Washington Journal of Law, Technology & Arts

Volume 12 | Issue 2

Article 3

1-1-2017

"Reasonable Zones of Privacy"—The Supreme Court's Struggle to Find Clarity in the American Landscape Regarding Fourth **Amendment Rights**

Alex Alben

Follow this and additional works at: https://digitalcommons.law.uw.edu/wjlta



Part of the Fourth Amendment Commons, and the Privacy Law Commons

Recommended Citation

Alex Alben, "Reasonable Zones of Privacy"—The Supreme Court's Struggle to Find Clarity in the American Landscape Regarding Fourth Amendment Rights, 12 WASH. J. L. TECH. & ARTS 145 (2017). Available at: https://digitalcommons.law.uw.edu/wjlta/vol12/iss2/3

This Article is brought to you for free and open access by the Law Reviews and Journals at UW Law Digital Commons. It has been accepted for inclusion in Washington Journal of Law, Technology & Arts by an authorized editor of UW Law Digital Commons. For more information, please contact lawref@uw.edu.

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS VOLUME 12, ISSUE 2 WINTER 2017

"REASONABLE ZONES OF PRIVACY"—THE SUPREME COURT'S
STRUGGLE TO FIND
CLARITY IN THE AMERICAN LANDSCAPE REGARDING FOURTH
AMENDMENT RIGHTS

Alex Alben *

© Alex Alben

CITE AS: 12 WASH. J.L. TECH. & ARTS 145 (2017) http://digital.law.washington.edu/dspace-law/handle/1773.1/1704 ABSTRACT

The U.S. Supreme Court has struggled over the years to develop the concept of what constitutes a "reasonable zone of privacy" when it comes to intrusion on an individual's physical space or activities. With the advent and widespread adoption of new technologies such as drones and listening devices, concern for protecting privacy has magnified, yet court doctrine remains inconsistent. The author, Washington State's Chief Privacy Officer, reviews the history of Supreme Court "search and seizure" rulings in prominent cases to identify both patterns and flaws on the topic of protecting citizen privacy.

^{*} Alex Alben was named the first chief privacy officer of Washington State in 2015. He is a graduate of Stanford University and Stanford Law School. In his first job he worked as a researcher for Walter Cronkite at CBS News and then for CBS Reports. After law school, he served as an entertainment lawyer for Orion Pictures and Warner Bros., before beginning a tech career in Seattle with senior management positions at Starwave Corp. and RealNetworks, Inc. Alben teaches a section of the Privacy Law Clinic at the University of Washington School of law. The opinions expressed in this article are his own.

TABLE OF CONTENTS

Intro	oduction 14	46
I.	New Technologies and Zones of Privacy 14	47
II.	Phase I – The Strange Doctrine of Curtilage and Open Fields (1891-1924)	
III.	Phase II – Wiretapping from <i>Olmstead</i> to <i>Katz</i> (1928-1967)	
IV.	Phase III – Open Fields and Drugs: The 1980s 15	54
Con	clusion	56
Prac	etice Pointers15	58

Introduction

On May 31, 2016, the Fourth Circuit Court of Appeals in Virginia ruled *en banc*, by a 12-3 vote, that our most durable privacy law—the Fourth Amendment—does not protect cell phone data pinpointing a caller's location. In this particular case, law enforcement convicted two Baltimore men of multiple armed robberies in 2011 by analyzing 221 days of their wireless location data, which pinpointed 29,000 different locations.² The court reasoned that, because cell phone owners know that their location information is shared with their wireless carrier, as under the thirdparty doctrine, an individual can claim "no legitimate expectation of privacy" in information that he has voluntarily turned over to a third party.³

The *Graham* ruling calls into question whether a "reasonable" expectation of privacy" exists with respect to wireless location data. It also seems to contradict the broad pro-privacy affirmation expressed the Supreme Court's unanimous decision in Rilev v.

¹ United States v. Graham, 824 F.3d 421, 428 (4th Cir. 2016) ("[T]he Government's acquisition of that information (historical CSLI) pursuant to § 2703(d) orders, rather than warrants, did not violate the Fourth Amendment.").

² See generally Graham, 824 F.3d 421 (4th Cir. 2016).

³ *Id.* at 427 ("Applying the third-party doctrine to the facts of this case, we hold that Defendants did not have a reasonable expectation of privacy in the historical CSLI.").

California, which held that police must obtain a search warrant before opening an individual's cell phone incident to a search.⁴

The definition of 'zones of privacy' has evolved over three distinct phases of Supreme Court jurisprudence. The first phase, from 1891-1924, involved the arcane "open fields" or "open view" doctrine." The second phase, from 1928-1967, allowed for widespread government wire-tapping, but ended with the Court's 1967 ruling in *Katz v. United States*, which articulated a "reasonable zone of privacy" standard. Finally, the "open fields" doctrine reemerged in the 1980's in conjunction with contemporary drug cultivation operations. As a result, the Court reverted to finding no violation of the Fourth Amendment —even in cases of intrusion on private property. Examining these three eras sheds considerable light on the privacy rights, or lack thereof, in America today.

I. NEW TECHNOLOGIES AND ZONES OF PRIVACY

While the Supreme Court has historically struggled to define a person's reasonable zone of privacy, technology has run circles around the judiciary. Fifteen years ago, the public had very little expectation that private companies would take satellite photographs to compile aerial views of every American neighborhood, down to recognizable houses, gardens, garages, and lawns.⁸ Nor did people commonly exercise property rights in vertical air space above her

⁴ Riley v. California, 134 S. Ct. 2473, 2493 (2014) ("[A] warrant is generally required before such a search, even when a cell phone is seized incident to arrest.).

⁵ The terms "open fields" and "open view" are used interchangeably in this article, although later decisions tend to use the "open view" phrase to describe the general doctrine.

⁶ Katz v. United States, 398 U.S. 347 (1967).

⁷ See Hester v. United States, 265 U.S. 57 (1923)

⁸ See generally, Samuel Gibbs, Google Maps: a decade of transforming the mapping landscape, THE GUARDIAN (Feb. 8 2015, 4:00 AM), https://www.theguardian.com/technology/2015/feb/08/google-maps-10-anniversary-iphone-android-street-view.

domain extending all the way up to outer space. With the rapid and widespread adoption of new technologies, lawmakers have generally surrendered potential privacy claims to Google, Bing and other mapping services as these technologies expanded.

Google Street View poses a closer case for privacy advocates, in part because of how it acquires data. ¹⁰ A camera-laden car mapping a neighborhood might snap a photograph of an individual in an embarrassing pose. This technology, however, has widely been ruled to be legal in a variety of jurisdictions because the mapping vehicle is using public streets and taking photos of scenery that can otherwise be seen with the naked eye. ¹¹ In this sense, Google's resources and technology have logarithmically expanded the old legal doctrine of "open view." ¹²

U.S. law might not have permitted Google Street View, however, had, a strange and enduring definition of a person's home through physical invasion or curtilage not been articulated by the Supreme Court over eighty years ago.¹³

⁹ While the ad coelum doctrine refers to ownership of land up to the heaven and down to the center of the earth, it had little practical application above ground until the invention of airplanes. See Environmental Justice, Peter S. Wentz, p. 177, SUNY Press, 1988. When a man tried to claim ownership of certain rights in asteroid Eros 433, the Ninth Circuit held that he stated no recognizable legal claim either under common law or the Outer Space Treaty. Nemitz v United States and or, Decision on motion to dismiss, 2004 WL 3167042 (D Nev 2004), ILDC 1986 (US 2004), 26th April 2004, United States.

¹⁰ Alexis C. Madrigal, *How Google Builds Its Maps—and What It Means for the Future of Everything*, THE ATLANTIC (Sep. 9, 2012),

https://www.theatlantic.com/technology/archive/2012/09/how-google-builds-its-maps-and-what-it-means-for-the-future-of-everything/261913/.

¹¹ See, e.g., Boring v. Google, Inc., 598 F. Supp. 2d 695, 700 (W.D. Pa. 2009) (ruling in favor of Google and dismissing privacy claims because Google Street View were images that were in plain sight. Interestingly the court noted it would be "hard to believe" the plaintiffs suffered "shame or humiliation.").

¹² The open fields doctrine holds that persons cannot assert protection for activities conducted in open fields because such areas are not protected places or things under a plain language reading of the fourth amendment. *See* Seth H. Ruzi, *Reviving Trespass-Based Search Analysis Under the open view Doctrine: Dow Chemical Co. v. United States*, 63 N.Y.U. L. Rev. 191, 196 (1988) (citing *Hester v. United States*, 265 U.S. 57 (1923)).

¹³ Olmstead v. United States, 277 U.S. 438 (1928).

II. PHASE I – THE STRANGE DOCTRINE OF CURTILAGE AND OPEN FIELDS (1891-1924)

Much of the failure of American courts to delineate reasonable zones of privacy traces back to the historic Supreme Court ruling in *Olmstead v. United States*. ¹⁴ In writing for the majority's ruling on relatively modern technology—telephones and the government interception of telephone wire transmissions—Chief Justice William Howard Taft drew on the ancient property concepts that informed most privacy law in the late 19th and early 20th centuries. ¹⁵ Taft concluded that a Fourth Amendment violation does not occur unless there has been an official search and seizure of a person's papers, or tangible material effects. ¹⁶ Further, a search would not occur unless there was an "actual physical invasion of his house or curtilage for the purpose of making a seizure."

Prior to *Olmstead*, courts adhered to an archaic construction of zones of privacy. One has to turn to the 1891 edition of Black's Law Dictionary to find a working definition of "curtilage:"

"The enclosed space of ground and buildings immediately surrounding a dwelling-house. In its most comprehensive and proper legal signification, it includes all that space of ground and buildings thereon which is usually enclosed within the *general fence* immediately surrounding a principal *messuage* and outbuildings, and yard closely adjoining to a dwelling-house, but it may be large enough for cattle to be *levant* and *couchant* therein."

¹⁴ *Id*.

¹⁵ Id

¹⁶ *Id.* at 466. Additionally, a Fourth Amendment analysis is outside the scope of this Article.

¹⁷ *Id.* (emphasis added)

¹⁸ *Curtilage*, BLACK'S LAW DICTIONARY 311 (6th ed. 1891) (first alteration in original) (emphasis added).

For those not familiar with "messuage," it is a property law term referring to a dwelling and its outbuildings and curtilage. ¹⁹ For those not raised in 18th century French farmhouses, "levant and couchant" refer to the practice of cattle rising up and lying down. ²⁰

While humans tend to conduct illegal activities indoors, we have the outdoorsy moonshine and marijuana-growing businesses to thank for the evolution of our legal doctrines on privacy and open fields. In *Hester v. United States*, ²¹ the Supreme Court explored the question of whether a person's zone of privacy extended to the open fields surrounding a home or farm, an inquiry that would lead to the creation of the "open fields" doctrine. In 1924, federal agents stood 50-100 yards away from Hester's farm and observed him handing a quart bottle to another man. ²² The bottle contained home-grown distilled spirits, illegal in the Prohibition Era. ²³ On this basis, the agents subsequently arrested Hester, who claimed in court that they had trespassed on his property and violated his Fourth Amendment rights. ²⁴

The Court felt no sympathy for Hester, reasoning that if his fields were readily visible from an adjacent property and the agents had conducted no physical trespass, the unfortunate moonshiner had no Fourth Amendment privacy argument to make.²⁵ Justice Oliver Wendell Holmes encapsulated the Court's reasoning, holding that "the special protection accorded by the Fourth Amendment to the people in their 'persons, houses, papers and effects', is not extended to the open fields."²⁶

Thus, "open fields" remained fair game for law enforcement for decades. First articulated in *Hester*, the doctrine informed much of the Supreme Court's thinking as new technologies came onto the scene after the turn of the century.

¹⁹ Messuage, BLACK'S LAW DICTIONARY (10th ed. 2014) available at Westlaw BLACKS.

²⁰ Levant and couchant, BLACK'S LAW DICTIONARY (10th ed. 2014) available at Westlaw BLACKS.

²¹ Hester v. United States, 265 U.S. 57 (1924).

²² *Id.* at 58.

²³ *Id*.

²⁴ *Id*.

²⁵ *Id*.

²⁶ *Id.* at 59.

III. PHASE II – WIRETAPPING FROM OLMSTEAD TO KATZ (1928-1967)

Over a forty-year period, American courts allowed telephone and broadcast technologies to flourish without scrutiny under the Fourth Amendment—at least in the context of wiretapping-- until *Olmstead v. United States*.²⁷ Presiding over the 1928 case of prominent Seattle bootlegger Roy Olmstead, the Supreme Court held that federal agents had not conducted a search-and-seizure within the meaning of the Fourth Amendment after wiretapping Olmstead's telephone line to record his conversations with members of his illegal liquor distribution operation.²⁸

In 1924, federal agents tapped Olmstead's phone and took notes on his conversations. These were then transcribed in a "black book" that the prosecutor used to charge a total of forty-seven defendants, including Olmstead's attorney and his wife Elise.²⁹ Given the unsophisticated technology of the time, the agents could not see the numbers that Olmstead and his associates were dialing. To solve this problem, they crossed the tapped phone line with another line, causing interference.³⁰ Olmstead then had to verbally instruct the operator which number he wished to dial. The FBI

²⁷ Olmstead, *supra* note 13; *see also* Daryl C. McClary, *Olmstead*, *Roy* (1886-1966) — *King of King County Bootleggers*, HISTORY LINK (Nov. 13, 2002), http://www.historylink.org/File/4015. (Olmstead had served on the Seattle Police force as an enforcer of Seattle's early prohibition law and later the 18th Amendment when it came into effect in 1920. Olmstead observed the operations of the region's bootleggers and concluded he could do better. After serving a brief prison sentence for running an alcohol smuggling operation while still a member of the force, he returned to bootlegging full time, smuggling alcohol from Canada primarily by small boats to beaches and coves in Washington State).

²⁸ Olmstead, *supra* note 13, at 464.

²⁹ See Daryl C. McClary, *Olmstead, Roy* (1886-1966) — *King of King County Bootleggers*, History Link (Nov. 13, 2002), http://www.historylink.org/File/4015.

³⁰ Olmstead, *supra* note 13, at 487.

agents posted within earshot of his office recorded these numbers in their notebooks, then did a "reverse look-up" to find the addresses linked to them.³¹ After a twenty-four-hour trial, Olmstead was sentenced to four years of hard labor and fined \$8,000.³²

The case arrived at the Supreme Court in 1928, when former President William Howard Taft presided as Chief Justice. Writing for the Court, Taft demonstrated he had a rudimentary understanding of telephony by stating that he simply did not see a Fourth Amendment violation because the government did not intrude on Olmstead's physical space: "[t]here was no searching. There was no seizure. The evidence was secured only by the sense of hearing. There was no entry of the houses or offices of the defendants."³³

The Supreme Court did not decide *Olmstead* unanimously. Justice Louis Brandeis examined the facts surrounding the wiretap and concluded that the federal agents had indeed violated the Constitution.³⁴ In his dissent, Brandeis inquired, "can it be that the Constitution affords no protection against such invasions of individual security?"³⁵ Justice Brandeis understood an invasion of privacy does not require a physical intrusion given the evolution of modern technology such as telephony.

Six years later, Congress passed the Communications Act in 1934, which explicitly outlawed the practice of wiretapping telephones without a court warrant.³⁶ However, the Act did not address the legality of bugs and other forms of electronic eavesdropping.³⁷

Thirty-three years later, the Supreme Court considered

³³ Olmstead, supra note 13, at 464.

³¹ See Daryl C. McClary, supra note 29.

³² *Id*.

³⁴ Olmstead, 277 U.S. at 464.

³⁵ *Id.* at 474 (Brandeis, J., dissenting).

³⁶ Communications Act, 47 U.S.C. §§151-622 (1934).

³⁷ See Congressional Research Service, "Privacy: An Overview of Federal Statutes Governing Wiretapping and Elctronic Eavesropping," Stevens and Doyle, October 9, 2012: "The Act neither expressly condemned law enforcement interceptions nor called for the exclusion of wiretap evidence, but it was read to encompass both, Nardone v. United States, 302 U.S. 379 (1937); Nardone v. United States, 308 U.S. 321 (1939)."

whether the FBI had violated a man's expectation of privacy under the Fourth Amendment when it tapped a phone booth outside of his Los Angeles apartment due to suspicion that he was placing illegal bets on college basketball games.³⁸ In 1967, Charles Katz was in fact one of the country's most successful basketball handicappers and bettors, having evaded persistent law enforcement efforts to catch him in the act.³⁹ By disabling one phone booth and planting recording devices on the tops of two others on Sunset Boulevard, FBI agents managed to overhear his betting conversations with associates in Miami and Boston.⁴⁰

There was one flaw with the FBI's plan: the agents did not have a search warrant when they intercepted Katz's conversations. As a result, Katz's attorneys filed an appeal arguing that the recordings could not be used as evidence against him on Fourth Amendment grounds. Following *Olmstead*, however, the court of appeals rejected Katz's argument, citing the absence of a physical intrusion into the phone booth itself and ignoring the FBI's elaborate surveillance scheme in targeting Katz and monitoring his calls via the two working phone booths.

Nevertheless, Katz ultimately prevailed. The Supreme Court ruled 7-1 that Katz was entitled to constitutional protection for his conversations.⁴⁴ Justice Potter Stewart wrote for the Court:

"The Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to

³⁸ Katz v. United States, 389 U.S. 347 (1967).

³⁹ See Matthew Lasar, *The crooks who created modern wiretapping law*, ARS TECHNICA (Jun. 2, 2011, 6:47 AM), https://arstechnica.com/techpolicy/2011/06/the-crooks-who-created-modern-wiretapping-law/.

⁴⁰ Katz at 131.

⁴¹ *Id*.

⁴² *Id.* at 133.

⁴³ *Id.* at 134.

⁴⁴ Katz, 389 U.S. 347, 359.

preserve as private, even in an area accessible to the public [e.g., a phone booth] may be constitutionally protected."45

A concurring opinion by John Marshall Harlan introduced the idea of a "reasonable" expectation of Fourth Amendment protection.⁴⁶ Harlan invented a two-part test for "reasonableness" in this context: "first, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"47

IV. PHASE III – OPEN FIELDS AND DRUGS: THE 1980s

As the illegal production of alcohol prompted many open fields cases in a prior era, several cases in the 1980s reached the Supreme Court dealing with a new illicit activity that triggered reflection on meaning of the Fourth Amendment.⁴⁸ Growing marijuana in open fields occupied the Court's attention in the 1984 case of *Oliver v. United States*.⁴⁹ Oliver cultivated a marijuana crop in a field adjacent to his Kentucky property. 50 Despite a posted "No Trespassing" sign, Kentucky State Police parked their vehicle, walked around a gate and proceeded down a footpath until they spotted the marijuana plants, about a mile from the gate.⁵¹ They arrested Oliver.⁵²

Once again, the Court found no search-and-seizure, due to the open nature of the landscape where the illegal growing operation was situated.⁵³ Seeking to draw a distinction between portions of a property where an individual or family might have some expectation

⁴⁵ *Id.* at 351.

⁴⁶ *Id.* at 361 (Harlan, J., concurring).

⁴⁷ *Id.* at 361 (Harlan, J., concurring).

⁴⁸ See Oliver v. United States, 466 U.S. 170 (1984) (cultivation of marijuana on property); United States v. Dunn, 480 U.S. 294, 296 (1987) (running a private chemical plant in a barn on personal property).

⁴⁹ Oliver v. United States, 466 U.S. 170 (1984).

⁵⁰ *Id.* at 173.

⁵¹ *Id*.

⁵² Id..

⁵³ *Id.* at 184.

of property and other portions where they would not, the Court reasoned: "open fields do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or surveillance." ⁵⁴

Three years later, agents of the Drug Enforcement Administration found a chemical manufacturing plant in a private barn on private ranch.⁵⁵ Led by the smell of chemicals and the sound of a running motor, they skirted several fences—including at least one spiked with barbed wire—crossed a gate and entered the barn, where they apprehended their target.⁵⁶ Although the Court of Appeals ruled that the barn—surrounded by several fences, was clearly within the owner's "curtilage"⁵⁷—the Supreme Court in *United States v. Dunn* disagreed, holding that this area was not "intimately tied to the home itself."⁵⁸ Apparently, running a drug lab is not an intimate family activity.

One might view *Hester*, *Oliver* and *Dunn* as 'result oriented' rulings, where courts knew that an illegal activity had occurred and chose to justify the fact that law enforcement failed to get a warrant by deciding that there is no zone of privacy if the activity is within 'open view' or even in a barn. Before sophisticated surveillance technology, such rulings posed a threat to moonshiners and pot growers, but not to the average citizen in terms of government spying on private activities indoors or outdoors. Privacy is no longer defined by the parameters of human senses such as vision or hearing, but now finds a new range of threats based on devices that take the concept of surveillance to a new plane. ⁵⁹ With the advent of drones,

⁵⁴ *Id.* at 179.

⁵⁵ United States v. Dunn, 480 U.S. 294, 296 (1987).

⁵⁶ Id

⁵⁷ United States v. Dunn, 674 F.2d 1093, 1100 (5th Cir. 1982), *cert. granted, judgment vacated*, 467 U.S. 1201, 104 S. Ct. 2380, 81 L. Ed. 2d 340 (1984), and *opinion reinstated*, 782 F.2d 1226 (5th Cir. 1986).

⁵⁸ United States v. Dunn, 480 U.S. at 294.

⁵⁹ See Richard G. Wilkins, Defining the 'Reasonable Expectation of Privacy': An Emerging Tripartite Analysis, 40 VAND. L. REV. 1077, 1114-28 (1987)

thermal imaging and high-resolution cameras, the game has changed. "Curtilage" seems like a very quaint notion when a police officer can operate a bird-sized battery-powered drone and maneuver it directly over a suspect's home or outside a window. In these cases, law enforcement should simply get a warrant. They might have been tipped to the location of drug operation by an informant or other lead, but flying a surveillance drone over the scene violates any basic "reasonable expectation" of privacy in one's property, whether indoors or outdoors.

CONCLUSION

Of all the Supreme Court's struggles to develop a consistent doctrine to define a zone of privacy, the *Katz* formulation makes the most sense, because privacy rights should travel with the individual. The inherent vagueness of what is 'reasonable'" in different situations only creates room for uncertainty, especially as technology and our cultural norms continue to evolve. Now that the Fourth Circuit has ruled that no warrant is required for a wireless carrier to turn location data over to law enforcement, U.S. citizens live in a 'Catch-22' where individuals supposedly have "reasonable expectations" of privacy in physical spaces, such as phone booths, but almost no expectation of location privacy when they are using their cell phones.

With the introduction of new technologies—ranging from Google Earth aerial photographs to drone surveillance—the question of where public space ends and private space begins has reached a critical phase. Deciding the scope of a person's "zone of privacy" will be the front-line question for judges and technology advocates to determine for the next generation. Examining the colorful and salient cases surveyed above hopefully provides a few

^{(&}quot;[T]he presence or absence of a physical intrusion ostensibly ceased to be the focal point of [F]ourth [A]mendment analysis.").

⁶⁰ Hope Reese, *Police are now using drones to apprehend suspects and administer non-lethal force: A police chief weighs in*, TECHREPUBLIC (Nov. 25 2015, 4:00 AM), http://www.techrepublic.com/article/police-are-now-using-drones-to-apprehend-suspects-and-administer-non-lethal-force-a-police-chief/.

clues as to the way courts may eventually answer the question of where privacy begins in the modern world of smart phones and surveillance technologies.

Given the inherent privacy interest of people as they move about the world, it seems paramount to address this question. Most Americans do not have a "reasonable expectation" that law enforcement can easily discover their whereabouts when making phone calls or strolling through a mall.⁶¹ Further, with the emergence of data analytics, law enforcement can potentially trace individuals through the course of a day, whenever they trigger a safety camera or license plate reader.⁶² The recent reforms of the Patriot Act passed in 2015 have pared back the government's right to intercept our private communications, but the surveillance apparatus still exists.⁶³ If we apply different privacy protections to different technologies, we run the risk of fundamentally eroding our remaining privacy rights. Despite the march of technology, is it too much to ask that we can conduct our legal private activities within reasonable zones of privacy?

⁶¹ Simon Hill, *Is your smartphone being tracked? We asked an expert*, DIGITAL TRENDS (May 17, 2015, 9:00 AM), http://www.digitaltrends.com/mobile/police-hackers-phone-tracking/.

⁶² Thirteen states have adopted varying limits on retention of automated license plate reader images. *See* National Conference of State Legislatures web page, dated Feb. 27, 2017 and last checked March 7, 2017.

⁶³ Fulfilling Rights and Ensuring Effective Discipline Over Monitoring (USA FREEDOM) Act of 2015, Pub. L. 114-23 (2015).

PRACTICE POINTERS

- Keep updated on new legislation. As the privacy landscape continues to rapidly evolve, we can identify new ideas for the protection of personal data and privacy rights, especially at the state and local levels.
- Keep up-to-date on new technology. New tools, platforms and devices may use personally-identifiable information in innovative ways, which inexorably creates novel privacy questions. Explore the data retention practices and policies of the new technologies you or your clients might adopt for personal use.
- Seek answers outside the field of law. Generally, privacy issues may not be limited to the legal field.
 Technology tends to outpace law, and consulting technology and communications publications will provide valuable context for considering privacy issues.