[30] The defendant, an Illinois-based retailer incorporated in Delaware, operates a nationwide website.[31] The plaintiff's standing and ability to sue mirrored *Choice Hotels*.[32]

The plaintiff alleged violations of Penal Code Sections 502(j) and 638.51, claiming the software facilitated identity resolution.[33] As in *Choice Hotels*, the plaintiff provided scant details on the software installation.[34]

On January 8, 2024, the defendant demurred on three grounds: (1) lack of sufficient facts to support the allegation, arguing that the plaintiff's claims did not meet the legal definitions of pen register or trap and trace software; (2) the plaintiff's consent by voluntarily visiting the website, similar to the defense in *Choice Hotels*; and (3) the absence of claimed damages or injuries warranting legal remedy.[35]

Judge Pfahler granted the demurrer with leave to amend on March 13, 2024, effectively dismissing the case.[36]

## III. ANALYSIS: *HICKORY FARMS* OFFERS A STRONGER ARGUMENT

In *Choice Hotels*, the court determined that a demurrer was not appropriate. The court found that the plaintiff had sufficiently alleged facts to support the claim that the defendant installed a pen register on the plaintiff's laptop by pleading the proper ultimate

---

[30] First Am. Compl. at 2, *Licea v. Hickory Farms LLC*, No. 23STCV26148 (Cal. Super. Ct., Los Angeles Co.).

[31] *Id. at 3.*

[32] *Id.* at 2.

[33] *Id. at 6-7.*

[34] *Id.*

[35] Notice of Dem. and Dem. to Pl.'s First Am. Compl. at 3, *Licea v. Hickory Farms LLC*, No. 23STCV26148 (Cal. Super. Ct., Los Angeles Co.).

[36] Min. Order at 1, 5, *Licea v. Hickory Farms LLC*, No. 23STCV26148 (Cal. Super. Ct., Los Angeles Co.).

facts.[37] The court viewed the specifics of the alleged software installation and its impacts as evidentiary facts that did not need to be detailed at the complaint stage.[38]

The court also rejected the defendant's argument for dismissal on the grounds that the plaintiff consented to any software downloads by voluntarily visiting the website.[39] Judge Nellon ruled that accepting the consent defense without further scrutiny would render the pen register law meaningless.[40] The court recognized that accepting such a defense based solely on voluntary website visits would allow defendants in similar situations to successfully claim consent, thus prematurely ending potential pen register litigation.[41]

In *Hickory Farms*, the court granted the demurrer with leave for the plaintiff to amend the complaint.[42] The court agreed with the defendant that the plaintiff had failed to provide specific factual details on how collecting the plaintiff's IP address violated California or federal law.[43]

Reviewing case law and legislative history, Judge Pfahler concluded that software collecting an IP address is not comparable to software collecting a "unique fingerprint" of information, such as location data.[44] Recording an IP address does not violate the law, as this information is considered non-content communication.[45] The court noted that the legislative history referred only to cordless or cell phone technology, with no mention of internet technologies or their legal applications.[46] IP addresses alone do not constitute a "legally protected privacy interest."[47]

---

[37] Min. Order at 3, *Levings v. Choice Hotels Int'l, Inc.*, No. 23STCV28359 (Cal. Super. Ct., Los Angeles Co.).

[38] *Id.* at 3 (citing to C.W. Johnson & Sons, Inc. v. Carpenter, 53 Cal. App. 5th 165, 169 (2020)).

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] Min. Order at 1, *Licea v. Hickory Farms LLC*, No. 23STCV26148 (Cal. Super. Ct., Los Angeles Co.).

[43] *Id.* at 2, 5.

[44] *Id.* at 5.

[45] *Id.*

[46] *Id.*

[47] *Id.* (quoting Heeger v. Facebook, Inc., 509 F. Supp. 3d 1182, 1190 (N.D. Cal. 2020)).

The *Hickory Farms* court thus found that the plaintiff failed to allege facts suggesting the defendant installed software equivalent to recording a "unique fingerprint."[48] As a result, the plaintiff's claim lacked standing.[49] The court also questioned whether the plaintiff had used a device covered by California or federal privacy law, noting that the complaint only mentioned a "device" without further specification.[50] Without this information, the court could not determine if the plaintiff had a valid claim, potentially making the lawsuit moot and a waste of judicial resources.

A significant distinction between *Choice Hotels* and *Hickory Farms* is the latter court's acceptance of the notion that a user consents to the recording of an IP address by voluntarily visiting a website.[51] The *Hickory Farms* court acknowledged the potential implications of allowing complaints lacking in detail, which could set a dangerous precedent and alter the operation of the internet and online retailers.[52] However, the court did not broadly declare that consent through voluntary website visits would always serve as a defense in similar lawsuits.[53]

## IV. *HICKORY FARMS'* ANALYSIS IS SUPPORTED BY LEGISLATIVE HISTORY AND CASE PRECEDENT

The court in *Hickory Farms* offers a more robust and legally grounded analysis, drawing from established law and legislative history.[54] By contrast, the court in *Choice Hotels* issued a notably brief order that lacked substantial reliance on legal precedent or legislative context.[55] The primary focus in *Choice Hotels* was that a plaintiff does not need to present all factual details before a trial court moves forward with a case.[56] While this principle has some merit, the *Hickory Farms* court persuasively argued that the plaintiff should at least provide sufficient facts to determine if the

---

[48] *Id.*

[49] *Id.*

[50] *Id.* at 6.

[51] *Compare* Licea Min. Order 6, *with* Min. Order at 3, *Levings v. Choice Hotels Int'l, Inc.*, No. 23STCV28359 (Cal. Super. Ct., Los Angeles Co.).

[52] Licea Min. Order 7.

[53] *Id.* at 6.

[54] *See generally id.*

[55] *See generally id.*

[56] *See generally id.*

device alleged to be subject to a pen register falls under the protections of the California Penal Code.[57]

The legislative history surrounding Section 638.51 indicates that the bill's author did not intend for the law to apply to internet technologies. The legislative intent, as reflected in discussions before various California Assembly and Senate committees, only addressed pen registers in the context of landline and mobile phones.[58] There was no mention of extending protections to internet technologies.[59] This aligns with the federal government's precedent, particularly the 2005 Department of Justice guidance, which categorized IP addresses as non-content material not subject to privacy expectations.[60]

Since California's legislative history does not encompass internet technologies within the scope of Section 638.51, the court in *Hickory Farms* rightfully affords significant deference to its absence. The judiciary's role is not to broaden the law's scope to address minor injuries absent a grave injustice. The court in *Choice Hotels*, on the other hand, appears inclined to expand the pen register statute's coverage, which seems unwarranted based on the legislative context.

*Hickory Farms*' deferential approach is also supported by precedent from other California privacy cases in which plaintiffs attempted to apply telephone-specific statutes to internet communications. In *Licea v. Cinmar, L.L.C.*, the same plaintiff as in *Hickory Farms* argued that Cinmar violated the California Invasion of Privacy Act (CIPA) Sections 631[61] and 632.7[62] by employing a third party to intercept and eavesdrop on conversations occurring over Cinmar's website.[63] The defendant allegedly used this intercepted data without the website visitor's

---

[57] *See generally id.*

[58] *See generally* Cal. Assembly Committee on Privacy and Consumer Protection Hearing Report on AB 929 (Apr. 17, 2015); *see also* Cal. Assembly Committee on Appropriations Hearing Report on AB 929 (Apr. 28, 2015); *see also* Cal. Senate Committee on Public Safety Hearing Report on AB 929 (June 15, 2015); *see also* Cal. Senate Floor Analysis on AB 929 (July 1, 2015); *see also* Cal. Assembly Floor Analysis on AB 929 (July 8, 2015).

[59] *See supra* note 58.

[60] *See* Bellovin et al, *supra* note 15, at 62-63.

[61] CAL. PENAL CODE § 631 (Deering 2024).

[62] *Id.* at § 632.7.

[63] Licea v. Cinmar, LLC, 659 F. Supp. 3d 1096, 1101 (C.D. Cal. 2023).

consent or knowledge.[64] The plaintiff accessed the defendant's website using either a smartphone or a Wi-Fi connected laptop, arguing that these devices used "a combination of cellular and landline telephony."[65]

California Penal Code Section 631(a) criminalizes the unauthorized tapping or connection to telegraph or telephone wires, lines, cables, or instruments.[66] The plaintiff sought to extend Section 631(a) to cover communications made via smartphones and Wi-Fi connected laptops, proposing that courts should adapt California law designed for older technologies to modern devices.[67] However, the court rejected this argument, limiting the statute's application to the technologies expressly mentioned, namely wired telegraph or telephone communications.[68]

Plaintiff Licea contended that smartphones should fall under Section 631(a) because they use cell towers and wired infrastructure for functionality.[69] The court dismissed this claim, stating, "[a]lthough iPhones contain the word 'phone' in their name, and have the capability of performing telephonic functions, they are, in reality, small computers."[70] Furthermore, the plaintiff argued that California's failure to amend the statute to specify its limitation to telegraph or telephone technology should be interpreted as an implicit intent to include modern technology.[71] The court rejected this, noting that legislative inaction to amend the law implies a deliberate choice not to broaden its scope.[72] Indeed, the legislature had amended the section as recently as 2022 without including internet communications, maintaining support for this narrow interpretation.[73] Consequently, the court granted the motion to dismiss the plaintiff's claim under Section 631(a).[74]

---

[64] *Id.*
[65] *Id.*
[66] CAL. PENAL CODE § 631(a) (Deering 2023).
[67] *Cinmar*, 659 F. Supp. 3d at 1105.
[68] *Id.*
[69] *Id.*
[70] *Id.* (quoting Mastel v. Miniclip SA, 549 F. Supp. 3d 1129, 1135 (E.D. Cal. 2021)).
[71] *Id.* at 1105-06.
[72] *Id.*
[73] *Id.* at 1106.
[74] *Id.* at 1111.

In the same case, the plaintiff sought to have computer equipment included in the definition of a landline telephone under Penal Code Section 632.7(a), which criminalizes the unauthorized interception or recording of communications between cellular and landline telephones.[75] The plaintiff's argument hinged on the legislature's inclusion of data transmission in Section 632.7(c)(3) as a communication.[76] The court dismissed this argument, again emphasizing that a plain reading of Section 632.7(a) limits its application to a specified list of telephone-related items, excluding computers.[77] The inclusion of "communication" in the statute was intended to encompass various types of information transmitted over telephones, not to extend the law's scope to internet communications.[78] The court also highlighted that the legislature had amended Section 632.7 multiple times, most recently in 2022, without addressing internet or web communications, reinforcing the intent to limit its scope to traditional telephone technology.[79]

The court went on to reject the plaintiff's argument that his use of a smartphone or laptop constituted "a combination of cellular and landline telephony," noting that the misconduct alleged involved using the smartphone as a computer rather than as a telephone.[80] The claim regarding the laptop was dismissed as conclusory, with no need for further determination.[81]

Similarly, in *Heeger v. Facebook, Inc.*, the plaintiff, Heeger, filed a claim under the California Information Privacy Act (CIPA)[82] against Facebook, alleging that the social media giant collected users' location histories without their consent, even when users had disabled location tracking on their devices.[83] Heeger claimed that Facebook gathered IP addresses yet provided no substantial information on the nature of his injury or the specific violation of CIPA by Facebook.[84] The core of the legal analysis in this case

---

[75] *Id.*
[76] *Id.*
[77] *Id.* at 1112.
[78] *Id.*
[79] *Id.*
[80] *Id.* at 1113.
[81] *Id.*
[82] *See* supra notes 61, 62.
[83] Heeger v. Facebook, Inc., 509 F. Supp. 3d 1182, 1186 (N.D. Cal. 2020).
[84] *Id.* at 1189.

revolved around whether IP addresses should be afforded the same level of privacy protection as cell-site location information (CSLI) data.[85]

The U.S. Supreme Court's decision in *Carpenter v. United States*, served as a crucial reference point.[86] In *Carpenter*, the Court held that CSLI data deserved privacy protection due to its invasive nature, as it is continuously recorded and can precisely pinpoint an individual's location, sometimes within an area as small as one-eighth of a square mile.[87] This ruling established that CSLI data is protected under an expectation of privacy.[88]

To distinguish *Carpenter*, the district court in *Heeger* concluded that IP addresses do not warrant the same level of protection under the CIPA.[89] The court highlighted a significant difference: unlike CSLI data, internet users are generally aware or should be aware that they are disclosing their IP addresses to third parties whenever they access websites.[90] This disclosure is necessary for the website provider to route and direct information back to the user.[91] As such, the court determined that there is no reasonable expectation of privacy for IP addresses that would support a claim under the CIPA.[92]

Consequently, the court granted Facebook's motion to dismiss, underscoring that the protections designed for mobile telephone user privacy, such as those established in *Carpenter*, do not necessarily extend to internet usage.[93] This decision is based on the view that legal standards developed for one type of technology, specifically telecommunication, do not automatically apply to another, like internet communications.[94] This distinction is critical in the evolving landscape of privacy law, where different types of

---

[85] *Id.*
[86] *See generally* Carpenter v. United States, 585 U.S. 296 (2018).
[87] *Id.* at 296, 312-13.
[88] *See id.* at 320.
[89] *Heeger*, 509 F. Supp. 3d at 1189-91.
[90] *Id.*
[91] *Id.*
[92] *Id.*
[93] *Id.* at 1190.
[94] *Id.*

data and their associated technologies demand tailored legal interpretations.[95]

## CONCLUSION

The opposite rulings in *Choice Hotels* and *Hickory Farms* in L.A. County beg the need for an appellate court to rule on how existing California law should apply to website tracking practices. The conflicting case results offer a cautionary tale of what can happen when trial judges, without guidance, are tasked with interpreting how laws should apply to technologies that they may not fully understand. To provide this guidance, the California legislature must draft statutes that expressly—and unequivocally—apply privacy protections against pen registers to a specific technology, such as the internet. As an alternative, the legislature could use catch-all language that could specify prohibited practices "in all media now known or hereafter devised," as entertainment companies use in their private contracts.[96] But, as the *Hickory Farms* ruling suggests, practices that may violate privacy in one technology may not violate privacy in a different technology.

As much as an omnibus, catch-all technology definition offers streamlined efficiency for legislatures, it is ultimately not a substitute for a narrowly constructed, technology-specific statute. Anything less could lead to varying interpretations that may cause uncertain or inconsistent applications of privacy protections. At the federal level, for example, the Stored Communications Act was drafted specifically to address the difference between content and non-content information, such as subscriber information, and

---

[95] Courts in the U.K. and Europe, as a substantive matter, may align more closely with Choice Hotels' activist position. But those jurisdictions have a history and tradition of more direct state interventions on speech than afforded by the First Amendment. They also have legislation in place drafted specifically to address data privacy in the digital environment. *See* Lloyd v. Google, [2021] UKSC 50, [1] (appeal taken from Eng.); *see also* Google Inc. v. Vidal-Hall., [2015] EWCA Civ. 311, [1], [3] (appeal taken from Eng); *see also* C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd, 2020 E.C.J. C:2020:559.

[96] Erin M. Jacobson, *Contract Language Explained: "In All Media Now Known or Hereafter Devised*,*"* INDIE ARTIST RES. (Feb. 5, 2016), https://indieartistresource.com/contract-language-explained-in-all-media-now-known-or-hereafter-devised/ [https://perma.cc/64DN-9YQE].

applying protections only with respect to content.[97] Even the Communications Act of 1934, the federal law that governs civilian communications in the U.S., typically segregates its provisions by technology, with separate provisions written for telephony, broadcasting, cable television, and the internet.[98]

For some privacy advocates, the ruling in *Choice Hotels* may be appealing. A website enlists software to identify and track users without their consent. Who would not want to be protected against this type of intrusive business practice? But, at the end of the day, if the California legislature wants to prohibit this type of business practice on the internet, then it should pass a law that specifically addresses it. This makes *Hickory Farms* the better of the two rulings for California courts.

---

[97] Stored Communications Act § 201(a), 18 U.S.C. § 2703(a).

[98] *See generally* Communications Act of 1934, 47 U.S.C. §§ 151-646 (containing provisions that apply to common carriers, radio broadcasters, public telecommunications facilities, cable communications, etc.).