UNT DALLAS COLLEGE of LAW

2019 ON • THE • CUSP 2020

LAW REVIEW

BOOK REVIEW

"KNOW YOUR RIGHTS"

CYRUS FARIVAR HABEAS DATA: PRIVACY VS. THE RISE OF SURVEILLANCE TECH

Brian L. Owsley[*]

In teaching both Federal Criminal Procedure and a course entitled "Fourth Amendment and Electronic Surveillance," I routinely tell people that the subject matter is compelling to just about everyone. Specifically, I note that the Fourth Amendment, at its core, is about what the proverbial "man" can and cannot do to all of us in our homes, cars, and elsewhere in our most private spaces. In Cyrus Farivar's *Habeas Data: Privacy vs. the Rise of Surveillance Tech* (*Habeas Data*), he captures many of the critical questions and debates surrounding the Fourth Amendment, privacy, and electronic surveillance that American society faces today.[1]

Each chapter in *Habeas Data* chronicles a different type of surveillance that poses a threat to individual privacy rights. For example, Farivar addresses how the Supreme Court of the United State's (Court) third-party doctrine created the path that led to the National Security Agency's data collection program that Edward Snowden eventually revealed.[2] Farivar writes about the Court's response in *Kyllo v. United States*,[3] which involved a thermal-imaging device, an invasive, new technology.[4] He expounds on *United States v. Jones*[5]—where the Court considered whether law enforcement officers needed a search warrant to place a tracking device on a suspect's vehicle.[6] Similarly, he uses *Riley v. California*,[7] a case where

[*] Brian L. Owsley, Assistant Professor of Law, University of North Texas Dallas College of Law; B.A., University of Notre Dame, J.D., Columbia University School of Law, M.I.A., Columbia University School of International and Public Affairs.

[1] *See generally* Cyrus Farivar *Habeas Data: Privacy vs. the Rise of Surveillance Tech* (2018).

[2] *Habeas Data*, supra note 1, at 57–80 (discussing Smith v. Maryland, 442 U.S. 735 (1979) and third-party doctrine).

[3] 533 U.S. 27 (2001).

[4] *Habeas Data*, supra note 1, at 107–27 (discussing Kyllo v. United States, 533 U.S. 27 (2001)).

[5] 565 U.S. 400 (2012).

[6] *See Habeas Data*, supra note 1, at 149–69 (discussing United States v. Jones, 565 U.S. 400 (2012)).

[7] 134 S. Ct. 2473 (2014).

the Court recently determined that law enforcement officers need a search warrant to examine an individual's cell phone as a basis to discuss whether one's cell phone can be searched.[8]

Other chapters include issues that the Court has not yet considered such as a third-party provider's obligation to assist the government in cracking a cell phone's password.[9] Furthermore, Farivar examines the use of license plate readers by law enforcement and that usage's implication for individual privacy rights.[10] Indeed, he raised the issue of the use of cell-site-location information in tracking an individual's whereabouts before *Carpenter v. United States*[11] settled the issue.[12]

These latter three examples demonstrate a theme in *Habeas Data*: notions about privacy have always been evolving, and now they are developing concurrently with the quickening pace of technology. The reader sees that insofar as *Katz v. United States*, decided in 1967, is essentially the oldest case that Farivar references.[13] Indeed, besides *Smith v. Maryland*, *Katz* is also the only significant case upon which he focuses decided in the twentieth century.[14] These three chapters reiterate a theme stressed throughout the book and, no doubt, in federal criminal procedure classrooms across the country. Specifically, that the nature of individual privacy rights in relation to constitutional protections is fluid, and people need to be aware of changes. As the English, punk-rock band The Clash proclaimed in one of their iconic songs, "Know Your Rights.!"[15] Farivar begins his book with a natural starting point for any discussion about the Fourth Amendment and privacy rights: *Katz v. United States*.[16] In that decision, the Court considered Charles Katz's petition to exclude evidence collected during his use of public telephones in Los Angeles to call in bets to bookies in Boston and Miami in violation of federal criminal law.[17] Based on FBI surveillance, agents attached a listening device to the top of the telephone booth, enabling them to record Katz's side of the telephone conversations.[18] Ultimately, the government used Katz's words to convict him at trial.[19] Farivar's use of *Katz* here is critical because that decision serves as the seminal case of Fourth Amendment jurisprudence, altering the landscape as it has previously existed. Justice Potter Stewart, in authoring the majority's decision in favor of Katz, explained that "[o]ne who occupies [a telephone booth], shuts the

---

[8] *See Habeas Data*, supra note 1, at 107–27 (discussing Riley v. California, 134 S. Ct. 2473 (2014)).
[9] *See Habeas Data*, supra note 1, at 26–56; *see generally* Brian L. Owsley, *Can Apple Build a Privacy Minded iPhone Security System so Secure that Apple Cannot Access It?*, 7 HEALTH & TECH. 369 (2017).
[10] *See Habeas Data*, supra note 1, at 81–106.
[11] 138 S. Ct. 2206 (2018).
[12] *See Habeas Data*, supra note 1, at 170–197.
[13] *See Habeas Data*, supra note 1, at 4.
[14] *Id.*
[15] The Clash, *Know Your Rights* (CBS 1982).
[16] 389 U.S. 347 (1967).
[17] *Id.* at 348.
[18] *Id.*
[19] *Id.*

door behind him, pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[20]

However, Justice John Harlan's concurrence is the opinion that has the lasting impact because he established the notion of an individual's reasonable expectation of privacy. Specifically, he enunciated a two-fold requirement for what Fourth Amendment protections exist in a given situation. First, a person must demonstrate an actual expectation of privacy.[21] Second, the expectation must be one that society is prepared to recognize as reasonable.[22] Farivar addresses *Katz* in lengthy detail that provides many interesting tidbits to lawyers and laypersons alike. However, it would have been beneficial for Farivar to develop more of a discussion of the historical approach to Fourth Amendment interpretation prior to the *Katz* decision. To be clear, he does note that, historically, physical trespass was essential to an individual's claim regarding a Fourth Amendment violation.[23] However, in a book replete with wonderful historical details, this critical notion gets short-changed.

In *Olmstead v. United States*, the Court considered a petition by Roy Olmstead who the federal agents suspected of being a bootlegger in Seattle during Prohibition.[24] Consequently, some agents installed wiretaps in the basement of Olmstead's building connecting to the three telephones that he had in his office as well as in the streets near his home for that land line.[25] There were numerous incriminating calls to Vancouver.[26] Olmstead was convicted with evidence obtained from the wiretaps.[27] Chief Justice William Howard Taft, writing for the majority, explained that Olmstead's Fourth Amendment rights were not infringed because the wiretapping was not a search and seizure within the Fourth Amendment's meaning.[28] Instead, the Court concluded that the Fourth Amendment's language refers to actual physical examinations of one's person, papers, tangible material effects, or home, but not their conversations.[29] Finally, courts may not bar wiretapping simply because it may be viewed as unethical.[30] This slight lapse does not detract from the overall work.

There are many other familiar stories to Fourth Amendment scholars and enthusiasts. However, some of the more interesting and novel chapters are the ones that deal with license plate readers and the ability of the government to compel third parties to assist in unlocking cell phone passwords. These chapters do not describe

---

[20] *Id.* at 352.
[21] *Id.* at 361.
[22] *Katz*, 389 U.S. at 361.
[23] *See Habeas Data*, supra note 1, at 8–9.
[24] 277 U.S. 438 (1928).
[25] *Id.* at 457.
[26] *Id.* at 456.
[27] *Id.* at 457.
[28] *Id.* at 464–66.
[29] *Id.* at 466.
[30] *Olmstead*, 277 U.S. at 466, 468.

what has happened, but instead present to the reader where the law is and questions for where it is going.

In 2009, a few years after her retirement from the United States Supreme Court, Justice Sandra Day O'Connor founded iCivics to promote civic education.[31] Specifically, she sought "[t]o cultivate a new generation of students for thoughtful and active citizenship" because "[c]ivic knowledge is a prerequisite for civic participation," but it "had largely disappeared from school curricula."[32] These iCivics materials promote understanding of how basic American government functions as well as how the Constitution provides rights to us all. Think Schoolhouse Rock for the social media era.[33]

Regarding the federal government's attempts to compel Apple to assist in unlocking its password-protected cell phones, we learn of the notable example of the shooting in San Bernardino, California. Apple had been developing more and more advanced operating systems that provided its customers with better security features such that some of its cell phone were very difficult to access without the password for fear of destroying all of the data on the phone.[34] The FBI and other federal law enforcement agencies started filing motions seeking Apple's assistance pursuant to the All Writs Act,[35] which was first enacted in the Judiciary Act of 1789.[36]

Ultimately, the dispute between Apple and the FBI regarding the San Bernardino cell phone landed in federal district court.[37] However, before the trial court rendered any decision regarding the merits, FBI Director James Comey announced that the FBI accessed the shooter's cell phone with the assistance of another entity.[38] It turns out that the FBI had paid over $1,000,000.00 to Cellebrite for services allegedly to hack the cell phone.[39] This incident was not the first attempt by the federal government to compel Apple to assist in accessing a cell phone nor will it be the last. More importantly, it demonstrates the lengths that federal and state governments will go to access personal individual data.

---

[31] iCivics, https://www.icivics.org/our-story (last visited Aug. 16, 2019).
[32] *Id.*
[33] *See generally Schoolhouse Rock: The Preamble* (ABC television broadcast Nov. 1, 1975); *see generally Schoolhouse Rock: I'm Just a Bill* (ABC television broadcast Mar. 23, 1976).
[34] *See, e.g., In re Apple, Inc.,* 149 F.Supp.3d 341 (E.D.N.Y. 2016).
[35] *See* 28 U.S.C. § 1651 (West).
[36] *See* Act of Sept. 24, 1789, 1 Stat. 73.
[37] Matt Zapotosky, *FBI has accessed San Bernardino shooter's phone without Apple's help*, Washington Post, Mar. 28, 2016, https://www.washingtonpost.com/world/national-security/fbi-has-accessed-san-bernardino-shooters-phone-without-apples-help/2016/03/28/e593a0e2-f52b-11e5-9804-537defcc3cf6_story.html.

[38] *Id.*
[39] Ellen Nakashima, *FBI paid professional hackers one-time fee to crack San Bernardino iPhone*, Washington Post, April 12, 2016, https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html.

Similarly, Farivar wrote about the increasing usage of license plate readers. These devices became known to the public in a reality television show entitled *Parking Wars*, which followed city employees enforcing parking ordinances, including enforcement using license plate readers that would tell the employees a specific vehicle owed many tickets and should be secured with a parking boot.[40] As with other electronic technologies, there are often multiple uses. Indeed, these license plate readers are used throughout the Nation, mounted at various intersections and roadways as well as on police cruisers.

In *Habeas Data*, Farivar discusses how police use license plate readers in and around his native Oakland, California.[41] Police records establish that license plate readers can capture one's whereabouts in extensive ways.[42] Similarly, Farivar was able to obtain the police records of all the data that was captured. He contacted a person, whose license plate the Oakland Police Department had captured, and could tell that person where he lived and worked based on the data he obtained.[43] This incident provides another example how law enforcement and the government obtain and maintain significant amounts of personal data.

Without addressing them in detail, Farivar explains that there are other new methods of surveillance and invasions of privacy, including facial recognition and DNA monitoring.[44] His analysis is well-taken because individuals need to better understand and know their rights to keep the government in check. Otherwise, people will have to sing another classic anthem by The Clash: *I Fought The Law* (and the law won).[45] Indeed, without an informed populace, people run the risk of forfeiting constitutional rights. *Habeas Data* is an important book that serves as a primer on the Fourth Amendment and electronic surveillance.

---

[40] *See generally Parking Wars* (A&E television broadcast Feb. 11, 2012).
[41] *See Habeas Data*, supra note 1, at 81–87.
[42] *See Habeas Data*, supra note 1, at 82–84; *see also* Julia Angwin & Jennifer Valentino-DeVries, *New Tracking Frontier: Your License Plates*, The Wall Street Journal, (Sept. 29, 2012), https://www.wsj.com/articles/SB10000872396390443995604578004723603576296.
[43] *See* Cyrus Farivar, *We know where you've been: Ars acquires 4.6M license plate scans from the cops*, Ars Technica (Mar. 24, 2015, 8:00 AM), https://arstechnica.com/tech-policy/2015/03/we-know-where-youve-been-ars-acquires-4-6m-license-plate-scans-from-the-cops/.
[44] *See Habeas Data*, supra note 1, at 228. As Farivar's book was going to press, the Golden State Killer was tracked and ultimately captured in California based on DNA analysis from data obtained via an ancestry website. Gina Kolata & Heather Murphy, *The Golden State Killer Is Tracked Through a Thicket of DNA, and Experts Shudder*, The New York Times (Apr. 27, 2018), https://www.nytimes.com/2018/04/27/health/dna-privacy-golden-state-killer-genealogy.html.
[45] The Clash, *I Fought The Law* (CBS Records 1979).