Duke Law Journal

VOLUME 69 JANUARY 2020 NUMBER 4

PRESCRIPTION-DRUG POLICING: THE RIGHT TO HEALTH-INFORMATION PRIVACY PRE- AND POST-*CARPENTER*

JENNIFER D. OLIVA†

ABSTRACT

This Article operates at the intersection of privacy law, Fourth Amendment doctrine, and prescription-drug surveillance instigated by the U.S. drug-overdose crisis. Reputable reporting sources frequently frame that ongoing crisis as a prescription-drug-overdose "epidemic." Current epidemiological data, however, indicate that the majority of American overdose deaths are now a result of illicit and polysubstance drug use and not prescription-opioid misuse. The prescription-opioid-centric frame has nonetheless sparked the rapid rise of surveillance of prescribers and patients in the form of state prescription-drug monitoring program ("PDMP") databases. State PDMPs, which maintain and analyze significant data concerning every dispensed controlled substance, surreptitiously collect a stunning amount of sensitive health information.

PDMPs are predominantly law enforcement investigative tools dressed up in public-health-promoting rhetoric. Under the guise of rogue prescriber, pill mill, and doctor–shopper crackdowns, the Drug Enforcement Administration ("DEA") routinely self-issues subpoenas that permit the agency to conduct warrantless sweeps of the voluminous data stored in state PDMP databases. These rampant law enforcement sweeps procure highly sensitive health information and raise serious

† Associate Professor of Law, Seton Hall University School of Law; J.D., Georgetown University; M.B.A., University of Oxford; B.S., United States Military Academy. I thankfully acknowledge and appreciate thoughtful feedback from Jennifer Bard, Valena Beety, Leo Beletsky, Teneille Brown, John Jacobi, Orin Kerr, Christopher Slobogin, Ric Simmons, Nic Terry, Stacey Tovino, and Stacey-Rae Simcox.

constitutional privacy concerns. The Supreme Court's recent Fourth Amendment decision in Carpenter v. United States*, however, may limit the DEA's otherwise unfettered access to state PDMP databases.*

Carpenter *and the Fourth Amendment doctrines central to its holding motivate this Article and animate its two core contentions. First, pertinent pre-*Carpenter *precedent requires the DEA to obtain a warrant in order to conduct sweeps of state PDMP databases. Second, courts are even more likely to rule that warrantless DEA searches of highly sensitive health-care data run afoul of the Fourth Amendment in the post-*Carpenter *world. Simply stated, patient prescribing records stored in state PDMP databases are entitled to Fourth Amendment protection.*

TABLE OF CONTENTS

INTRODUCTION

> Physicians are not agents of the police power of government, and should not be forced to choose between protecting their patients against prosecution or protecting them against disease.[1]

The United States is in the throes of "the deadliest drug [overdose] crisis in American history."[2] Each day, nearly two hundred Americans die from drug overdoses;[3] in 2016, drug overdoses superseded car accidents as the number one cause of accidental deaths in the country.[4]

1. Amicus Curiae Brief of the Ass'n of Am. Physicians & Surgeons in Support of Respondent-Appellant Abbas T. Zadeh, in Support of Reversal at 8, United States v. Zadeh, 820 F.3d 746 (5th Cir. 2016) (Nos. 15-10202 & 15-10195), 2015 WL 4380678, at *8.

2. Maya Salam, *The Opioid Epidemic: A Crisis Years in the Making*, N.Y. TIMES (Oct. 26, 2017), https://www.nytimes.com/2017/10/26/us/opioid-crisis-public-health-emergency.html [https://perma.cc/S34L-UMZN].

3. HOLLY HEDEGAARD, MARGARET WARNER & ARIALDI M. MINIÑO, U.S. DEP'T OF HEALTH & HUMAN SERVS., DRUG OVERDOSE DEATHS IN THE UNITED STATES, 1999–2016, at 1 (Dec. 2017), https://www.cdc.gov/nchs/data/databriefs/db294.pdf [https://perma.cc/ZR22-C8BR].

4. Gillian Mohney, *Deaths from Opioid Overdoses Now Higher than Car Accident Fatalities*, HEALTHLINE (Mar. 30, 2018), https://www.healthline.com/health-news/deaths-from-opioid-overdoses-higher-than-car-accident-fatalities#1 [https://perma.cc/AT3M-A7JJ].

On October 26, 2017, President Donald J. Trump declared the drug-overdose crisis "a public health emergency."[5]

Journalists, public-health experts, and pundits frequently frame this public-health catastrophe as a *prescription-drug*-overdose crisis[6] primarily attributable to the overprescribing of opioid analgesics.[7] Even assuming this description of the overdose crisis was once accurate, the national health-data statistics tell a much different story today. According to the Centers for Disease Control and Prevention ("CDC"), nearly two-thirds of overdose deaths in 2016 were attributable to *illicit* substances, such as heroin, fentanyl, methamphetamines, cocaine, or some lethal combination thereof, and not *prescription* drugs.[8]

Moreover, the percentage of chronic-pain patients prescribed an opioid treatment regime who develop use disorder is exceedingly low. "[S]tudies show an incidence [of misuse of prescription opioids in such

5. Julie Hirschfeld Davis, *Trump Declares Opioid Crisis a 'Health Emergency' but Requests No Funds*, N.Y. TIMES (Oct. 26, 2017), https://www.nytimes.com/2017/10/26/us/politics/trump-opioid-crisis.html [https://perma.cc/U7AX-3WS8].

6. *See, e.g.*, Thomas C. Buchmueller & Colleen Carey, *The Effect of Prescription Drug Monitoring Programs on Opioid Utilization in Medicine*, 10 AM. ECON. J. 77, 78 (2018) ("The *misuse of prescription opioids* has become a serious epidemic in the United States." (emphasis added)); Sarah Vander Schaaff, *Amid the Opioid Crisis, Some Seriously Ill People Risk Losing Drugs They Depend On*, WASH. POST (July 14, 2018), https://www.washingtonpost.com/national/health-science/amid-the-opioid-crisis-some-seriously-ill-people-risk-losing-drugs-they-depend-on/2018/07/13/65850640-730d-11e8-805c-4b67019fcfe4_story.html [https://perma.cc/QGP9-EKR6] (reporting that "the nation [is] now fighting to reverse a drug epidemic fed *by prescription opioids*" (emphasis added)).

7. *See, e.g.*, Aaron Kessler, Elizabeth Cohen & Katherine Grise, *CNN Exclusive: The More Opioids Doctors Prescribe, the More Money They Make*, CNN (Mar. 12, 2018), https://www.cnn.com/2018/03/11/health/prescription-opioid-payments-eprise/index.html [https://perma.cc/Y25X-DWHV].

8. Press Release, U.S. Dep't of Health & Human Servs., Ctrs. for Disease Control & Prevention, U.S. Drug Overdose Deaths Continue to Rise; Increase Fueled by Synthetic Opioids (Mar. 29, 2018), https://www.cdc.gov/media/releases/2018/p0329-drug-overdose-deaths.html [https://perma.cc/7FP2-D825]; *see also* Nicolas Terry, *Reports on the Opioid Crisis Are Full of Misidentified Problems and Poorly Calibrated Solutions*, BILL HEALTH (July 19, 2018), http://blogs.harvard.edu/billofhealth/2018/07/19/reports-on-the-opioid-crisis-are-full-of-misidentified-problems-and-poorly-calibrated-solutions [https://perma.cc/VY94-S6CV] (explaining that "increasingly, the substance abuse crisis goes beyond opioids, with the . . . (DEA) recently reporting a significant spike in the availability and use of cocaine, and methamphetamine . . . on the rise nationwide" and "the . . . crisis now revolves around the abuse of non-prescription opioids by non-medical users, typified by . . . U.S. Post Office-delivered fentanyl").

patients ranging] from less than 1 percent to 8 percent."[9] As a recent study reaffirmed, most Americans who suffer opioid use disorder did not develop that disease in the normal course of indicated medical treatment.[10] They are more typically individuals with extensive histories of polysubstance use and misuse.[11]

The ongoing and flawed framing of the overdose crisis as a prescription-drug problem has provoked policymakers to focus on supply-side, law-enforcement-oriented solutions[12] while ignoring the root causes and socioeconomic drivers of drug consumption.[13] This supply-side-dominated approach has resulted in the enactment of numerous dragnet-style laws at the state and federal level aimed at cracking down on rogue prescribers, pain-pill mills, and prescription-drug "doctor shoppers."[14] It also has sparked the rapid rise of prescriber and patient surveillance in the form of federal monitoring legislation[15] and state prescription-drug monitoring programs ("PDMPs").[16]

---

9. Sally Satel, *The Truth About Painkiller Addiction*, ATLANTIC (Aug. 4, 2019), https://www.theatlantic.com/ideas/archive/2019/08/what-america-got-wrong-about-opioid-crisis/595090 [https://perma.cc/JAB7-W9LV].

10. Khary K. Rigg, Katherine McLean, Shannon M. Monnat, Glenn E. Sterner III & Ashton M. Verdery, *Opioid Misuse Initiation: Implications for Intervention*, 10 J. ADDICTIVE DISEASES 1 (2019).

11. *Id.*

12. *See, e.g.*, David Herzberg, Honoria Guarino, Pedro Mateu-Gelabert & Alex S. Bennett, *Recurring Epidemics of Pharmaceutical Drug Abuse in America: Time for an All-Drug Strategy*, 106 AM. J. PUB. HEALTH 408, 408 (2016) (explaining that, while "[s]upply-side and criminal justice approaches" continue to dominate U.S. drug policy, "history offers little evidence that primary reliance on such strategies can genuinely reduce problematic drug use").

13. *See, e.g.*, Nabarun Dasgupta, Leo Beletsky & Daniel Ciccarone, *Opioid Crisis: No Easy Fix to Its Social and Economic Determinants*, 108 AM. J. PUB. HEALTH 182, 182 (2018) (arguing that the root causes of the opioid crisis are "[e]roding economic opportunity, evolving approaches to pain treatment, and limited drug treatment"); Zachary Seigel, *The Opioid Crisis Is About More Than Corporate Greed*, NEW REPUBLIC (July 30, 2019), https://newrepublic.com/article/154560/opioid-crisis-corporate-greed [https://perma.cc/KL2V-N2RN] (arguing that the opioid crisis was fueled not by "a few bad apples in the pharmaceutical industry" but rather by the country's entire profit-driven health-care system and the neglectful or incompetent DEA).

14. *See, e.g.*, Jan Hoffman, *Medicare Is Cracking Down on Opioids. Doctors Fear Pain Patients Will Suffer*, N.Y. TIMES (Mar. 27, 2018), https://www.nytimes.com/2018/03/27/health/opioids-medicare-limits.html [https://perma.cc/D7FP-45YM]; Barry Meier, *A New Painkiller Crackdown Targets Drug Distributors*, N.Y. TIMES (Oct. 17, 2012), https://www.nytimes.com/2012/10/18/business/to-fight-prescription-painkiller-abuse-dea-targets-distributors.html [https://perma.cc/5WSV-L5Y6].

15. National All Schedules Prescription Electronic Reporting Act of 2005, Pub. L. No. 109–60, 119 Stat. 1979 (codified as amended at 42 U.S.C. § 208g-3 (2018)).

16. Buchmueller & Carey, *supra* note 6, at 2.

State PDMP laws mandate that dispensers report patients' prescription-related health information to an electronic database maintained and monitored by a designated state agency.[17] Every time a pharmacy dispenses a controlled substance to a patient, state PDMPs receive a host of sensitive health data, including the patient's name, address, age, and gender; the date and place the prescription is filled; the identity of the prescribing physician; the drug prescribed, the drug dosage; and the drug quantity.[18] PDMPs then make that information available to "authorized users," such as prescribers, pharmacists, and state medical boards. While the ostensible purposes of PDMPs vary across jurisdictions, the U.S. Department of Justice ("DOJ") contends that PDMPs "constitute a tool used primarily by medical professionals to enhance patient care when prescribing and dispensing controlled substances."[19] DOJ further claims that PDMPs provide medical professionals with access to real-time patient-prescribing data in order "to support the best clinical decisions regarding the appropriate treatment for patients, to reduce the likelihood of adverse drug reactions, and to assist with addiction treatment."[20]

DOJ's characterization of PDMPs as public-health-promoting tools, however, is unsurprisingly suspect. As explained in more detail below, there is no reliable evidence that supports the conclusion that PDMPs have either encouraged prescribers to provide evidence-based treatment to individuals with opioid use disorder or reduced the drug-overdose rate. Moreover, the United States has been engaged in an unproductive, decades-long "war on drugs," in which the government's go-to weapons have been surveillance, punishment, and incapacitation. DOJ is not in the business of providing addiction treatment that promotes evidence-based public-health outcomes. The agency's

17. *See, e.g.*, U.S. DEP'T OF JUSTICE, BUR. OF JUSTICE ASSISTANCE, JUSTICE SYSTEM USE OF PRESCRIPTION DRUG MONITORING PROGRAMS 5 (Jan. 2015), https://www.bja.gov/Publications/Global-JusticeSystemUsePDMPs.pdf [https://perma.cc/72KF-PFWJ].

18. *See generally* Christopher R. Smith, *Somebody's Watching Me: Protecting Patient Privacy in Prescription Health Information*, 36 VT. L. REV. 931, 931 (2012) (explaining that "[i]n today's ever-expanding world of internet technology and electronic data transmission, patient disclosure of prescription health information is being distributed to a widening circle of entities and individuals, raising serious patient privacy concerns, especially when the patient has not given consent to such dissemination").

19. JUSTICE SYSTEM USE OF PRESCRIPTION DRUG MONITORING PROGRAMS, *supra* note 17, at 5.

20. *Id.*

mission is to prosecute and punish "over prescribers" and individuals who suffer from drug-use disorders.

In fact, the United States has relegated many of the functions central to the regulation of controlled substances not to public-health experts but to a federal law enforcement agency—the U.S. Drug Enforcement Administration ("DEA")—for almost fifty years.[21] The DEA, which is a subagency within DOJ, derives its broad authority to classify, regulate, and surveil controlled substances from the Controlled Substances Act of 1970 ("CSA").[22] The CSA created a closed chain for controlled-substance distribution specifically designed to monitor legal products as they were transferred among DEA-registered handlers ("registrants") to prevent their "diversion"—that is, trade, sale, or other delivery—into the illicit market.[23]

The DEA manages diversion by maintaining strict control over the availability of controlled substances "through quotas, registration, recordkeeping, reporting, and security requirements."[24] The agency has described a CSA-compliant distribution of a controlled substance from manufacturer to patient as follows:

---

21. The DEA was created in 1973 by President Nixon by executive order. Exec. Order No. 11727, 38 Fed. Reg. 18,357 (July 10, 1973). It should be noted that, while the Food and Drug Administration ("FDA") has primary responsibility for ensuring the safety and effectiveness of pharmaceuticals, regardless of whether they are controlled substances under the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. §§ 301–99i (2018), the FDA does not have primary authority to regulate or monitor the use of controlled substances, JOHNATHAN H. DUFF, CONG. RES. SERV., OPIOID TREATMENT PROGRAMS AND RELATED FEDERAL REGULATIONS 1 (June 12, 2019), https://crsreports.congress.gov/product/pdf/IF/IF10219 [https://perma.cc/J6G7-CSHG] ("Under the Controlled Substances Act . . . the . . . DEA . . . in the Department of Justice (DOJ) has primary responsibility for regulating the use of controlled substances for legitimate medical, scientific, research, and industrial purposes, and for preventing these substances from being diverted for illegal purposes.").

22. Controlled Substances Act of 1970, Pub. L. No. 91-513, 84 Stat. 1236, 1242–84 (codified as amended at 21 U.S.C. §§ 801–971). Technically, the CSA delegates the duty to regulate controlled substances to the U.S. Attorney General. 21 U.S.C. § 801. The Attorney General, in turn, has delegated that authority by regulation to the DEA. 21 C.F.R. § 0.100(b) (2018).

23. *See, e.g.*, 21 U.S.C. § 823(a)(1) (explaining that, in determining whether to register a Schedule I or II manufacturer applicant, the DEA should consider "maintenance of effective controls against diversion of particular controlled substances and any controlled substance in schedule I or II compounded therefrom into other than legitimate medical, scientific, research, or industrial channels"); *see also* Gonzales v. Raich, 545 U.S. 1, 12–13 (2005) (observing that "[t]he main objectives of the CSA were to conquer drug abuse and to control the legitimate and illegitimate traffic in controlled substances" and pointing out that "Congress was particularly concerned with the need to prevent the diversion of drugs from legitimate to illicit channels" (footnote omitted)).

24. John A. Gilbert & Barbara Rowland, *Practicing Medicine in a Drug Enforcement World*, *in* HEALTH LAW HANDBOOK 394 (Alice G. Gosfield ed., 2015).

> [A] controlled substance, after being manufactured by a DEA-registered manufacturer, may be transferred to a DEA-registered distributor for subsequent distribution to a DEA-registered retail pharmacy. After a DEA-registered practitioner, such as a physician or a dentist, issues a prescription for a controlled substance to a patient (i.e., the ultimate user), that patient can fill that prescription at a retail pharmacy to obtain that controlled substance. In this system, the manufacturer, the distributor, the practitioner, and the retail pharmacy are all required to be DEA registrants, or to be exempted from the requirement of registration, to participate in the process.[25]

The CSA, in turn, requires controlled-substance manufacturers and distributors to submit reports detailing every sale, delivery, or other disposal of those drugs, including opioids, to the DEA.[26] These drug transaction reports are then uploaded to the DEA's Automation of Reports and Consolidated Orders System ("ARCOS") database, which summarizes them into reports that can be used to identify suspicious orders and the potential diversion of "high abuse potential" controlled substances, including prescription opioids.[27] Importantly, and unlike state PDMP databases, ARCOS does not track prescription opioids from the time of prescribing to the sale and dispensing of the drugs to the individual patient.[28] As a result, ARCOS does not store any sensitive, patient-identifying health-care data.

In addition to mandating that the DEA manage all controlled-substance transfers throughout the pharmaceutical-distribution chain,[29] the CSA delegates to the agency final authority to categorize

---

25. Disposal of Controlled Substances by Persons Not Registered with the Drug Enforcement Administration, 74 Fed. Reg. 3480, 3481 (Jan. 21, 2009) (to be codified at 21 C.F.R. pts. 1300, 1301, 1304, 1305, 1307).

26. 21 U.S.C. § 827(d)(1).

27. *Id.* § 827(d)(1); 21 C.F.R. § 1304.33. ARCOS is "an automated, comprehensive drug reporting system which monitors the flow of DEA controlled substances from their point of manufacture through commercial distribution channels to point of sale or distribution at the dispensing/retail level . . . ." Declaration of John J. Martin in Support of the United States of America's Brief Posing Objections to Disclosure of ARCOS Data at 2, *In re* Nat'l Prescription Opiate Litig., MDL No. 2804 (N.D. Ohio June 25, 2018). ARCOS data includes the following information for each CSA-regulated drug transaction: supplier's name, DEA registration number, address and business activity, buyer's name, DEA registration number and address, prescription-drug code, transaction date, total dosage units, and total grams. *Id.* The CSA also imposes specific duties upon wholesale distributors to monitor, identify, halt, and report "suspicious orders" of prescription opioids. 21 C.F.R. § 1301.74.

28. 21 U.S.C. § 827(d)(1); 21 C.F.R. § 1304.33.

29. Michael C. Barnes & Gretchen Arndt, *The Best of Both Worlds: Applying Federal Commerce and State Police Powers to Reduce Prescription Drug Abuse*, 16 J. HEALTH CARE L.

drugs, substances, and chemicals into five schedules (I–V) based on their medicinal utility and relative "abuse" potential.[30] The CSA defines Schedule I substances, which include, among other things, heroin, LSD, and cannabis, as drugs with "no currently accepted medical use in treatment in the United States"[31] and "a high potential for abuse."[32] Schedule II drugs are those that have both a medically accepted use[33] and a high potential for abuse.[34] Consequently, most opioids are classified as Schedule II controlled substances.[35]

The drugs enumerated in Schedules III–V, by contrast, have moderate to low potential for abuse.[36] State PDMPs nonetheless frequently monitor all Schedule II–V drugs—and even drugs that are unscheduled, which

> include a number of frequently prescribed medications used to treat a wide range of serious medical conditions, including nausea and weight loss in cancer patients undergoing chemotherapy, weight loss associated with AIDS, anxiety disorders, panic disorders, post-traumatic stress disorder, alcohol addiction withdrawal symptoms, opioid addiction, testosterone deficiency, gender identity/gender dysmorphia, chronic and acute pain, seizure disorder, narcolepsy, insomnia, and attention deficit hyperactivity disorder.[37]

& POL'Y 271, 281 (2013) ("Under the CSA, the DEA is responsible for preventing, detecting, and investigating diversion of controlled substances while ensuring the availability of these drugs for legitimate use.").

30. 21 U.S.C. § 812(b). The CSA also mandates that the DEA establish aggregate annual-production quotas for each basic class of controlled substance listed in Schedules I and II. *Id.* § 826.

31. *Id.* § 812(b)(1)(B).

32. *Id.* § 812(b)(1)(A).

33. *Id.* § 812(b)(2)(B).

34. *Id.* § 812(b)(2)(A).

35. 21 C.F.R. § 1308.12(b)–(c) (2018) (listing all Schedule II opium and opiate substances); *see also, e.g.*, DEA: U.S. DRUG ENF'T ADMIN., https://www.dea.gov/drug-scheduling [https://perma.cc/E69P-ZUMY] (explaining that "Schedule II drugs, substances, or chemicals are defined as drugs with a high potential for abuse, with use potentially leading to severe psychological or physical dependence," opining that "[t]hese drugs are also considered dangerous," and enumerating the following opioids as Schedule II drugs: "[c]ombination products with less than 15 milligrams of hydrocodone per dosage unit (Vicodin), . . . methadone, hydromorphone (Dilaudid), meperidine (Demerol), oxycodone (OxyContin), [and] fentanyl"). A small group of narcotic controlled substances, including the opioid agonist buprenorphine, which is used to treat opioid use disorder, and drugs that contain relatively low milligrams per dosage units of codeine, are classified as Schedule III substances. 21 C.F.R. § 1308.13(e).

36. 21 U.S.C. § 812(b)(3)–(5).

37. Brief for Plaintiffs-Intervenors-Appellees at 4, Or. Prescription Drug Monitoring Program v. U.S. Drug Enf't Admin., 860 F.3d 1228 (9th Cir. 2017) (No. 14-35402).

PDMPs, therefore, maintain a wealth of personal prescribing information that has no meaningful connection to the prescribing of either opioids or other substances with high potentials for misuse or diversion. The fact that Americans filled 4,063,166,658 prescriptions at retail pharmacies in 2017 alone places in context the extent of data that PDMPs collect on an annual basis.[38]

These data also happen to be both highly personal and incredibly revealing. This is because, in the age of personalized medicine and precision-targeted pharmacogenetic therapy, it is often possible to divine a patient's medical condition, diagnosis, or disease—and even the stage and severity of that condition, diagnosis, or disease—simply by reference to the patient's prescribing history.[39] A patient's prescribing information also details her contraceptive prescribing history and could reveal other reproductive-related health conditions or treatments, such as abortion, pregnancy, and infertility, depending on her indicated pharmaceutical treatment.[40] The open question, then, is whether PDMPs produce positive health-care outcomes in a manner that somehow justifies their exceptional privacy intrusions.

Unfortunately, the jury is still out as to whether PDMPs effectively reduce drug-overdose deaths, prevent problematic drug use, or impede diversion into illegal markets. Scholars have argued that prescription-drug monitoring actually exacerbates—rather than mitigates—the national drug-overdose crisis for at least four reasons.[41] First, PDMP surveillance and law enforcement scrutiny may encourage individuals

38. HENRY J. KAISER FAMILY FOUND., NUMBER OF RETAIL PRESCRIPTION DRUGS FILLED AT PHARMACIES BY PAYER (2017), https://www.kff.org/health-costs/state-indicator/total-retail-rx-drugs [https://perma.cc/73UA-WNNT]. This means that at least four-hundred million prescriptions are captured by PDMPs on an annual basis. BRIAN T. YEH, CONG. RES. SERV., R40548, LEGAL ISSUES RELATED TO THE DISPOSAL OF DISPENSED CONTROLLED SUBSTANCES 5 n.23 (Oct. 19, 2010), https://fas.org/sgp/crs/misc/R40548.pdf [https://perma.cc/A687-2BBS] ("[B]etween 10%-11% of all drug prescriptions written in the United States are for pharmaceutical controlled substances.").

39. Amicus Curiae Brief of the State Med. Ass'ns in Support of the Plaintiffs-Intervenors-Appellees at 23, *Or. Prescription Drug Monitoring Program*., 860 F.3d at 1228 ("[P]rescription records can reveal a patient's medical condition, treatment or diagnosis.").

40. *See, e.g.*, Doe v. Se. Pa. Transp. Auth., 72 F.3d 1133, 1138 (3d Cir. 1995) ("It is now possible from looking at an individual's prescription records to determine that person's illnesses, or even to ascertain such private facts as whether a woman is attempting to conceive a child through the use of fertility drugs.").

41. Scott M. Fishman et al., *Regulating Opioid Prescribing Through Prescription Monitoring Programs: Balancing Drug Diversion and Treatment of Pain*, 5 PAIN MED. 309, 311 (2004).

to forgo needed health-care treatment.[42] Second, mandatory PDMP reporting may incentivize physicians to avoid prescribing PDMP-monitored substances, even when medically indicated.[43] In fact, in May 2019, the New Hampshire Board of Medicine disciplined a Portsmouth physician for inappropriately restricting a chronic-pain patient's daily dose of his long-term opioid treatment regimen and then abandoning the patient after he developed suicidal ideation stemming from inadequate pain management.[44] After an investigation, the Board of Medicine determined that the physician violated the ethical standards of professional conduct that apply to medical doctors in New Hampshire.[45] As one news outlet reported:

> [The Board's] conclusion highlights how concerns about the "opioid crisis," reinforced by real or perceived demands from the government, have perverted the doctor-patient relationship, making physicians agents of the war on drugs, which is inconsistent with their professional duties. The medical board's decision suggests that New Hampshire regulators understand the dangers of those conflicting priorities. Perhaps not coincidentally, New Hampshire is also fighting the Drug Enforcement Administration's demands for warrantless access to [PDMP] records.[46]

Moreover, physician imposition of rapid, involuntary opioid tapering and abandonment of chronic-pain patients in response to increasing threats of law enforcement investigation and prosecution is

---

42. *See, e.g.*, Linda A. Johnson, *Americans Are Filling Fewer Prescriptions for Opioids Amid Rising Fear of Addiction*, TIME (Apr. 19, 2018), https://www.yahoo.com/news/americans-filling-fewer-prescriptions-opioids-154016384.html [https://perma.cc/K6T7-63TS].

43. M. Mofizul Islam & Ian S. McRae, *An Inevitable Wave of Prescription Drug Monitoring Programs in the Context of Prescription Opioids: Pros, Cons and Tensions*, 15 BMC PHARMACOLOGY & TOXICOLOGY 1, 2 (2014).

44. Jacob Sullum, *State Regulators Punish Doctor for Cutting a Pain Patient's Opioid Dose and Dropping Him After He Became Suicidal*, REASON (July 10, 2019, 12:45 PM), https://reason.com/2019/07/10/state-regulators-punish-doctor-for-cutting-a-pain-patients-opioid-dose-and-dropping-him-after-he-became-suicidal [https://perma.cc/3YN4-BL2K].

45. Shawne K. Wickham, *Portsmouth Doctor Reprimanded for Treatment of Chronic Pain Patient*, N.H. UNION LEADER (July 6, 2019), https://www.unionleader.com/news/health/portsmouth-doctor-reprimanded-for-treatment-of-chronic-pain-patient/article_d45611d5-f0e3-5a8f-ace5-46bc9d945c90.html [https://perma.cc/89FG-Y4XX].

46. Sullum, *supra* note 44.

no minor matter.[47] Approximately fifty million Americans suffer from chronic pain.[48]

Third, study data link PDMP surveillance and law enforcement supply-side crackdowns on prescription drugs to the dramatic spike in illicit drug misuse and overdose.[49] Washington State, for example, has realized a 40 percent decrease in overdoses linked to prescription opioids since 2009, yet "there's been little progress in driving down the rate of opioid overdoses overall."[50] This is because the state has seen a dramatic uptick in overdoses attributable to heroin and illicit fentanyl.[51] Finally, "[m]onitoring programs and the predictive technologies that they deploy may perpetuate biases and have a disproportionate impact on underprivileged citizens, given their common roots with other kinds of surveillance of poor, immigrant, and stigmatized communities."[52] The bottom line is that "we do not have a firm understanding of PDMPs' effectiveness, nor the potential for unintended PDMP consequences or other legal or ethical quagmires."[53]

---

47. Nina Shapiro, *Amid Pressure to Prescribe Fewer Opioids, Doctors Struggle to Ease Patients' Pain*, SEATTLE TIMES (June 9, 2019 4:24 PM), https://www.seattletimes.com/seattle-news/health/amid-pressure-to-prescribe-fewer-opioids-doctors-struggle-to-ease-patients-pain [https://perma.cc/PZF9-JP8C] ("Health-care providers who [treat patients on opioids] – and many refuse – face stigma, a tangle of rules and guidelines, medical and ethical challenges and potential scrutiny that has not only shut down clinics locally and nations but has led to arrests.").

48. James Dahlhamer et al., *Prevalence of Chronic Pain and High-Impact Chronic Pain Among Adults – United States, 2016*, 67 MORBIDITY & MORTALITY WKLY REP. 1001, 1002 (2018), https://www.cdc.gov/mmwr/volumes/67/wr/pdfs/mm6736a2-H.pdf [https://perma.cc/9P3L-7SVF].

49. *See, e.g.*, Theodore J. Cicero, Matthew S. Ellis & Hilary L. Surratt, *Effect of Abuse-Deterrent Formulation of Oxycontin*, 367 NEW ENG. J. MED. 187, 189 (2012); Pradip K. Muhuri, Joseph C. Gfroerer & M. Christine Davies, *Associations of Nonmedical Pain Reliever Use and Initiation of Heroin Use in the United States*, SUBSTANCE ABUSE AND MENTAL HEALTH SERVS. ADMIN., CTR. FOR BEHAVIORAL HEALTH STATISTICS & QUALITY (2013), https://www.samhsa.gov/data/sites/default/files/DR006/DR006/nonmedical-pain-reliever-use-2013.htm [https://perma.cc/AB34-EFCU]; U.S. DEP'T OF JUSTICE, NAT'L DRUG INTELLIGENCE CTR., *Narcotics*, *in* NATIONAL DRUG THREAT ASSESSMENT 2003 (2003), http://www.justice.gov/archive/ndic/pubs3/3300/pharm.htm [https://perma.cc/L5C3-P2WR]; U.S. DEP'T OF JUSTICE, NAT'L DRUG INTELLIGENCE CTR., NATIONAL DRUG THREAT ASSESSMENT 2011, at 37 (2011), http://www.justice.gov/archive/ndic/pubs44/44849/44849p.pdf [https://perma.cc/B5CJ-CW7P].

50. Shapiro, *supra* note 47.

51. *Id.*

52. Leo Beletsky, *Deploying Prescription Drug Monitoring to Address the Overdose Crises: Ideology Meets Reality*, 15 IND. HEALTH L. REV. 139, 142 (2018).

53. Rebecca L. Haffajee, *Preventing Opioid Misuse with Prescription Drug Monitoring Programs: A Framework for Evaluating the Success of State Public Health Laws*, 67 HASTINGS L.J. 1621, 1637 (2016).

What is clear is that PDMPs are extremely popular with law enforcement agencies, including the DEA. Several states expressly require law enforcement to obtain a warrant to access PDMP data.[54] The DEA, however, contends that those state warrant requirements are preempted by the CSA.[55] The DEA has broad power under the CSA to issue administrative subpoenas to investigate drug crimes.[56] CSA § 876 subpoenas permit the DEA to access any and all records it finds *relevant or material* to a drug investigation without a court order.[57] The DEA's widespread use of agency-issued administrative subpoenas to conduct warrantless searches of the myriad, individually identifying health information collected by PDMP databases raises serious Fourth Amendment concerns. These concerns likely existed under longstanding Fourth Amendment case law. A recent Supreme Court decision, *Carpenter v. United States*,[58] bolsters this contention.

Carpenter held that the government must obtain a warrant to access an individual's historic cell-site-location information.[59] *Carpenter* and the Fourth Amendment doctrines central to its holding motivate this Article and animate its two core contentions. First, pertinent, pre-*Carpenter* precedent requires the DEA to obtain a warrant in order to conduct sweeps of state PDMP databases to search patient prescribing information. Second, courts are even more likely to rule that warrantless DEA searches of such sensitive and revealing prescribing information run afoul of the Fourth Amendment in the post-*Carpenter* world.

This Article proceeds in five parts. Part I provides a brief overview of the American drug-overdose crisis. It then chronicles the explosion of PDMPs created in response to that crisis and critiques the DEA's ability to access and mine PDMP data without individualized suspicion, probable cause, or judicial review under its CSA administrative-subpoena authority. It maintains that the current framing of the U.S.

54. PRESCRIPTION DRUG MONITORING PROGRAM TRAINING & TECH. ASSISTANCE CTR., LAW ENFORCEMENT ACCESS TO PDMP REPORTS (Aug. 24, 2017), http://www.pdmpassist.org/pdf/Law_Enforcement_Access_Methods_20170824.pdf [https://perma.cc/V68Q-NYH9] (demonstrating that at least twenty-eight states require law enforcement to obtain a warrant or court order to obtain PDMP data).

55. 21 U.S.C. §§ 801–971 (2018).

56. *Id.* § 876(a).

57. *Id*.

58. Carpenter v. United States, 138 S. Ct. 2206 (2018).

59. *See id.* at 2217 n.3 ("It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.").

drug-overdose crisis has contributed to the development of law-enforcement-centric public policy solutions, including overbroad and potentially counterproductive prescription-drug surveillance. Part I further contends that state PDMPs are targets for abuse by overzealous law enforcement due to the troves of sensitive, individually identifying health information that they collect and store. Part II examines two pre-*Carpenter* federal district court cases involving Fourth Amendment challenges to DEA administrative subpoenas demanding prescribing data from state PDMPs. Part III evaluates whether state PDMP health information is entitled to Fourth Amendment protection under applicable pre-*Carpenter* precedent. Part IV introduces and examines *Carpenter*. Part V applies *Carpenter* to DEA PDMP searches and concludes that PDMP prescribing data is entitled to Fourth Amendment protection. It then concludes by identifying challenges to the analysis presented, including the potential application of the highly regulated industries exception to the warrant requirement.

I. THE RISE OF EXPANSIVE STATE PDMPS

> It seems that, far more than prescribed opioids, the unpredictability of heroin and the turbocharged lethality of fentanyl have been a prescription for an overdose disaster.[60]

A. PDMP Provocation: The U.S. Drug-Overdose Crisis

The United States is in the midst of an extravagant drug-overdose crisis. According to the CDC, 70,237 Americans died of a drug overdose in 2017 alone.[61] Moreover, over two-thirds of those deaths, or 47,600 overdoses, involved an opioid.[62] Drug-overdose deaths are now the most common cause of death for Americans under the age of fifty.[63]

---

60. Sally Satel, *The Myth of What's Driving the Opioid Crisis: Doctor-Prescribed Painkillers Are Not the Biggest Threat*, POLITICO (Feb. 21, 2018), https://www.politico.com/magazine/story/2018/02/21/the-myth-of-the-roots-of-the-opioid-crisis-217034 [https://perma.cc/9MRU-8S54].

61. LAWRENCE SCHOLL, PUJA SETH, MBABAZI KARIISA, NANA WILSON & GRANT BALDWIN, U.S. DEP'T OF HEALTH & HUMAN SERVS., CTRS. FOR DISEASE CONTROL & PREVENTION, DRUG AND OPIOID-INVOLVED OVERDOSE DEATHS — UNITED STATES, 2013–2017 (2019), https://www.cdc.gov/mmwr/volumes/67/wr/mm675152e1.htm?s [https://perma.cc/8VHK-Z6V2].

62. *Id.*

63. Josh Katz, *You Draw It: Just How Bad Is the Drug Overdose Epidemic?*, N.Y. TIMES (Oct. 26, 2017), https://www.nytimes.com/interactive/2017/04/14/upshot/drug-overdose-epidemic-you-draw-it.html [https://perma.cc/9AQD-9TVH].

The precise nature of the overdose crisis and its causes, however, are hotly debated among prescribers, patients, politicians, and public-health experts. This is likely because the prevailing mainstream narrative—that the United States is suffering a *prescription*-opioid-overdose crisis[64] largely attributable to *physician overprescribing*[65]—is challenged by the evolving epidemiological data. Those data demonstrate that (1) "deaths involving prescription painkillers have levelled off";[66] (2) opioid prescribing has decreased dramatically;[67] (3)

64. *See, e.g.*, Haffajee, *supra* note 53, at 1622 ("The United States is in the midst of a prescription opioid misuse crisis."); Bertha K. Madras, *The Surge of Opioid Use, Addiction, and Overdoses*, 74 JAMA PSYCHIATRY 441, 441 (2017) ("Prescription opioids remain a primary driver of opioid-related fatalities.").

65. *See* Dasgupta, Beletsky & Ciccarone, *supra* note 13, at 182 ("The accepted wisdom about the US opioid crisis singles out opioid analgesics as causative agents of harm, with physicians as unwitting conduits and pharmaceutical companies as selfish promoters . . . ."); *The Myth of an Opioid Prescription Crisis*, CATO INST. (Sept./Oct. 2017), https://www.cato.org/policy-report/septemberoctober-2017/myth-opioid-prescription-crisis [https://perma.cc/A4Q3-FARJ] (arguing that "only one-quarter of people who take opioids for nonmedical reasons get them by obtaining a prescription," "the opioid-related overdose rate for people who are on chronic pain medicine under the guidance of a doctor is 0.2 percent," and "that the big cause of overdose problems now is heroin"); Satel, *supra* note 60 ("The myth that the epidemic is driven by patients becoming addicted to doctor-prescribed opioids . . . [which] is now a media staple and a plank in nationwide litigation against drug makers . . . misconstrues the facts."); *see also, e.g.*, J. Baxter Oliphant, *Prescription Drug Abuse Increasingly Seen as U.S. Public Health Problem*, PEW RES. CTR. (Nov. 15, 2017), http://www.pewresearch.org/fact-tank/2017/11/15/prescription-drug-abuse-increasingly-seen-as-a-major-u-s-public-health-problem/ [https://perma.cc/W65X-EKXW] (pointing out that, in October 2017, "76% of the public sa[id] that prescription drug abuse is an extremely or very serious problem in America").

66. Beletsky, *supra* note 52, at 139; *see also* Josh Katz, *The First Count of Fentanyl Deaths in 2016: Up 540% in Three Years*, N.Y. TIMES (Sept. 2, 2017), https://www.nytimes.com/interactive/2017/09/02/upshot/fentanyl-drug-overdose-deaths.html [https://perma.cc/8QSC-D2UB] ("There is a downward trend in deaths from prescription opioids alone."); Maia Szalavitz, *Why Trump's Opioid Plan Will Harm More People Than It Will Save*, SELF (Mar. 28, 2018), https://www.self.com/story/trump-opioid-plan [https://perma.cc/CD94-XS9S] (explaining that "[d]octors are already prescribing opioids less frequently and reducing the average dose they're giving patients" and "[t]he most risky prescribing—high-dose opioid prescribing—was down in 86.5 percent of U.S. counties since 2010").

67. *See* Dasgupta, Beletsky & Ciccarone, *supra* note 13, at 183 ("Overdose deaths attributable to prescription opioids have not decreased proportionally to dispensing."); IQVIA INST. FOR HUMAN DATA SCIENCE, MEDICINE USE AND SPENDING IN THE U.S.: A REVIEW OF 2017 AND OUTLOOK TO 2022, at 20 (Apr. 19, 2018), https://www.iqvia.com/institute/reports/medicine-use-and-spending-in-the-us-review-of-2017-outlook-to-2022 [https://perma.cc/YK64-HSE9] (explaining that prescription-opioid volumes peaked in 2011 and have since declined by 29 percent, and that 23.3 billion fewer morphine milligram equivalents were dispensed to patients on a volume basis in 2017); Szalavitz, *supra* note 66 (notwithstanding the fact that "[t]he number of overall opioid prescriptions . . . has been falling for years . . . opioid overdose deaths in 30 states actually increased between 2010 and 2015, largely because of people switching to illegal drugs").

overdose deaths continue to rise;[68] and (4) overdose deaths are increasingly driven by the consumption of illicit opioids, such as street heroin and fentanyl,[69] as well as benzodiazepines, cocaine, and methamphetamine.[70] In fact, the rate of drug-overdose deaths involving fentanyl, fentanyl analogs, and tramadol doubled from 2015 to 2016[71] and was up 540 percent over the three-year period from 2014 to 2016.[72] Annual overdose deaths involving benzodiazepines, cocaine, and methamphetamine—often in combination with an opioid—also have spiked since 1999.[73]

Media coverage of the opioid crisis has thus been "marred by a false narrative that suggests most addictions start among pain patients who become 'accidentally' addicted, when in reality, nearly 75 percent of those who begin misusing prescription drugs do not get those substances directly from doctors."[74] The CDC recently acknowledged

68. John Gramlich, *As Fatal Overdoses Rise, Many Americans See Drug Addiction as a Major Problem in Their Community*, PEW RES. CTR. (May 30, 2018), http://www.pewresearch.org/fact-tank/2018/05/30/as-fatal-overdoses-rise-many-americans-see-drug-addiction-as-a-major-problem-in-their-community [https://perma.cc/6DCU-4PDA] ("Nationally, more than 63,600 people died of a drug overdose in 2016, the most recent year for which full data are available. . . . That's an increase of 21% from the prior year and nearly double the 34,425 drug overdose deaths that occurred a decade earlier.").

69. *See* Puja Seth, Rose A. Rudd, Rita K. Noonan & Tamara M. Haegerich, *Quantifying the Epidemic of Prescription Opioid Overdose Deaths*, 108 AM. J. PUB. Health 500, 500 (2018) ("From 2013 to 2014, fentanyl submissions increased by 426%. The increases were strongly correlated with increases in synthetic opioid deaths but not with pharmaceutical fentanyl prescribing rates, suggesting that the increases were largely due to [illicitly manufactured fentanyl]."); *see also* Katz, *supra* note 66 ("Drug overdoses are expected to remain the leading cause of death of Americans under 50, as synthetic opioids – primarily fentanyl and its analogues – continue to push the death count higher.").

70. *See, e.g.*, OHIO DEP'T OF HEALTH, 2017 OHIO DRUG OVERDOSE DATA: GENERAL FINDINGS 2 (2017), https://odh.ohio.gov/wps/wcm/connect/gov/5deb684e-4667-4836-862b-cb5eb59acbd3/2017_OhioDrugOverdoseReport.pdf?MOD=AJPERES [https://perma.cc/GCR7-DZN4] ("Cocaine-related overdose deaths as well as deaths involving methamphetamine/other psychostimulants increased substantially in 2017, and many of these deaths also involved an opioid like fentanyl and related drugs . . . ."); *Benzodiazepines and Opioids*, NAT'L INST. ON DRUG ABUSE (Mar. 2018), https://www.drugabuse.gov/drugs-abuse/opioids/benzodiazepines-opioids [https://perma.cc/AH4V-UCN5] ("More than 30 percent of overdoses involving opioids also involve benzodiazepines, a type of prescription sedative commonly prescribed for anxiety or to help with insomnia.").

71. Hedegaard, Warner & Miniño, *supra* note 3, at 5.

72. Katz, *supra* note 63.

73. *See Overdose Death Rates*, NAT'L INST. ON DRUG ABUSE (Jan. 2019), https://www.drugabuse.gov/related-topics/trends-statistics/overdose-death-rates [https://perma.cc/7943-YWZK] (featuring figures showing the increase in overdose deaths from various drugs from 1999 to 2017).

74. Szalavitz, *supra* note 66.

that it has perpetuated this narrative by overattributing opioid-overdose deaths to prescription painkillers. In an April 2018 article, the CDC conceded that it "[t]raditionally . . . includ[ed] synthetic opioid deaths in estimates of 'prescription' opioid deaths" and that such methodology overestimated the number of Americans who succumbed to prescription-opioid overdoses at 32,445 in 2016.[75] Using an updated methodology, which included "deaths involving only natural[,] semisynthetic opioids and methadone," the CDC ratcheted down its 2016 prescription-opioid-overdose death toll to 17,087 Americans, approximately 53 percent of its initial count.[76]

In July 2018, Food and Drug Administration Commissioner Scott Gottlieb issued a series of tweets acknowledging that the "opioid crisis [has] evol[ved] from an epidemic mostly involving prescription drugs to one that's increasingly fueled by illicit substances being purchased online or off the street."[77] He also admitted that "actions taken to curtail opioid abuse and misuse in one part of the market can be thwarted as demand shifts to other, even more dangerous channels."[78] A recent *Politico* article took a similar view, explaining that

> multiple surveys . . . show that only a minority of people who are prescribed opioids for pain become addicted to them, and those who do become addicted and who die from painkiller overdoses tend to obtain these medications from sources other than their own physicians. Within the past several years, overdose deaths are overwhelmingly attributable not to prescription opioids but to illicit fentanyl and heroin. These "street opioids" have become the engine of the opioid crisis in its current, most lethal form. If we are to devise sound solutions to this overdose epidemic, we must understand and acknowledge this truth about its nature.[79]

Notwithstanding the epidemiological data and expert commentary about the ever-evolving nature of the American drug-overdose crisis,

---

75. Seth et al., *supra* note 69, at 500.

76. *Id.*

77. Scott Gottlieb (@SGottliebFDA), TWITTER (July 1, 2018, 7:39 AM), https://twitter.com/SGottliebFDA/status/1013431855465598976 [https://perma.cc/32GG-4XTU]; *see also* Jeffery A. Singer, *FDA Commissioner Gottlieb's Sunday "Tweetorial" Is Both Encouraging and Frustrating*, CATO INST. (July 2, 2018, 5:06 PM), https://www.cato.org/blog/fda-commissioner-gottliebs-sunday-tweetorial-both-encouraging-frustrating [https://perma.cc/5EDF-MJFC] ("[T]he overdose crisis has always been primarily caused by non-medical users accessing drugs in a dangerous black market fueled by drug prohibition.").

78. Gottlieb, *supra* note 77.

79. Satel, *supra* note 60.

the media, policymakers, and even certain high-profile physicians continue to perpetuate the false narrative that the county's skyrocketing drug-related death rate is primarily fueled by prescription opioids. Needless to say, ill-defined public-health problems beget poorly designed and targeted public-health interventions. In this particular instance, the prescription-opioid narrative has provoked—and continues to encourage—supply-side, prescription-drug surveillance-centric responses to the crisis, including the ubiquitous adoption of privacy-intrusive PDMPs, with little consideration about those policies' potentially harmful collateral consequences.

B. PDMP Overview

PDMPs are state-administered electronic databases that collect, analyze, and make available prescription information on controlled substances dispensed by pharmacies and prescribers to "authorized users," such as physicians, dispensers, and state pharmaceutical and medical professional boards.[80] These databases often track all substances enumerated in Schedules II through V of the CSA as well as other nonscheduled "drugs of concern."[81] PDMPs are administered across jurisdictions by a wide variety of distinct state agencies ranging from state pharmacy and licensing boards to departments of health and law enforcement entities.[82]

Although the particularities pertaining to PDMP data collection differ among states, all jurisdictions collect the following information from dispensers: "[t]ype of drug dispensed," "[q]uantity of drug dispensed," "[n]umber of days a given quantity is supposed to last," "[d]ate dispensed," "prescriber and pharmacy identifiers," and "[p]atient identifiers," such as "name, address, zip code, and date of birth."[83]

---

80. Substance Abuse & Mental Health Servs. Admin., *Prescription Drug Monitoring Programs: A Guide for Healthcare Providers*, IN BRIEF, Winter 2017, at 1.

81. *See* PRESCRIPTION DRUG MONITORING PROGRAM TRAINING & TECH. ASSISTANCE CTR., DRUGS MONITORED BY PDMP (Dec. 5, 2017), http://www.pdmpassist.org/pdf/PDMP_Substances_Tracked_20171205.pdf [https://perma.cc/Q8BV-BG5J] (showing state PDMP monitoring schemes).

82. *See* PRESCRIPTION DRUG MONITORING PROGRAM TRAINING & TECH. ASSISTANCE CTR., PDMP BY OPERATING STATE AGENCY TYPE (Aug. 24, 2017), http://www.pdmpassist.org/pdf/PDMP_Agency_Type_20170824.pdf [https://perma.cc/8YST-QYMW] (showing the state agencies used to operate PDMP programs).

83. SAMHSA, CTR. FOR THE APPLICATION OF PREVENTION TECHNOLOGIES, USING PRESCRIPTION DRUG MONITORING PROGRAM DATA TO SUPPORT PREVENTION PLANNING, 1, 2 & n.3, https://www.edc.org/sites/default/files/uploads/pdmp-overview.pdf [https://perma.cc/

The majority of states mandate PDMP enrollment for prescribers or dispensers or both—the so-called "registration mandate."[84] A smaller number require that medical providers query the database—the "use mandate"—if they either suspect drug misuse or satisfy other objective criteria, such as the prescribing or dispensing of certain controlled substances or certain dosages of particular drugs.[85]

The fact that the majority of state PDMPs do not even require prescribers to query patient data proves that the databases are largely criminal and regulatory surveillance tools dressed up in public-health-promoting rhetoric.[86] The express purpose of these drug monitoring programs is to help enforcement agencies "identify problem patients, rogue prescribers, and pharmacists who may be diverting potentially addictive and otherwise risky drugs"[87] and, thereby, "deter 'aberrant' practices"[88] "in an effort to reduce prescription drug abuse."[89] According to the Prescription Drug Monitoring Program Training and Technical Assistance Center ("TAC"), the "overriding goal of PDMPs is to uphold both the state laws ensuring access to appropriate pharmaceutical care by citizens and the state laws deterring diversion"[90] of controlled substances.

More troubling, there is little evidence that even the state PDMPs that mandate prescriber use "ensure[] access to appropriate pharmaceutical care," "enhance patient care" or "assist in developing

---

4X7X-EJBJ].

84. *See* PRESCRIPTION DRUG MONITORING PROGRAM TRAINING & TECH. ASSISTANCE CTR., PDMP MANDATORY ENROLLMENT OF PRESCRIBERS AND DISPENSERS (Aug. 2018), http://www.pdmpassist.org/pdf/Mandatory_Enrollment_20180801.pdf [https://perma.cc/W4UG-LKDB] (showing that forty states plus Guam have implemented a registration mandate).

85. *See* PRESCRIPTION DRUG MONITORING PROGRAM TRAINING & TECH. ASSISTANCE CTR., CRITERIA FOR MANDATORY QUERY OF PDMP (Jan. 2, 2018), http://www.pdmpassist.org/pdf/Mandatory_Query_Conditions_20180102.pdf [https://perma.cc/USS5-25LJ] (outlining state-by-state mandatory-query criteria).

86. PRESCRIPTION DRUG MONITORING PROGRAM TRAINING & TECH. ASSISTANCE CTR., TECHNICAL ASSISTANCE GUIDE: HISTORY OF PRESCRIPTION DRUG MONITORING PROGRAMS 2 (Mar. 2018) [hereinafter HISTORY OF PDMPS], http://www.pdmpassist.org/pdf/PDMP_admin/TAG_History_PDMPs_final_20180314.pdf [https://perma.cc/B7VX-CLWX] ("The earliest PDMPs were established primarily as enforcement and regulatory tools providing data to officials responsible for enforcing drug laws and overseeing the prescribing and dispensing of these drugs by health care professionals.").

87. Beletsky, *supra* note 52, at 140.

88. *Id.*

89. Wendy K. Mariner, *Reconsidering Constitutional Protection for Health Information Privacy*, 18 U. PA. J. CONST. L. 975, 989 (2016); *see also* HISTORY OF PDMPS, *supra* note 86, at 2.

90. HISTORY OF PDMPS, *supra* note 86, at 2.

drug abuse prevention and treatment strategies."[91] "Although mandates are not meant to deter opioid prescribing per se, resistant clinicians may simply decline to prescribe opioids, raise prescribing thresholds, refer patients elsewhere, or substitute to non-monitored drugs—all of which could compromise appropriate symptom management."[92] PDMP mandates, in other words, "pressure[] doctors to cut back on prescribing, and then their legitimately suffering patients are driven to the illegal market where they get laced opioids, or they go to cheaper heroin and, of course, that is where the overdoses occur."[93]

A recent summary of various studies examining the effects of PDMPs pointed to research indicating that prescription-drug surveillance was neither associated with decreases in nonmedical use of controlled substances nor reductions in drug-overdose mortality rates.[94] One of those studies, in fact, concluded that "implementation of PDMPs was associated with an 11 percent increase in drug overdose mortality."[95] "Rising overdose mortality[,] despite decreasing opioid prescribing[,] suggests that merely reducing the prescription-opioid supply will have little positive short-term impact. Reducing prescribing could even increase the death toll as people with opioid use disorder or untreated pain shift into the unstable, illicit drug market."[96] In sum, PDMPs may operate to put additional lives at risk by incentivizing opioid patients to opt out of the health-care delivery system to avoid law enforcement surveillance and possible prosecution.

---

91. Haffajee, *supra* note 53, at 1621 (explaining that "PDMP policies are widespread . . . [and] largely uninformed by robust evidence or a systematic assessment of best practices" and "[w]hether [PDMPs] successfully reduce opioid misuse and overdoes remains unclear").

92. Rebecca L. Haffajee, Anupam B. Jena & Scott G. Weiner, *Mandatory Use of Prescription Drug Monitoring Programs*, 313 JAMA PSYCHIATRY 891, 892 (2015).

93. *The Myth of an Opioid Prescription Crisis*, *supra* note 65.

94. JANET WEINER, YUHUA BAO & ZACHARY MEISEL, PENN LEONARD DAVIS INST. OF HEALTH ECON., PRESCRIPTION DRUG MONITORING PROGRAMS: EVOLUTION AND EVIDENCE 5 (June 8, 2017), https://ldi.upenn.edu/brief/prescription-drug-monitoring-programs-evolution-and-evidence [https://perma.cc/D4YR-GT5Y].

95. Guohua Li et al., *Prescription Drug Monitoring and Drug Overdose Mortality*, INJURY EPIDEMIOLOGY 1, 3 (2014), https://link.springer.com/content/pdf/10.1186%2F2197-1714-1-9.pdf [https://perma.cc/M97C-2YZZ].

96. Sarah E. Wakeman & Michael L. Barnett, *Primary Care and the Opioid-Overdose Crisis: Buprenorphine Myths and Realities*, 397 NEW ENG. J. MED. 1, 3 (2018); *The Myth of an Opioid Prescription Crisis*, *supra* note 65.

C. Law Enforcement Access to PDMP Data

The DEA has repeatedly invoked its authority to conduct warrantless searches of patient prescribing data by issuing administrative subpoenas to state PDMPs pursuant to the CSA.[97] The CSA expressly empowers the DEA to self-issue administrative subpoenas to investigate drug crimes.[98] Under § 876 of the Act, the DEA "may subpoena witnesses, compel the attendance and testimony of witnesses, and require the production of any records (including books, papers, documents, and other tangible things which constitute or contain evidence) which the [agency] finds relevant or material to the investigation."[99] DEA administrative subpoenas are not subject to a probable cause requirement, are issued without court scrutiny or approval, and are judicially enforceable "to compel [the] compliance" of recipients.[100]

The DEA concedes that it frequently utilizes administrative subpoenas to search state PDMP databases,[101] including in states that require law enforcement to secure a warrant in order to access PDMP information.[102] Because PDMP prescribing information is highly sensitive, state agencies, prescribers, and patients in at least three jurisdictions have challenged the DEA's self-issuance of these general-warrant-like subpoenas on Fourth Amendment and due process grounds.[103] To date, the DEA has successfully invoked, among other things, federal preemption defenses and the Fourth Amendment third-party doctrine,[104] which has traditionally held that a person forfeits any

97. 21 U.S.C. §§ 801–971 (2018).

98. *Id.* § 876(a).

99. *Id.*

100. *Id.* § 876(c).

101. Declaration of Diversion Investigator Robert Churchwell at 3, U.S. Dep't of Justice v. Utah Dep't of Commerce, 2017 WL 3189868 (D. Utah July 27, 2017) (No. 2:16-cv-611) (conceding that "[w]hen examining and reviewing the prescribing activities of a DEA registrant, one of the principle investigative resources available to DEA investigative personnel is information contained within the Prescription Database Monitoring Programs (PDMPs) of the various states").

102. Or. Prescription Drug Monitoring Program v. U.S. Drug Enf't Admin., 860 F.3d 1228, 1234 (9th Cir. 2017).

103. U.S. Dep't of Justice v. Ricco Jonas, No. 18-mc-56-LM, 2018 WL 6718579 (D.N.H. Nov. 1, 2018), *adopted by* No. 19-cv-030-LM, 2019 WL 251246 (D.N.H. Jan. 17, 2019); *Utah Dep't of Commerce*, 2017 WL 3189868; Or. Prescription Drug Monitoring Program v. U.S. Drug Enf't Admin., 998 F. Supp. 2d 957 (D. Or. 2014), *rev'd*, 860 F.3d 1228 (9th Cir. 2017).

104. *Or. Prescription Drug Monitoring Program*, 860 F.3d at 1234–35; *Utah Dep't of Commerce*, 2017 WL 3189868, at *6–9.

privacy interest or property right in information that she voluntarily turns over to a third party.[105]

II. PRE-*CARPENTER* PDMP LITIGATION: OREGON & UTAH CASES

Prior to the Supreme Court's *Carpenter* decision, the federal courts only had two occasions to examine the constitutionality of a DEA § 876 subpoena seeking data without a warrant from a state PDMP. Those cases were provoked by the Oregon and Utah PDMPs' refusals to comply with DEA administrative subpoenas pursuant to their respective states' statutory mandates denying law enforcement access to PDMP data without a warrant supported by probable cause. A thorough examination of the merits of the legal arguments raised in those cases first requires an overview of the pertinent Fourth Amendment and related legal doctrines on which the parties relied, which is provided in the following Section.

A. Fourth Amendment Overview

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."[106] The basic purpose of the Amendment is to safeguard "the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government, without regard to whether the government actor is investigating crime or performing another function."[107] In other words,

105. The most recent case, *United States Department of Justice v. Ricco Jonas*, is the only PDMP case that the DEA filed post-*Carpenter*. *Ricco Jonas*, 2018 WL 6718579, at *1. The *Ricco Jonas* litigation was provoked by the New Hampshire Board of Pharmacy's refusal to comply with a DEA § 876 subpoena seeking access to the state's PDMP data based on, among other things, the state's warrant requirement for law enforcement access to the database. *See* N.H. REV. STAT. ANN. § 318-B:35, I(b)(3) (2019) (providing that access to PDMP data shall be given to "[a]uthorized law enforcement officials on a case-by-case basis for the purpose of investigation and prosecution of a criminal offense *when presented with a court order based on probable cause*," meaning that "[n]o law enforcement agency or official shall have direct access to query program information" (emphasis added)). The Board lost before the United States District Court for the District of New Hampshire and the case is currently on appeal before the United States Court of Appeals for the First Circuit. *Ricco Jonas*, 2018 WL 6718579, at *7.

106. U.S. CONST. amend. IV.

107. City of Ontario v. Quon, 560 U.S. 746, 755–56 (2010); *see also* Camara v. Mun. Court of S.F., 387 U.S. 523, 528 (1967).

the Fourth Amendment "applies equally to civil and criminal law enforcement."[108]

Traditionally, courts interpreted the Fourth Amendment from a property-centric perspective and, as such, required an individual seeking its protection to establish that she had suffered a physical invasion of—or a trespass to—her private property at the hands of the government.[109] Constitutional jurisprudence, however, has evolved and now provides a second path for those who seek sanctuary in the skirts of the Fourth Amendment: the reasonable expectation of privacy test outlined by Justice Harlan in his *Katz v. United States*[110] concurrence.[111]

The question in *Katz* was whether the FBI's use of a listening device attached to a phone booth to intercept the petitioner's telephone calls constituted a "search" for Fourth Amendment purposes.[112] The *Katz* Court answered that question in the affirmative and rejected the traditional notion that a Fourth Amendment "search" is limited to instances that involve a "physical intrusion" into a "constitutionally protected area."[113] In doing so, the Court famously asserted that the Fourth Amendment "protects people, not places."[114]

---

108. Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 758 (1994).

109. *See, e.g.*, Nita A. Farahany, *Searching Secrets*, 160 U. PA. L. REV. 1239, 1245 (2012) (explaining property law's longstanding "stranglehold on Fourth Amendment doctrine"); Jace C. Gatewood, *It's Raining* Katz *and* Jones*: The Implications of* United States v. Jones*—A Case of Sound and Fury*, 33 PACE L. REV. 683, 697 (2013) ("Historically, the doctrinal definition of a 'search' within the meaning of the Fourth Amendment involved some physical intrusion into a constitutionally protected area and, thus, trespass became the driving force behind Fourth Amendment protection."); Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 423 (2007) ("Prior to *Katz*, the Court largely defined a search as a function of some physical invasion by the government.").

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

111. *Id.* at 361 (Harlan, J., concurring); *see also, e.g.*, Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 105 (2008) (asserting that *Katz* "untethered" the Fourth Amendment from "the law of trespass").

112. *Katz*, 389 U.S. at 348.

113. *Id.* at 350–53; *see also id.* at 353 ("The premise that property interests control the right of the Government to search and seize has been discredited." (quoting Warden v. Hayden, 387 U.S. 294, 304 (1967)).

114. *Id.* at 351; *see also id.* at 361 (Harlan, J., concurring). As legal commentators have argued, "the Fourth Amendment's text both explicitly and implicitly addresses privacy rights. The explicit recognition of privacy rights arises from the enumeration of the people's right [t]o be secure in their persons [and] papers." Richard Sobel, Barry Horwitz & Gerald Jenkins, *The Fourth Amendment Beyond* Katz*,* Kyllo *and* Jones*: Reinstating Justifiable Reliance as a More Secure Constitutional Standard for Privacy*, 22 B.U. PUB. INT. L.J. 1, 6 (2013). Moreover, "[i]mplicit recognition of the right to privacy, and a basis for its protections in an evolving technological

Justice Harlan concurred with that sentiment and created a two-pronged test, which provides that a Fourth Amendment search has occurred when (1) an individual has a subjective expectation of privacy in the items or area searched and (2) society recognizes that expectation as objectively reasonable.[115]

The Supreme Court adopted Justice Harlan's privacy test a dozen years later in *Smith v. Maryland*.[116] The *Smith* Court did not just invoke the test; rather, it applied its principles to arrive at the Court's most expansive interpretation of the third-party doctrine.[117] As the Court explained, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," and thus, no right to invoke the Fourth Amendment to protect such information from search or seizure.[118] The *Smith* Court went on to hold that the petitioner had no reasonable expectation of privacy in information he had voluntarily turned over to his telephone company.[119]

The evolution of the *Katz* test and the third-party doctrine are critical to understanding the arguments advanced by the parties in the Oregon and Utah PDMP cases. An additional line of cases that involve the standard applicable to administrative subpoenas, including *Oklahoma Press Publishing Co. v. Walling*[120] and *United States v.*

environment, can also be found in the final enumerated term: the security of one's 'effects.'" *Id.* at 7.

115. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

116. Smith v. Maryland, 442 U.S. 735, 740–41 (1979).

117. Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1930–31 (2017) (explaining that "[t]he third party doctrine has remained relatively undisturbed in the years since *Smith*" and "[o]ver time, it seems that the *Smith* inquiry and its application has calcified into a binary one, in which any information disclosed to a third party for any reason is public and does not merit Fourth Amendment protection"). As this Article further points out, even Stephen Sachs, the then-Attorney General who argued *Smith* on behalf of the State of Maryland in 1979, has acknowledged how dangerously expansive the decision is—and has become—in the modern day. *Id.* at 1933 (citing *1979 Supreme Court Ruling Becomes Focus of NSA Tactics*, NPR (Dec. 21, 2013, 5:13 PM), http://www.npr.org/2013/12/21/256114227/1979-supreme-court-ruling-becomes-focus-of-nsa-tactics [https://perma.cc/38QB-4CSX] (pointing out that Sachs told NPR that "[t]he current situation is really a far cry from the world in 1979. . . . The massive intrusion now is world's [sic] apart from what we argued in 1979. . . . I don't even like the notion that this is part of my legacy").

118. *Smith*, 442 U.S. at 743–44.

119. *Id.* at 747.

120. Okla. Press Publ'g Co. v. Walling, 327 U.S. 186 (1946).

Morton Salt Co.,[121] was particularly important in the Utah litigation.[122] In lockstep with those decisions, the Tenth Circuit held in *Becker v. Kroll*[123] that "an investigatory or administrative subpoena is not subject to the same probable cause requirements as a search warrant."[124] Instead, "the Fourth Amendment requires only that a subpoena be 'sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome.'"[125] As explained below, the Utah district court relied on *Becker*'s "reasonable relevance" test in its decision to enforce the DEA's § 876 subpoena.

B. Oregon PDMP v. U.S. DEA[126]

The Oregon legislature created its statewide PDMP in 2009.[127] Oregon's PDMP statute requires all in-state pharmacies to report the following information to its electronic database upon dispensing any Schedule II–IV drug: (1) the name, address, and date of birth of the patient; (2) the identification of the pharmacy; (3) the identification of the practitioner who prescribed the drug; (4) the identification of the drug; (5) the date of the prescription; (6) the date the drug was dispensed; and (7) the quantity of the drug dispensed.[128] "The primary purpose of the PDMP is to provide practitioners and pharmacists a tool to improve health care, by providing health care providers with a means to identify and address problems related to the side effects of drugs, risks associated with the combined effects of prescription drugs . . . and overdose."[129]

Oregon's PDMP statute expressly provides that prescription monitoring data constitutes protected health information ("PHI") and,

121. United States v. Morton Salt Co., 338 U.S. 632 (1950).

122. U.S. Dep't of Justice v. Utah Dep't of Commerce, No. 2:16-cv-611, 2017 WL 3189868, at *5 (D. Utah July 27, 2017).

123. Becker v. Kroll, 494 F.3d 904 (10th Cir. 2007).

124. *Id.* at 916 (citing See v. City of Seattle, 387 U.S. 541, 544 (1967)).

125. *Id.*

126. Or. Prescription Drug Monitoring Program v. U.S. Drug Enf't Admin., 860 F.3d 1228 (9th Cir. 2017).

127. *See* OR. REV. STAT. § 431.962 (2014).

128. *Id.* § 431.964(1)(a)–(g); *see also* Or. Prescription Drug Monitoring Program v. U.S. Drug Enf't Admin., 998 F. Supp. 2d 957, 960 (D. Or. 2014), *rev'd*, 860 F.3d 1228 (9th Cir. 2017).

129. *Or. Prescription Drug Monitoring Program*, 998 F. Supp. 2d at 960 (citation omitted) (quotations omitted).

as such, is subject only to limited disclosure.[130] In fact, neither physicians nor pharmacists may access PDMP data unless they "certif[y] that the requested information is for the purpose of evaluating the need for or providing medical or pharmaceutical treatment for a patient to whom the practitioner or pharmacist anticipates providing, is providing or has provided care."[131] The statute also prohibits the PDMP custodian from disclosing prescribing data to law enforcement without a warrant.[132]

Notwithstanding that warrant requirement, the DEA served at least two separate § 876 administrative subpoenas on the Oregon PDMP in 2012.[133] The first, which was served on September 11, 2012, requested an individual patient's prescribing information.[134] The second, which was served six days later, demanded a "summary of all prescription drugs prescribed by two physicians."[135]

The Oregon PDMP refused to comply with those administrative subpoenas.[136] Instead, it filed a complaint in federal district court seeking a declaration that "it cannot be compelled to disclose an individual's protected health information to the DEA pursuant to an administrative subpoena unless so ordered by a federal court."[137] Shortly thereafter, the American Civil Liberties Union of Oregon, four John Doe patients, and Dr. James Roe intervened in the action and challenged the DEA's issuance of the subpoenas on Fourth Amendment grounds.[138]

The district court analyzed the parties' Fourth Amendment claim under the *Katz* reasonable expectation of privacy test. The court

130. OR. REV. STAT. § 431.966(1)(a)(A) (2014) (expressly stating that "prescription monitoring information submitted . . . to the prescription monitoring program . . . [i]s protected health information").

131. *Or. Prescription Drug Monitoring Program*, 998 F. Supp. 2d at 960 (quoting OR. REV. STAT. § 431.966(2)(a)).

132. OR. REV. STAT. § 431.966(2)(a)(G) (providing that the PDMP may disclose such information only "[p]ursuant to a valid court order based on probable cause and issued at the request of a federal, state or local law enforcement agency engaged in an authorized drug-related investigation involving a person to whom the requested information pertains").

133. Memorandum in Support of Plaintiff's Motion for Summary Judgment at 4, *Or. Prescription Drug Monitoring Program*, 998 F. Supp. 2d 957 (No. 3:12-cv-12-2023).

134. Declaration of Nina Englander in Support of Motion for Summary Judgment at 2, *Or. Prescription Drug Monitoring Program*, 998 F. Supp. 2d 957 (No. 3:12-cv-12-2023).

135. *Id.*

136. *Id.*

137. Complaint for Declaratory Judgment at 4, *Or. Prescription Drug Monitoring Program*, 998 F. Supp. 2d 957 (No. 3:12-cv-12-2023).

138. *Or. Prescription Drug Monitoring Program*, 998 F. Supp. 2d at 959.

acknowledged that the intervenors were entitled to "invoke the protections of the Fourth Amendment" if they could show that "they have an actual (subjective) expectation of privacy and . . . that the expectation be one that society is prepared to recognize as 'reasonable.'"[139] With regard to the first prong of the *Katz* test, the court determined that "each of the patient intervenors has a subjective expectation of privacy in his prescription information, as would nearly any person who has used prescription drugs."[140] The court had forecasted that outcome earlier in its opinion when it acknowledged that

> depending on the drug prescribed, the information reported to PDMP can reveal a great deal of information regarding a particular patient including the condition treated by the prescribed drug. Schedule II–IV drugs can be used to treat a multitude of medical conditions including AIDS, psychiatric disorders, chronic pain, drug or alcohol addiction, and gender identity disorder.[141]

The court also held that physician–intervenor James Roe had "a subjective expectation of privacy in his prescribing information."[142] In reaching that conclusion, the court pointed to Dr. Roe's declaration, which "describ[ed] his duty of confidentiality to his patients and how law enforcement has made doctors, including himself, reluctant to prescribe schedule II–IV drugs where medically indicated."[143] The court further explained that "the DEA inserts itself into a decision that should ordinarily be left to the doctor and his or her patient" when it surveils prescribing data.[144]

The Oregon district court then proceeded to the second prong of *Katz*, which queries whether society is prepared to recognize the intervenors' subjective expectations of privacy as objectively reasonable. The court explained that "[m]edical records, of which prescription records form a not insignificant part, have long been treated with confidentiality."[145] It supported that statement by pointing to the ancient Hippocratic Oath, the Health Insurance Portability and

139. *Id.* at 964 (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).
140. *Id.* at 964.
141. *Id.* at 960.
142. *Id.* at 964.
143. *Id.*
144. *Id.*
145. *Id.*

Accountability Act ("HIPAA") Privacy Rule,[146] and the Ninth Circuit's decision in *Tucson Woman's Clinic v. Eden*,[147] which held that "all provision of medical services in private physicians' offices carries with it a high expectation of privacy for both physician and patient."[148] Ultimately, the "court easily conclude[d] that the intervenors' subjective expectation of privacy in their prescription information [wa]s objectively reasonable."[149] According to the court,

> it is more than reasonable for patients to believe that law enforcement agencies will not have unfettered access to their records. . . . By obtaining the prescription records for [certain intervenors], a person would know that they have used testosterone in particular quantities and by extension, that they have gender identity disorder and are treating it through hormone therapy. *It is difficult to conceive of information that is more private or more deserving of Fourth Amendment protection*.[150]

The court also rejected the DEA's argument that the third-party doctrine undermined the intervenors' reasonable expectation of privacy in their prescribing data.[151] In so doing, the court distinguished the leading third-party doctrine cases: *United States v. Miller*[152] and *Smith*. First, the court explained that PDMP records are "more inherently personal or private"[153] than the bank records in *Miller* and the dialed telephone numbers in *Smith* and, as such, are "entitled to and treated with a heightened expectation of privacy."[154] Second, it pointed out that, while *Miller* and *Smith* largely turned on the voluntary conveyance of the information at issue in those cases, "patients and doctors are not voluntarily conveying information to the PDMP" because those conveyances are "required by law."[155]

The DEA appealed the district court's ruling to the Ninth Circuit. The appellate court, however, held that the intervenors lacked standing to raise Fourth Amendment claims because they were not the targets

146. *Id.*

147. Tucson Woman's Clinic v. Eden, 379 F.3d 531, 550 (9th Cir. 2004).

148. *Id.* at 550.

149. *Or. Prescription Drug Monitoring Program*, 998 F. Supp. 2d at 966.

150. *Id.* (emphasis added) (citations omitted).

151. *Id.* at 967.

152. United States v. Miller, 425 U.S. 435 (1976).

153. *Or. Prescription Drug Monitoring Program*, 998 F. Supp. 2d at 967 (quoting United States v. Golden Valley Elec. Ass'n, 689 F.3d 1108, 1116 (9th Cir. 2012)).

154. *Id.*

155. *Id.*

of the DEA subpoenas at issue.[156] Although it was precluded from reaching the merits of the intervenors' Fourth Amendment challenge as a result of its standing determination, the Ninth Circuit did "acknowledge the particularly private nature of the medical information at issue."[157] The court also denied the Oregon PDMP's request for declaratory relief, which did not implicate the Fourth Amendment, on the theory that the Oregon warrant requirement was preempted by the CSA.[158]

C. DOJ v. Utah DOC[159]

Approximately four weeks after the Ninth Circuit decided the Oregon PDMP case, a Utah federal district court issued a decision based on similar facts. Utah created its state PDMP, which is administered by the Utah Department of Commerce ("DOC"), in 1995.[160] Utah's PDMP contains record data about "every prescription for a controlled substance dispensed in the state to any individual other than an inpatient in a licensed health care facility."[161] Specifically, Utah requires all nonhospital dispensers to electronically report the following information to its PDMP: (1) the name, date of birth, gender, and street address of the patient; (2) positive identification information for the patient; (3) the name of the prescriber; (4) the name of the drug; and (5) the strength, quantity, and dosage of the drug dispensed.[162]

On November 12, 2015, the DEA served an administrative subpoena on the Utah DOC requesting "all prescription records associated with DEA Registrant #1 for the time period of January 8, 2015 to present,"[163] including "all controlled substance prescriptions issued by the subject of the investigation and to whom these prescriptions were issued."[164] Much like Oregon, Utah's PDMP enabling statute requires law enforcement to obtain a warrant to access

156. Or. Prescription Drug Monitoring Program v. U.S. Drug Enf't Admin., 860 F.3d 1228, 1234–35 (9th Cir. 2017).

157. *Id.* at 1235.

158. *Id.* at 1236.

159. U.S. Dep't of Justice v. Utah Dep't of Commerce, No. 2:16-cv-611, 2017 WL 3189868 (D. Utah July 27, 2017).

160. UTAH CODE ANN. §§ 58-37f-101–801 (West 2016).

161. *Id.* § 58-37f-201(5)(a); *Utah Dep't of Commerce*, 2017 WL 3189868, at *3.

162. *See* UTAH CODE ANN. § 58-37f-203(3); UTAH ADMIN. CODE R156-37f-203(1)(a) (2019).

163. Declaration of Diversion Investigator Robert Churchwell at 4, *Utah Dep't of Commerce*, 2017 WL 3189868.

164. *Utah Dep't of Commerce*, 2017 WL 3189868, at *3.

PDMP data.[165] The Utah DOC, therefore, refused to comply with the administrative subpoena.[166] The DEA responded by filing a petition to enforce the subpoena in federal district court.[167] Several parties intervened in the action as respondents opposed to the DEA's petition, including the Salt Lake County Firefighters, Equality Utah, American Civil Liberties Union of Utah, and two John Doe patients.[168]

As alluded to previously, the Utah district court held that the DEA's administrative subpoena was subject to the *Becker v. Kroll*[169] "reasonable relevance test."[170] In *Becker*, the Tenth Circuit held that administrative investigatory subpoenas were not subject to the same threshold requirements as a Fourth Amendment warrant.[171] Instead, such subpoenas pass muster so long as they are "sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome."[172] Because the DEA subpoena at issue in the Utah PDMP litigation only "requested records for one specific physician for a limited time period," "[wa]s relevant in purpose," "[wa]s specific in directive," and was in response to an ongoing investigation, the district court found that it easily satisfied the reasonable relevance test.[173]

The court then evaluated whether the Utah patients and prescribers had a reasonable expectation of privacy in their PDMP data. Although the court acknowledged that "[m]edical records, including prescriptions, are no doubt personal and private matters," it concluded that the "expectation of privacy analysis nonetheless weighs in the DEA's favor," relying on the third-party doctrine and the highly regulated industries exception to the Fourth Amendment.[174]

165. UTAH CODE ANN. § 58-37f-301(2)(m) (stating that the Utah DOC is prohibited from disclosing PDMP data to law enforcement unless it is presented with a "valid search warrant . . . related to: (i) one or more controlled substances; and (ii) a specific person who is a subject of the investigation"); *see also* UTAH ADMIN. CODE R156-37f-301(5)(a) ("Federal, state and local law enforcement authorities and state and local prosecutors requesting information from the [PDMP] . . . shall provide a valid search warrant authorized by the courts . . . ."); *Utah Dep't of Commerce*, 2017 WL 3189868, at *1 ("[T]he State claims the Utah Controlled Substance Database Act (the 'Database Act') requires a warrant for law enforcement searches of the Database.").

166. *Utah Dep't of Commerce*, 2017 WL 3189868, at *3.

167. *Id.*

168. *Id.* at *1.

169. Becker v. Kroll, 494 F.3d 904 (10th Cir. 2007).

170. *Utah Dep't of Commerce*, 2017 WL 3189868, at *7.

171. *Becker*, 494 F.3d at 916.

172. *Id.* (quoting See v. City of Seattle, 387 U.S. 541, 544 (1967)).

173. *Utah Dep't of Commerce*, 2017 WL 3189868, at *7.

174. *Id.* at *8.

Consequently, the court granted the DEA's petition to enforce the subpoena.[175]

III. EVALUATING THE PDMP CASES UNDER PRE-*CARPENTER* PRECEDENT

The DEA advanced several arguments in its campaign to enforce the administrative subpoenas it served on the Oregon and Utah PDMPs. Specifically, the DEA argued that its administrative investigatory subpoena was exempt from the Fourth Amendment probable cause standard, the CSA preempted the states' warrant requirements, patients lacked any reasonable expectation of privacy in their prescribing data, and the third-party doctrine exempted the agency from the Fourth Amendment warrant requirement. This Section describes and dissects each of those contentions. In so doing, it argues that the Oregon district court reached the correct result and the Utah case was wrongly decided under the applicable pre-*Carpenter* precedent.

*A. Pre-*Carpenter *Administrative-Subpoena Cases*

The Supreme Court has deemed "searches conducted outside the judicial process . . . *per se* unreasonable . . . subject only to a few specifically established and well-delineated exceptions"[176] and has generally required individualized suspicion for warrantless searches.[177] There is a line of pre-*Carpenter* decisions, however, that hold that certain investigatory or administrative subpoenas are not subject to the Fourth Amendment probable cause requirement. Under those cases, which trace their lineage to *Oklahoma Press Publishing Co. v. Walling*[178] and *United States v. Morton Salt Co.*,[179] "when an

175. *Id.* at *9.

176. Katz v. United States, 389 U.S. 347, 357 (1967).

177. Chandler v. Miller, 520 U.S. 305, 308 (1997).

178. *See* Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 216 (1946) (determining that the administrator of the FTC's "investigative function" is "essentially the same as the grand jury's, or the court's in issuing other pretrial orders for the discovery of evidence, and is governed by the same limitations . . . that he shall not act arbitrarily or in excess of his statutory authority" but recognizing that "this does not mean that his inquiry must be 'limited . . . by forecasts of the probable result of the investigation. . . .'" (quoting Blair v. United States, 250 U.S. 273, 282 (1919))).

179. *See* United States v. Morton Salt Co., 338 U.S. 632, 652 (1950) (recognizing that "a governmental investigation into corporate matters may be of such a sweeping nature and so unrelated to the matter properly under inquiry as to exceed the investigatory power" but opining

administrative agency subpoenas *corporate books or records*, the Fourth Amendment requires [only] that the subpoena be sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome."[180]

The DEA based its authority to conduct warrantless searches of Oregon and Utah PDMP data primarily on these grounds and, in fact, prevailed on that argument in the Utah litigation. There, the DEA contended that that the court's role in reviewing an agency's petition to enforce an administrative subpoena is "strictly limited" to the reasonable relevance test.[181] As explained above, the Utah district court agreed and held that the DEA subpoena at issue easily satisfied that lenient standard of review.[182]

There are, however, at least two reasons to question whether the district court applied the right test in reaching its ruling in the Utah PDMP case. First, the cases on which the court relied in applying the reasonable relevance test are of suspect applicability because they expressly limit their holdings to administrative subpoenas seeking *corporate* books or records.[183] The prescribing data stored in state PDMPs, however, are patients' private health records—not corporate records. Second, the state agencies from which the DEA sought records in the PDMP cases are not corporations. Rather, they are

---

that "it is sufficient if the inquiry is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant" (citation omitted)).

180. See v. City of Seattle, 387 U.S. 541, 544 (1967) (emphasis added).

181. Memorandum in Support of Petition to Enforce DEA Administrative Subpoenas at 4, U.S. Dep't of Justice v. Utah Dep't of Commerce, No. 2:16-cv-611 (D. Utah June 14, 2016) (quoting United States v. Zadeh, 820 F.3d 746, 757 (5th Cir. 2016)). The DEA raised the same argument in the Oregon PDMP litigation. *See* Or. Prescription Drug Monitoring Program v. United States Drug Enf't Admin., 998 F. Supp. 2d 957, 966 (D. Or. 2014) (characterizing the DEA's argument), *rev'd*, 860 F.3d 1228 (9th Cir. 2017).

182. *Utah Dep't of Commerce*, 2017 WL 3189868, at *7.

183. *See Morton Salt Co.*, 338 U.S. at 651–52 (limiting its Fourth Amendment inquiry to the request for corporate records); *Okla. Press*, 327 U.S. at 210; ("The only records or documents sought were corporate ones."); *see also* Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 816 (2005) ("[A]ll of these [early twentieth-century-administrative subpoena] cases involved government attempts to obtain corporate or other business documents. Throughout the first half of the twentieth century, the Court had intimated that subpoenas for private records might have to meet a higher standard."); Katherine Scherb, Comment, *Administrative Subpoenas for Private Financial Records: What Protection for Privacy Does the Fourth Amendment Afford?*, 1996 WIS. L. REV. 1075, 1085 ("The Supreme Court decisions of the 1940s and 1950s which developed the current Fourth Amendment standard for administrative subpoenas addressed administrative subpoenas seeking corporate records.").

"government actors, subject to the strictures of the Fourth Amendment."[184]

1. *State PDMP Data Are Not Corporate Books or Records*. The PDMP records sought by the DEA in the Utah and Oregon cases are distinguishable from the corporate books and records subpoenaed in *Oklahoma Press* and *Morton Salt*. State PDMPs are populated with prescriber, dispenser, and patient health-care data, all of which are uploaded to the databases by dispensers subject to a state mandate and much of which is derived from confidential patient–physician communications. This is important because the Supreme Court has long distinguished between the Fourth Amendment rights that pertain to corporations and those that apply to private individuals.[185]

In *Oklahoma Press*, several newspaper-publishing corporations challenged the right of the U.S. Department of Labor to judicially enforce its investigatory subpoenas for corporate records.[186] The corporate petitioners contended that "enforcement would permit the [government] to conduct general fishing expeditions into [their] books, records, and papers" without probable cause.[187] The Court rejected the corporations' argument that the probable cause standard applies to administrative subpoenas and, in so doing, explained that corporations "are not entitled to all of the constitutional protections which private individuals have."[188] Instead, the Court held that, insofar as administrative subpoenas for corporate records are concerned, the Fourth Amendment "at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be 'particularly described,' if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are

184. Ferguson v. City of Charleston, 532 U.S. 67, 76 (2001); *see also* New Jersey v. T.L.O., 469 U.S. 325, 335 (1985) (explaining that "this Court has never limited the [Fourth] Amendment's prohibition on unreasonable searches and seizures to operations conducted by the police"; instead, "the Court has long spoken of the Fourth Amendment's strictures as restraints imposed upon 'governmental action'—that is, 'upon the activities of sovereign authority'" (quoting Burdeau v. McDowell, 256 U.S. 465, 475 (1921))).

185. Jack W. Campbell IV, Note, *Revoking the "Fishing License:" Recent Decisions Place Unwarranted Restrictions on Administrative Agencies' Power to Subpoena Personal Financial Records*, 49 VAND. L. REV. 395, 407 (1996) (reporting that "[c]ourts have asserted that subpoenas for personal, as opposed to corporate, . . . records implicate greater privacy concerns" and that "[t]his distinction underlies heightened suspicion requirements for enforcement of administrative subpoenas seeking personal . . . records").

186. *Okla. Press*, 327 U.S. at 189.

187. *Id.* at 195.

188. *Id.* at 205.

relevant."[189] In reaching that result, the Court emphasized that the challenged administrative subpoena sought *corporate*, as opposed to *private*, papers.[190]

Much the same can be said about the Court's ruling in *Morton Salt*. There, the respondents—several corporate salt producers and a trade union—challenged the Federal Trade Commission's ("FTC") power to require them to file reports indicating compliance with a federal court decree enforcing a cease and desist order.[191] The *Morton Salt* Court upheld the FTC's right to subpoena those compliance reports under the relaxed reasonable relevance standard[192]—and explained that corporations do not merit the same degree of Fourth Amendment protection as private persons:

> While they may and should have protection from unlawful demands made in the name of public investigation, corporations can claim no equality with individuals in the enjoyment of a right to privacy. They are endowed with public attributes. They have a collective impact upon society, from which they derive the privilege of acting as artificial entities.[193]

In other words, "the clear import of *Oklahoma Press* and *Morton Salt* is that the standard for judicial enforcement of administrative subpoenas of a private citizen's private papers is stricter than that for corporate papers."[194]

Skeptics might complain that since *Oklahoma Press* and *Morton Salt* were decided the federal courts have abandoned any meaningful distinction between corporate and private papers insofar as

189. *Id.* at 208.

190. *Id.* at 204–05 ("[I]t has been settled that corporations are not entitled to all of the constitutional protections which private individuals have in these and related matters.").

191. United States v. Morton Salt Co., 338 U.S. 632, 634–35 (1950).

192. *See id.* at 652–53 (noting that an administrative investigation is "sufficient" if it is "within the authority of the agency, . . . not too indefinite[,] . . . reasonably relevant," and not unreasonable (citing *Okla. Press*, 327 U.S. at 208)).

193. *Id.* at 652 (citations omitted).

194. Parks v. FDIC, 65 F.3d 207, 211 (1st Cir. 1995), *reh'g en banc granted*, *opinion withdrawn* (Nov. 20, 1995); *see also* FDIC v. Wentz, 55 F.3d 905, 908 (3d Cir. 1995) ("When personal documents of individuals, as contrasted with business records of corporations, are the subject of an administrative subpoena, privacy concerns must be considered."); *In re* McVane, 44 F.3d 1127, 1137 (2d Cir. 1995) (noting than an administrative subpoena directed at individuals implicates privacy rights); Resolution Tr. Corp. v. Walde, 18 F.3d 943, 948 (D.C. Cir. 1994) (distinguishing between administrative subpoenas that seek corporate records and those that seek personal papers).

administrative subpoenas are concerned.[195] They have a point. As one legal scholar has explained, "the minimal relevance standard once used primarily in connection with business subpoenas now authorizes access to vast amounts of personal information, to wit, *any* personal information that is in record form" and "that regime seems to conflict with the Fourth Amendment's injunction that searches and seizures of papers, as well as of houses, persons, and effects, are unreasonable unless authorized by a warrant based on probable cause."[196]

Yet, save for one fairly obscure and easily distinguishable 1964 case, *Ryan v. United States*,[197] the Supreme Court has never held that the reasonable relevance standard applies to administratively subpoenaed private papers where the target of the investigation has a personal privacy interest in those documents.[198] Moreover, the Court made it clear ten years after *Ryan* that the Fourth Amendment prohibits even a grand jury subpoena from requiring a target to produce "private books and records that would incriminate him."[199] As a result, to the extent that highly sensitive and revealing patient PDMP prescribing data are fairly characterized as private health-care records—that is, records in which the individual target has a personal privacy interest—PDMP records are arguably distinct from corporate records for constitutional purposes and are entitled to heightened Fourth Amendment protection.

2. *PDMP Data Are Maintained by State Actors*. The PDMP cases are further distinguishable from *Oklahoma Press* and *Morton Salt* because PDMP data are collected by state actors subject to the Fourth Amendment and not by corporate entities. One of the primary

195. *See* Slobogin, *supra* note 183, at 817–20 (describing the erosion of "the sixty-year-old distinction between corporate and personal records in connection with the subpoena process").

196. *Id*. at 826.

197. Ryan v. United States, 379 U.S. 61 (1964). In *Ryan*, the Supreme Court issued a terse order holding that the IRS could subpoena the books of a private taxpayer under suspicion of tax fraud to ascertain his actual income without a showing of probable cause. *Id.* at 62. The Court provided no rationale for its decision except "we sustain the judgment of the Court of Appeals for the reasons given in *United States v. Powell*." *Id.* (citation omitted). *Powell*, however, was a case that exclusively involved an IRS subpoena for *corporate tax records*. *United States v. Powell*, 379 U.S. 48, 49 (1964). One could also argue that *Ryan* is unique insofar as the target was under a pre-subpoena legal obligation to provide the contents of the documents sought—his annual-earnings information—to the very agency seeking those documents—the IRS.

198. *See* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) ("[T]his Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy.").

199. United States v. Dionisio, 410 U.S. 1, 11 (1973).

rationales for the application of a lenient standard of suspicion to administrative subpoenas is that such subpoenas do not involve actual searches and, therefore, merit no Fourth Amendment protection at all. For example, in *Oklahoma Press*, the Court contended that administrative subpoenas do not amount to "actual searches" because "[n]o officer or other person has sought to enter petitioners' premises against their will, to search them, or to seize or examine their books, records or papers without their assent";[200] rather, at best, they constitute "constructive" searches *conducted by the target of the investigation themselves and not the government*.[201]

The DEA administrative subpoenas at issue in the PDMP cases, however, do not fit comfortably into this "constructive" search framework.[202] In the PDMP context, one government actor—the state legislature—legally compels drug dispensers to submit patient prescribing data to a state agency database while expressly limiting law enforcement agency access to that database via a warrant requirement. A second government actor—the DEA—then demands that sensitive health-care information from the state PDMP without any individualized suspicion, warrant, or other judicial order in violation of the express limitations placed on its access to that information by the state legislature. It is, therefore, problematic to characterize DEA administrative subpoenas directed at state PDMPs as "constructive searches" *conducted by the target of the investigation themselves and not the government*. Rather, the DEA subpoenas demand that a state agency, which itself is a government actor bound by the Fourth Amendment, conduct an actual search for private health records sought by law enforcement and often without notice to the target of the investigation.[203]

---

200. Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 195 (1946).

201. *Id.* at 202; Slobogin, *supra* note 183, at 827.

202. Slobogin, *supra* note 183, at 827 (explaining that "several Supreme Court justices have suggested that document subpoenas are not Fourth Amendment searches [because]: (1) They rely on the recordholder, not the government, to produce the documents; (2) the target can challenge them before surrendering any items; and (3) they do not involve physical trespass or intrusion").

203. *See, e.g.*, U.S. Dep't of Justice v. Utah Dep't of Commerce, No. 2:16-cv-611, 2017 WL 3189868, at *7 (D. Utah July 27, 2017); *see also* Slobogin, *supra* note 183, at 827 (noting that one of the rationales supporting the lenient reasonable relevance standard that applies to administrative subpoenas is the target's ability to "challenge them before surrendering any items" and characterizing this rationale as specious given that "[t]he fact that it is the target (or a third party) rather than the police who locates the documents obviously does not change the nature of the revelations they contain, which can include information about medical treatment, finances, education, the identity of one's communicants, and even the contents of one's communications"); *id.* (explaining further that "[t]he target's ability to challenge a subpoena, while it may inhibit

Fourth Amendment case law draws a meaningful line between law enforcement's demand that an investigatory target or a corporate third party conduct a search and law enforcement's demand that *another government agency* do the same. For instance, in *Ferguson v. City of Charleston*,[204] the policy at issue involved a collaboration between a "public hospital operated in the city of Charleston by the Medical University of South Carolina ("MUSC") . . . concerned about an apparent increase in the use of cocaine by patients who were receiving prenatal treatment"[205] and the City of Charleston Police Department ("CPD"), prosecutors, and other law enforcement officials.[206] Pursuant to that collaboration, the state hospital, MUSC, identified pregnant patients suspected of drug abuse and then surreptitiously tested those patients for cocaine use through a urine drug screen if they met certain criteria.[207] When a patient tested positive for cocaine via the screen, MUSC then referred her either to substance-abuse treatment or to the police for arrest and prosecution for illicit drug use—or both.[208]

The Supreme Court described the question presented in *Ferguson* broadly as "whether a state hospital's performance of a diagnostic test to obtain evidence of a patient's criminal conduct for law enforcement purposes is an unreasonable search if the patient has not consented to the procedure"; and, "more narrowly," as "whether the interest in using the threat of criminal sanctions to deter pregnant women from using cocaine can justify a departure from the general rule that an official nonconsensual search is unconstitutional if not authorized by a valid warrant."[209] The Court ruled that "MUSC is a state hospital, [and] the members of its staff are government actors, subject to the strictures of the Fourth Amendment" and, as such, "the urine tests conducted by those staff members were indisputably searches within the meaning of the Fourth Amendment."[210] It was, therefore, highly relevant in *Ferguson* that the initial search was conducted by a state actor bound

---

some fishing expeditions, at most will only delay government access to the records, unless something beyond the current relevance standard is applicable").

204. Ferguson v. City of Charleston, 532 U.S. 67 (2001).

205. *Id.* at 70.

206. *See id.* at 70–73 (describing the policy at issue).

207. *Id.* at 71.

208. *Id.* at 72.

209. *Id.* at 69–70.

210. *Id.* at 76. The Court recognized that "[n]either the District Court nor the Court of Appeals concluded that any of the nine criteria used to identify the women to be searched provided either probable cause to believe that they were using cocaine, or even the basis for a reasonable suspicion of such use." *Id.*

by the Fourth Amendment and not an individual target or a corporation.

Moreover, in holding that the MUSC–CPD policy violated the petitioners' Fourth Amendment rights, the Court was careful to distinguish the policy from its previous "special needs" cases, in which the Court had held that suspicionless drug tests conducted by certain state actors—public employers and school officials—were permissible.[211] In doing so, the Court emphasized three points. First, the "special needs" or "administrative search" exception to the warrant requirement is expressly confined to a "search policy designed to serve non-law-enforcement ends"[212] whereas the "central and indispensable feature of the [MUSC–CPD] policy from its inception was the use of law enforcement to coerce the patients into substance abuse treatment."[213] Second, "[i]n the previous four [special-needs] cases, there was no misunderstanding about the purpose of the test or the potential use of the test results, and there were protections against the dissemination of the results to third parties" generally, and law enforcement specifically.[214] Finally, "[t]he reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent"[215] and "an intrusion on that expectation [of privacy] may have adverse consequences because it may deter patients from receiving needed medical care."[216]

The obvious parallels between *Ferguson* and the PDMP cases make it easy to understand why the DEA failed to invoke the special-needs doctrine in support of its warrantless searches in the Utah and Oregon litigation. There, both cases involved a state actor's disclosure of patient prescribing data to law enforcement without patient consent. Recognizing this important distinction, the DEA attempted to distinguish *Ferguson* on the sole basis that, in that case, law enforcement relied on a collaborative policy and not on the service of administrative subpoenas to collect private health information from

211. *Id.* at 77–80.
212. *Id.* at 74.
213. *Id.* at 80.
214. *Id.* at 78.
215. *Id.*
216. *Id.* at 78 n.14.

another state actor.[217] The Oregon district court, which relied on *Ferguson* in ruling in favor of the intervenors,[218] refused to even address that argument.[219] The Utah district court, on the other hand, did distinguish *Ferguson* at least in part on that basis, explaining that "[a]lthough *Ferguson* involved information passed from one government entity to another, it did not involve an administrative subpoena."[220]

The Utah district court's disposal of *Ferguson* on such grounds is specious for several reasons. First, the pertinent legal distinction between law enforcement's extraction of private prescribing information from another government agency under the special-needs exception and the same conduct pursuant to an administrative subpoena is that a special-needs target is actually better off than a subpoena target. As *Ferguson* and the PDMP cases illustrate, investigatory targets can challenge either of those warrantless searches in federal district court. The Fourth Amendment protections provided to targets of warrantless searches under the special-needs doctrine's balancing test, however, well exceed the minimal relevance standard that applies to targets of warrantless administrative subpoenas.[221]

Second, the PDMP patients and prescribers arguably have a higher—and even more reasonable—expectation of privacy in their prescribing data than did the patients in *Ferguson*. This is because the *Ferguson* patients were not provided any guarantees by the hospital—or any other state actor—that the results of their drug tests would not be shared with law enforcement. Instead, the *Ferguson* patients' privacy interests emanated from an assumption: that any patient reasonably expects that hospitals will not share their diagnostic testing results with nonmedical personnel without their consent.[222] The Utah

217. Reply in Support of Petition to Enforce DEA Administrative Subpoenas at 25 n.13, U.S. Dep't of Justice v. Utah Dep't of Commerce, No. 2:16-cv-611, 2017 WL 3189868 (D. Utah Nov. 23, 2016).

218. *See* Or. Prescription Drug Monitoring Program v. U.S. Drug Enf't Admin., 998 F. Supp. 2d 957, 965–66 (D. Or. 2014) (referencing *Ferguson* in its discussion determining that the intervenors' expectation of privacy was reasonable), *rev'd*, 860 F.3d 1228 (9th Cir. 2017).

219. *Id.*

220. *Utah Dep't of Commerce*, 2017 WL 3189868, at *6.

221. *See, e.g.*, Ferguson, 532 U.S. at 78 (espousing that, in the special-needs cases, the Court "employed a balancing test that weighed the intrusion on the individual's interest in privacy against the 'special needs' that supported the program" and not the reasonable relevance test).

222. *See id.* ("The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent.").

patients' reasonable expectation that their PDMP health data would not be subject to a warrantless search by law enforcement, on the other hand, is based on the fact that the Utah legislature expressly enacted a statute that requires law enforcement to obtain a warrant to access PDMP data.[223]

*B. Pre-*Carpenter *Third-Party Doctrine*

The DEA also argued in the Oregon and Utah cases that it was entitled to PDMP prescribing data without a warrant under the third-party doctrine.[224] The third-party doctrine is implicated whenever an individual voluntarily shares information with a third party that later submits that information to the government. As the Supreme Court has held, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," and, thus, no cause to seek shelter in the Fourth Amendment to protect any information held by a third party from government search or seizure.[225] This is because a person who voluntarily turns over information to third parties "assume[s] the risk" that the third party will disclose that information to the government.[226] As Professor Monu Bedi recently explained,

> [t]he early cases applying the third party doctrine centered on face-to-face conversations with government informants. Under these decisions, as long as agents did not trespass on a person's property, individuals did not have Fourth Amendment protection in what they disclosed to an undercover informant, irrespective of the individual's belief that the informant would not disclose the information to the government. . . . As the Court articulated, "a wrongdoer's misplaced belief that a person to whom he voluntary confides his wrongdoing will not reveal it" receives no protection under the Fourth Amendment.[227]

The Supreme Court expanded the third-party doctrine to encompass documents over the course of three 1970s-era decisions:

---

223. UTAH CODE ANN. § 58-37f-301 (2018).

224. Or. Prescription Drug Monitoring Program, 998 F. Supp. 2d at 967; DEA Administrative Subpoenas at 18–22, U.S. Dep't of Justice v. Utah Dep't of Commerce, No. 2:16-cv-611-DN-DBP (D. Utah Nov. 23, 2016).

225. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

226. *Id.* at 744.

227. Monu Bedi, *The Fourth Amendment Disclosure Doctrines*, 26 WM. & MARY BILL RTS. J. 461, 463 (2017) (footnotes omitted) (quoting Hoffa v. United States, 385 U.S. 293, 302 (1966)).

Couch v. United States,[228] *United States v. Miller*,[229] and *Smith v. Maryland*.[230] Any discussion of the third-party doctrine—and its applicability to PDMP prescribing data—must begin with *Miller* and *Smith*.[231] Moreover, and as explained below, while the Court's decisions in *United States v. Jones*[232] and *Riley v. California*[233] are instructive, they did not alter the *Miller–Smith* regime.

1. United States v. Miller. In *Miller*, the U.S. Department of the Treasury presented grand jury subpoenas to two banks requesting Miller's account records.[234] The banks complied with those subpoenas and produced Miller's checks, deposit slips, financial statements, and monthly statements to the government.[235] The district court denied Miller's motion to suppress those records, but the court of appeals reversed, holding "that the [g]overnment had improperly circumvented . . . [Miller's] Fourth Amendment right against unreasonable searches and seizures" by obtaining his bank records without a warrant.[236] The government appealed that decision, arguing that Miller had no Fourth Amendment interest in the records. The Supreme Court agreed pursuant to the third-party doctrine.[237]

Miller is often quoted[238] for its statement that the Fourth Amendment's warrant clause "does not prohibit the obtaining of information revealed to a third party and conveyed by him to

228. Couch v. United States, 409 U.S. 322 (1973).

229. United States v. Miller, 425 U.S. 435 (1976).

230. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

231. *Couch* held that a defendant taxpayer could not invoke either the Fourth or Fifth Amendments to protect tax documents that he had knowingly and voluntarily provided to his accountant and that his accountant provided to the government. *Couch*, 409 U.S. at 335–36. Because it is well settled that taxpayers have no reasonable expectation of privacy in their tax-related documents and there was no dispute that Couch knowingly and voluntarily provided his tax documents to his accountant, *id.*, *Couch* is inapposite to the PDMP-data cases and warrants no additional discussion.

232. United States v. Jones, 565 U.S. 400 (2012).

233. Riley v. California, 573 U.S. 373 (2014).

234. *Miller*, 425 U.S. at 437.

235. *Id.* at 438.

236. *Id.* at 438–39.

237. *Id.* at 439, 444.

238. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 117 (1984); Smith v. Maryland, 442 U.S. 735, 744 (1979); United States v. Morel, 922 F.3d 1, 8–9 (1st Cir. 2019); Palmieri v. United States, 896 F.3d 579, 588 (D.C. Cir. 2018); Presley v. United States, 895 F.3d 1284, 1291 (11th Cir. 2018); United States v. Riley, 858 F.3d 1012, 1019 (6th Cir. 2017); United States v. Caira, 833 F.3d 803, 806 (7th Cir. 2016); United States v. Wheelock, 772 F.3d 825, 828 (8th Cir. 2014); Kerns v. Bader, 663 F.3d 1173, 1184 (10th Cir. 2011).

[g]overnment authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[239] The breadth and scope of that contention is sweeping. It is important to point out, however, that *Miller* acknowledged the Court's obligation to "*examine the nature of the particular documents sought to be protected* in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents" in deciding the Fourth Amendment claim presented—and it did just that.[240] Specifically, the Court held that Miller had no legitimate expectation of privacy in his checks and deposit slips because "checks are not confidential communications but negotiable instruments to be used in commercial transactions."[241] The Court also emphasized the voluntariness of Miller's banking transactions, pointing out that "all of the documents obtained . . . *contain only information voluntarily conveyed to the banks*."[242]

2. Smith v. Maryland. Three years after *Miller*, the Court decided *Smith*.[243] That case involved a telephone company's installation of a pen register at its central offices at the police's request in order to record the numbers Smith dialed from his home phone.[244] The Court applied the *Katz* test to Smith's Fourth Amendment challenge and held that it failed both prongs.[245] First, the Court ruled that "people in general [do not] entertain any actual expectation of privacy in the numbers they dial" from their home phones.[246] Second, it concluded that "even if [Smith] did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not one that society is prepared to recognize as reasonable"[247] because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[248]

---

239. *Miller*, 425 U.S. at 443.

240. *Id.* at 442 (emphasis added).

241. *Id.*

242. *Id.* (emphasis added).

243. *Smith*, 442 U.S. at 735.

244. *Id.* at 737.

245. *See id.* at 739–46 (conducting its Fourth Amendment analysis based on *Katz v. United States*, 389 U.S. 347 (1967)).

246. *Id.* at 742.

247. *Id.* at 743 (quoting *Katz*, 389 U.S. at 361).

248. *Id.* at 743–44 (citing United States v. Miller, 425 U.S. 435, 442–44 (1976)).

The Court reasoned that when Smith used his home phone, he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[249] As a result, he "assumed the risk that the company would reveal to police the numbers he dialed"[250] and abandoned any Fourth Amendment protection in the numbers he voluntarily conveyed to the phone company.

3. *The Fourth Amendment Supervillain*, Jones, *and* Riley. "The third-party doctrine has been subject to tsunamis of criticism"[251] as a result of its alleged failure to put any "constitutional limits on dragnet data collection."[252] Professor Orin Kerr proffered that "[t]he third-party doctrine is the Fourth Amendment rule scholars love to hate. It is the *Lochner* of search and seizure law, widely criticized as profoundly misguided."[253] Professor Jane Bambauer opined that "[t]he third-party doctrine has become the Fourth Amendment's supervillain"[254] and Professor Daniel Solove characterized the doctrine as "one of the most serious threats to privacy in the digital age."[255] In sum, "[t]here are few areas of constitutional law that raise scholars' ire and trouble jurists like the Fourth Amendment's third-party doctrine."[256]

The Supreme Court is well aware of these critiques. In fact, in *United States v. Jones*,[257] five Justices openly discussed the third-party

249. *Id.* at 744.

250. *Id.*

251. United States v. Chavez, No. 3:14-cr-00185, 2016 WL 740246, at *2 (D. Conn. Feb. 24, 2016); *see also* Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 214–15 (2006) (arguing that Fourth Amendment protections cannot vanish due to advances in technology that allow the government to obtain information from third parties without a warrant); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 976–77 (2007) (noting criticism of the third-party doctrine).

252. Jane Bambauer, *Other People's Papers*, 94 TEX. L. REV. 205, 261 (2015).

253. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

254. Bambauer, *supra* note 252, at 261.

255. Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 753 (2005).

256. Peter C. Ormerod & Lawrence J. Trautman, *A Descriptive Analysis of the Fourth Amendment and the Third-Party Doctrine in the Digital Age*, 28 ALB. L.J. SCI. & TECH. 73, 73 (2018).

257. United States v. Jones, 565 U.S. 400 (2012). The third-party doctrine was inapposite to the Court's holding in *Jones*, which was that the police's "attachment of a Global-Positioning-System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to

doctrine's inability to resolve modern-day surveillance and data-aggregation cases given the frequency with which personal data is transmitted electronically, stored by third-party intermediaries, and, therefore, not obtained by a physical invasion or trespass.[258] In her *Jones* concurrence, Justice Sotomayor urged "reconsider[ation of] the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[259] She added that the doctrine "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks," including the disclosure of "*medications they purchase to online retailers*."[260] Justice Sotomayor also cautioned that "by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the government, in its unfettered discretion, chooses to track," digital surveillance techniques, like GPS monitoring, "may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[261]

The Supreme Court further evidenced its interest in limiting the extension of certain analog-era Fourth Amendment doctrines to electronically stored information in *Riley v. California*.[262] *Riley* involved a police search of a suspect's cell phone incident to his arrest.[263] As the Court colorfully explained, *Riley* "require[d it] to decide how the search incident to arrest doctrine applies to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[264]

The *Riley* Court unanimously held that police are required to secure a warrant in order to conduct a search of an individual's cell phone incident to arrest.[265] In reaching that result, Chief Justice Roberts observed that, while the "categorical" search incident to arrest

---

monitor the vehicle's movements on public streets" constituted a Fourth Amendment search. *Id.* at 402.

258. *Id.* at 417–18 (Sotomayor, J., concurring); *id.* at 418 (Alito, J., concurring in the judgment).

259. *Id.* at 417 (Sotomayor, J., concurring) (citations omitted).

260. *Id.* (emphasis added).

261. *Id.* at 416 (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

262. Riley v. California, 573 U.S. 373 (2014).

263. *Id.* at 378–80.

264. *Id.* at 385.

265. *Id.* at 403.

rule established in *United States v. Robinson*[266] "strikes the appropriate balance [between an individual's privacy and the promotion of legitimate government interests] in the context of physical objects, neither of its rationales [*e.g.*, harm to officers and destruction of evidence] has much force with respect to digital content on cell phones."[267] He further declared that "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person," largely due to their capacity to store vast quantities of personal information[268] and "pervasiveness."[269]

The *Riley* Court found the government's argument that cell-phone-data searches are materially indistinguishable from searches of physical items patently absurd, responding: "[t]hat is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together."[270] The importance of *Riley* is that it represents the Court's willingness to depart from the mechanical application of analog-era Fourth Amendment doctrines to the search of mass storage, digital devices which, as the Court recognized, "hold for many Americans 'the privacies of life.'"[271]

This Fourth Amendment digital doctrinal renaissance had little material impact on the third-party doctrine prior to *Carpenter*.[272] *Miller* and *Smith*, therefore, remained binding precedent. As a result, law enforcement agencies, including the DEA, relied heavily on their holdings to conduct sweeping, warrantless investigations of personal data held by third parties, including suspicionless searches of sensitive health information contained in state PDMP electronic databases.[273]

266. United States v. Robinson, 414 U.S. 218 (1973).

267. *Riley*, 573 U.S. at 386.

268. *Id.* at 393.

269. *Id.* at 395.

270. *Id.* at 393.

271. *Id.* at 403 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

272. *See, e.g.*, California v. Greenwood, 486 U.S. 35, 38–39 (1988) (upholding a warrantless search of defendants' trash).

273. U.S. Dep't of Justice v. Utah Dep't of Commerce, No. 2:16-cv-611, 2017 WL 3189868, at *5 (D. Utah July 27, 2017); Or. Prescription Drug Monitoring Program v. U.S. Drug Enf't Admin., 998 F. Supp. 2d 957, 967 (D. Or. 2014), *rev'd*, 860 F.3d 1228 (9th Cir. 2017).

*C. Application of Pre-*Carpenter *Third-Party-Doctrine Precedent to the PDMP Cases*

Nonetheless, even pre-*Carpenter* precedents such as *Miller* and *Smith* do not sanction a DEA warrantless search of PDMP prescribing data. A close reading of those cases indicates that the third-party doctrine is subject to two important limiting principles. First, neither case asserts a categorical rule excluding all information transmitted to a third party from Fourth Amendment protection. Instead, *Miller* and *Smith* require courts *to evaluate the nature of the documents held by a third party* to ascertain whether an individual target has a reasonable expectation of privacy in the information sought by law enforcement. Second, the third-party doctrine's application is limited to information *voluntarily* or *consensually* disclosed to another. Consequently, where dispensers are legally *compelled* to disclose prescribing data to a government agency—as was the case in the Oregon and Utah PDMP litigation—extension of the third-party doctrine to that information is unwarranted.

1. *Oregon PDMP Litigation*. The district court's rejection of the DEA's request to enforce its subpoenas in the Oregon PDMP litigation was predicated on the third-party doctrine's limitations. The court recognized that the case before it was "markedly different from *Miller* and *Smith* for two reasons."[274] First, the PDMP records at issue were "more inherently personal or private than [the] bank records" at issue in *Miller*.[275] Second, "patients and doctors are not voluntarily conveying information to the PDMP."[276] Instead "[t]he submission of prescription information to the PDMP is required by law. The only way to avoid submission of prescription information to the PDMP is to forgo medical treatment or to leave the state, [sic] This is not a meaningful choice."[277]

Forgoing necessary medical treatment under any circumstances is detrimental. But choosing to do so in order to avoid warrantless law enforcement searches seems particularly problematic—legally and practically. The Supreme Court has recognized as much and said that "an intrusion on [a patient's reasonable] expectation [of privacy in

274. *Or. Prescription Drug Monitoring Program*, 998 F. Supp. 2d at 967.

275. *Id.* (quoting United States v. Golden Valley Elec. Ass'n, 689 F.3d 1108, 1116 (9th Cir. 2012)).

276. *Id.*

277. *Id.*

their health-care data] may have adverse [public health] consequences because it may deter patients from receiving needed medical care."[278]

2. *Utah PDMP Litigation*. Unlike the Oregon district court, the Utah court enforced the DEA administrative subpoena based on a categorical reading of the third-party doctrine. It conceded that "[m]edical records, including prescriptions, are no doubt personal and private matters."[279] It went on to conclude, however, that "[t]he expectation of privacy analysis nonetheless weighs in the DEA's favor"[280] for at least two reasons. First, the court invoked the third-party doctrine without meaningfully acknowledging that dispensers are legally compelled to transmit prescribing data to PDMPs.[281] It found that, when patients convey confidential information to their doctors for the purpose of medical treatment or diagnosis, they assume the risk that their doctors will turn that information over to the PDMP, as doctors are required to do by statute.[282] Patients, then, presumably also assume the risk that the state PDMP will turn over their sensitive prescribing data to law enforcement without a warrant in violation of state law.[283] Specifically, the court explained that "[a] patient in Utah decides to trust a prescribing physician with health information to facilitate a diagnosis" and, "[i]n so doing, a patient takes the risk . . . that his or her information will be conveyed to the government as required by the [PDMP statute]."[284]

This reasoning misses the point. It seems incredible to argue that Utah patients assumed any risk that their protected, private health information, which was required to be turned over to the state PDMP by their dispenser, would then be turned over to law enforcement by the PDMP pursuant to an administrative subpoena. The more plausible contention is that Utah patients reasonably assumed, in reliance on state law, that the PDMP would make no such conveyance to law enforcement without a warrant supported by probable cause.

Fortunately, the Supreme Court recently provided additional guidance regarding the application of the third-party doctrine to

278. Ferguson v. City of Charleston, 532 U.S. 67, 78–79 n.14 (2001).

279. U.S. Dep't of Justice v. Utah Dep't of Commerce, No. 2:16-cv-611, 2017 WL 3189868, at *8 (D. Utah July 27, 2017).

280. *Id.*

281. *See id.*

282. *Id.*

283. *See id.*

284. *Id.*

personal information obtained by law enforcement from a third-party electronic database without a warrant. We turn now to that decision.

IV. *CARPENTER V. UNITED STATES*

On June 22, 2018, the U.S. Supreme Court issued its highly anticipated decision in *Carpenter v. United States*, which held that law enforcement agencies must obtain a warrant to access an investigatory target's cell-site-location information ("CSLI") from a third-party cellular phone company.[285] Chief Justice Roberts authored the majority opinion, joined by Justices Ginsburg, Breyer, Sotomayor, and Kagan. The remaining four members of the court—Justices Kennedy, Thomas, Alito, and Gorsuch—each filed separate, dissenting opinions. The pertinent factual, technical, and substantive aspects of the case are discussed below.

A. Factual and Procedural Background

In April 2011, police officers arrested four suspects for a string of armed robberies of Radio Shack and T-Mobile stores in Michigan and Ohio.[286] One of the arrestees confessed to police that the group was responsible for the robberies and that as many as fifteen additional accomplices had participated in the crimes as getaway drivers and lookouts.[287] The informant supplied the FBI with his personal cell phone number and the cell phone numbers of several other suspects.[288] The FBI used the confessant's call logs to identify additional phone numbers that he had dialed around the time of the robberies.[289] One of these numbers belonged to Timothy Carpenter. Upon receipt of Carpenter's cell phone number, the FBI submitted applications for Stored Communications Act § 2703(d) orders directed at Carpenter's wireless carriers—MetroPCS and Sprint.[290] Those orders sought Carpenter's historic CSLI over a 152-day period during which the string of robberies occurred.[291]

CSLI records enable law enforcement to reconstruct in detail where an individual has traveled throughout the time period covered

285. Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).
286. *Id.* at 2212.
287. *Id.*
288. *Id.*
289. *Id.*
290. *Id.*
291. *Id.*

by the data. This is because "[c]ell phones perform their wide and growing variety of functions by connecting to a set of radio antennas called 'cell sites.'"[292] "Each time the phone connects to a cell site, it generates a time-stamped record known as [CSLI]," which "[w]ireless carriers collect and store . . . for their own business purposes."[293]

> The precision of [CSLI] information depends on the size of the geographic area covered by the cell site. The greater the concentration of cell sites, the smaller the coverage area. As data usage from cell phones has increased, wireless carriers have installed more cell sites to handle the traffic. That has led to increasingly compact coverage areas, especially in urban areas.[294]

The Stored Communications Act ("SCA") creates privacy protections for CSLI and the content of stored wire and electronic communications.[295] Under § 2703(d) of the SCA, law enforcement can compel the production of CSLI when "specific and articulable facts show[] that there are reasonable grounds to believe that . . . the records . . . sought, are relevant and material to an ongoing criminal investigation."[296] The "relevant and material" standard of suspicion that applies to § 2703(d) orders is similar to but more demanding than the "relevant or material" test that applies to CSA § 876 administrative subpoenas.[297] Both standards, of course, are far more lenient than the Fourth Amendment probable cause requirement.

Unlike the CSA, however, the SCA requires law enforcement to obtain a court order before searching *the content* of a target's electronic communications and related information.[298] In addition—and, again, unlike the CSA—the SCA requires the government to obtain a warrant before it can access *the content* of a customer's or subscriber's electronic communications, unless the government provides the customer or subscriber prior notice.[299] However, the SCA does not require such prior notice to obtain a customer's or subscriber's CSLI.[300]

---

292. *Id.* at 2211.

293. *Id.* at 2211–12.

294. *Id.*

295. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860–68 (codified as amended at 18 U.S.C. §§ 2701–2711 (2018)).

296. 18 U.S.C. § 2703(d).

297. 21 U.S.C. § 876(a) (2018).

298. *Compare* 18 U.S.C. § 2703(d), *with* 21 U.S.C. § 876(a).

299. 18 U.S.C. § 2703(b)(A).

300. *Id.* § 2703(c)(3).

Two federal magistrate judges determined that the FBI had met the relevant and material standard of suspicion required by § 2703(d) to obtain Timothy Carpenter's historic CSLI records and issued orders requiring Carpenter's wireless carriers to submit that data spanning the 152-day period requested by the FBI.[301] MetroPCS and Sprint complied with those orders and collectively provided the FBI with CSLI spanning more than four months, which included "12,898 location points cataloging Carpenter's movements—an average of 101 data points per day."[302] According to the government, Carpenter's CSLI data placed his phone near several of the robberies.[303] Consequently, the FBI charged Carpenter with six counts of robbery and six counts of carrying a firearm during a federal crime of violence.[304]

Carpenter's motion to suppress his CSLI data was denied by the district court.[305] He subsequently went to trial, was convicted by a jury on all but one of the charged counts, and was sentenced to over one hundred years in federal prison.[306] Carpenter appealed the district court's denial of his motion to suppress to the U.S. Court of Appeals for the Sixth Circuit.[307]

The Sixth Circuit affirmed the district court's refusal to suppress Carpenter's CSLI data, ruling "that the government's collection of business records containing cell-site data was not a [Fourth Amendment] search" under the third-party doctrine.[308] It did, however, explain the type of information that is protected by the Fourth Amendment warrant requirement notwithstanding third-party disclosure. Relying on *Smith*,[309] the Sixth Circuit explained that "the federal courts have long recognized a core distinction [regarding personal communications]: although the *content of personal communications* is private, the information necessary to get those communications from point A to point B is not."[310] The court then

301. Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

302. *Id.*

303. *Id.* at 2212–13.

304. *Id.* at 2212.

305. *Id.*

306. *Id.* at 2212–13.

307. United States v. Carpenter, 819 F.3d 880, 885 (6th Cir. 2016), *rev'd*, 138 S. Ct. 2206 (2018).

308. *Id.* at 890.

309. *Id.* at 889 ("[T]he question presented here . . . is answered by [Smith v. Maryland, 442 U.S. 735 (1979)].").

310. *Id.* at 886 (emphasis added).

applied that distinction to Carpenter's CSLI records and found that they "fall on the unprotected side of the line" because "the cell-site data—like mailing addresses, phone numbers, and IP addresses—are information that facilitate personal communications, rather than part of the content of those communications themselves."[311] The Supreme Court granted Carpenter's petition for certiorari.

B. Majority Opinion

Chief Justice Roberts wrote the majority opinion in *Carpenter*, which held that "the [g]overnment conducts a search under the Fourth Amendment when it accesses [seven days of] historical cell phone records that provide a comprehensive chronicle of the user's past movements."[312] He began with a brief exposition of Fourth Amendment fundamentals, pointing out that the Amendment's "basic purpose . . . is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[313] Borrowing substantially from the Court's opinion in *Riley*, he explained that the Framers drafted the Amendment "as a 'response to the reviled "general warrants" and "writs of assistance" of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.'"[314]

Chief Justice Roberts next invoked *Katz*, explaining that "the Fourth Amendment protects people, not places."[315] He went on to note that "[w]hen an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' . . . official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause."[316] The Chief Justice also emphasized that one of the "basic guideposts"[317] of the Fourth Amendment is "to place obstacles in the way of a too permeating police surveillance."[318] Pointing to *Kyllo v. United States*[319] and *Riley* as examples, he further reflected on the

311. *Id.* at 887.

312. Carpenter v. United States, 138 S. Ct. 2211, 2211, 2217 n.3 (2018).

313. *Id.* at 2213 (quoting Camara v. Mun. Court of S.F., 387 U.S. 523, 528 (1967)).

314. *Id.* (quoting Riley v. California, 573 U.S. 373, 403 (2014)).

315. *Id.* (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

316. *Id.* (quoting Smith v. Maryland, 442 U.S. 735, 740 (1979)).

317. *Id.* at 2214.

318. *Id.* (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

319. Kyllo v. United States, 533 U.S. 27 (2001). At issue in *Kyllo* was law enforcement's use of a thermal-imaging device to scan the defendant's home without a warrant "to determine

Court's evolving application of a less mechanical and more nuanced application of pre-digital Fourth Amendment doctrines in the face of technological innovation and the government's enhanced surveillance capabilities.[320]

Chief Justice Roberts then explained that the "personal location information maintained by a third party . . . lie[s] at the intersection of two lines of [Fourth Amendment] cases."[321] The first set of those cases, *United States v. Knotts*[322] and *Jones*, establish the boundaries of an individual's privacy interest in his physical location and movements.[323] The Chief Justice distinguished *Knotts*, which held that police were not required to obtain a warrant to track a beeper they had placed in a suspect's car, from *Jones*, which held that the police's warrantless placement of a GPS tracking device on a suspect's car and subsequent twenty-eight-day surveillance of that vehicle's movements ran afoul of the Fourth Amendment.[324] In the majority's view, the important differences between *Knotts* and *Jones* revolve around the varying levels of sophistication and pervasiveness of the law enforcement surveillance systems at issue in each case. While *Knotts* involved "rudimentary tracking facilitated by the beeper . . . during a discrete 'automotive journey,'"[325] *Jones* encompassed "sophisticated surveillance," which tracked the target's "every movement" over an approximately four-week-long time period.[326]

The Court then shifted to the second line of cases implicated by the FBI's warrantless collection of Carpenter's CSLI: *Miller*, *Smith*, and the third-party doctrine.[327] As the Court saw it, "[t]here is a world of difference between the limited types of personal information

whether an amount of heat was emanating from petitioner's home . . . consistent with the use of [high-intensity] lamps" typically used for indoor marijuana growth. *Id.* at 29. After acknowledging that "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology," the Court analyzed the issue presented under the two-part *Katz* test. *Id.* at 33–35. The Court subsequently concluded that "[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." *Id.* at 40.

320. *Carpenter*, 138 S. Ct. at 2214.

321. *Id.*

322. United States v. Knotts, 460 U.S. 276 (1983).

323. *Carpenter*, 138 S. Ct. at 2215.

324. *Id.*

325. *Id.* (quoting *Knotts*, 460 U.S. at 285).

326. *Id.* (quoting United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring in the judgment)).

327. *Id.* at 2216.

addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today."[328] The Chief Justice went on to say that

> [g]iven the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from Carpenter's wireless carriers was the product of a search.[329]

Perhaps most notably, the Chief Justice invoked both of the third-party doctrine's limiting principles discussed above while distinguishing *Miller* and *Smith*. First, he rejected the government's argument that the third-party doctrine operates categorically and without constraint to eviscerate any Fourth Amendment protection for records maintained by a commercial entity, insisting that *Miller* and *Smith* "did not rely solely on the act of sharing."[330] Instead, those cases require courts to consider "'the nature of the particular documents sought' to determine whether 'there is a "legitimate expectation of privacy" concerning their contents.'"[331] The Court then held that historic CSLI was entitled to Fourth Amendment protection because such information constitutes "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years" and, thus, "implicates privacy concerns far beyond those considered in *Smith* and *Miller*."[332]

Second, the Court rejected the contention that Carpenter voluntarily disclosed his CSLI to his wireless carriers.[333] It observed that CSLI "is not truly 'shared' as one normally understands the term" for two reasons[334]: (1) because cell phones are "indispensable to participation in modern society," carrying one may not actually be a

328. *Id.* at 2219.
329. *Id.* at 2217.
330. *Id.* at 2219.
331. *Id.* (quoting United States v. Miller, 425 U.S. 435, 442 (1976)).
332. *Id.* at 2220.
333. *Id.* at 2219.
334. *Id.*

completely voluntary choice;[335] and (2) cell phones are constantly in connection with cell sites and, thereby, generate CSLI "without any affirmative act on the part of the user beyond powering up."[336] Consequently, Carpenter had not "voluntarily 'assume[d] the risk' of turning over a comprehensive dossier of his physical movements."[337]

The Court also held that individuals have a reasonable expectation of privacy in CSLI.[338] Relying on the *Jones* concurrences, Chief Justice Roberts announced that society can reasonably expect law enforcement to refrain from monitoring and cataloguing an individual's every movement.[339] Analogizing CSLI surveillance to the GPS monitoring at issue in *Jones*, he further observed that "the time-stamped [CSLI] data provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations."[340] This is because "[a] cell phone faithfully follows its owner beyond public thoroughfares and into *private* residences, *doctor's offices*, political headquarters, and *other potentially revealing locales*."[341] Finally, the Court expressed concern that "the retrospective quality of the [CSLI] gives police access to a category of information otherwise unknowable" and the only limit on the government's ability to gather CSLI is the length of time the wireless carriers retain the data, "which currently [is] for up to five years."[342]

The Chief Justice concluded *Carpenter* by characterizing it as a "narrow" decision so as not to "embarrass the future."[343] He emphasized that *Miller* and *Smith* were still good law insofar as they apply to "conventional surveillance techniques and tools, such as security cameras."[344] The Court also explained that the case did not extend to "other collection techniques involving foreign affairs or national security."[345]

---

335. *Id.*
336. *Id.*
337. *Id.*
338. *Id.* at 2217.
339. *Id.*
340. *Id.* (quotations omitted)
341. *Id.* at 2218 (emphasis added).
342. *Id.*
343. *Id.* at 2220 (quoting Nw. Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)).
344. *Id.*
345. *Id.*

C. Justice Kennedy's Dissent

Justice Kennedy's dissent appears primarily motivated by his disagreement with the majority's interpretation and application of the third-party doctrine. In his view, Carpenter's CSLI records differed immaterially from the business records at issue in *Miller* and *Smith*.[346] Therefore, he concluded that the government's collection of CSLI records from Carpenter's wireless carriers did not constitute a search under the Fourth Amendment.[347] Deploying similar reasoning, he also contended that Carpenter could not have any reasonable expectation of privacy in his CSLI data because he neither owned nor controlled those records.[348]

D. Justice Alito's Dissent

Justice Alito's dissent advanced two distinct grievances with the majority opinion. First, he complained that "the Court ignores the basic distinction between an actual search (dispatching law enforcement officers to enter private premises and root through private papers and effects) and an order merely requiring a party to look through its own records and produce specified documents."[349] He further argued that "[t]he order in this case was the functional equivalent of a subpoena for documents, and there is no evidence that these writs were regarded as 'searches' at the time of the founding."[350]

In support of that proposition, Justice Alito expounded on the advent and deployment of subpoenas *duces tecum* and other forms of compulsory process under the common law from the reign of King Richard II until the founding of the United States.[351] He also provided a short history on the Court's evolution from *Boyd v. United States*,[352] which "held the compulsory production of documents to the same standard as actual searches and seizures,"[353] to *Oklahoma Press*,[354] which applied the considerably more lenient reasonable relevance test

346. *Id.* at 2232–33 (Kennedy, J., dissenting).
347. *Id.* at 2230.
348. *Id.* at 2229.
349. *Id.* at 2247 (Alito, J., dissenting).
350. *Id.*
351. *Id.* at 2247–50.
352. Boyd v. United States, 116 U.S. 616 (1886).
353. *Carpenter*, 138 S. Ct. at 2253 (Alito, J., dissenting).
354. Okla. Press Publ'g Co. v. Walling, 327 U.S. 186 (1946).

to subpoenas for corporate books and records.[355] According to Justice Alito, the common law history and applicable Court precedent make one thing clear: the compulsory production of documents pursuant to a subpoena is not a Fourth Amendment search subject to the warrant requirement because such production does not entail any physical intrusion or trespass.[356] At best, it is a "constructive search" subject only to the reasonable relevance standard of suspicion.[357]

Chief Justice Roberts responded to Justice Alito's subpoena-related arguments in the majority opinion. At the outset, he explained that "this Court has never held that the [g]overnment may subpoena third parties for records in which the suspect has a reasonable expectation of privacy" and that "[a]lmost all of the examples Justice Alito cites . . . contemplated requests for evidence implicating *diminished privacy interests* or *for a corporation's own books*."[358] Chief Justice Roberts further contended that "[i]f the choice to proceed by subpoena provided a categorical limitation on Fourth Amendment protection, [as purported by Justice Alito], *no type of record would ever be protected by the warrant requirement*."[359] This is because, "[u]nder Justice Alito's view, private letters, digital contents of a cell phone—any personal information reduced to document form, in fact—may be collected by subpoena for no reason other than 'official curiosity.'"[360]

Justice Alito's second grievance involved the Court's treatment of the third-party doctrine, which he maintained "destabilizes long-established Fourth Amendment doctrine."[361] His point was straightforward: Carpenter had no ownership interest in the CSLI records, which were the wireless carriers' property, and, consequently, he had no right to raise any Fourth Amendment objection regarding those records under *Miller* and *Smith*.[362] Justice Alito characterized the majority's decision, which permitted Carpenter to object to the search of third-party property, as "revolutionary" and inconsistent with "the original understanding of the Fourth Amendment and more than a century of Supreme Court precedent."[363]

355. *Carpenter*, 138 S. Ct. at 2252–54 (Alito, J., dissenting).
356. *Id.* at 2255 (Alito, J., dissenting).
357. *Id.*
358. *Id.* at 2221 (majority opinion) (emphasis added).
359. *Id.* at 2222 (emphasis added).
360. *Id.*
361. *Id.* at 2247 (Alito, J., dissenting).
362. *Id.* at 2257–61.
363. *Id.* at 2247.

Chief Justice Roberts also pushed back on Justice Alito's arguments that centered around textualism and precedent. The Chief Justice explained that the CSLI data at issue in the case, which tracked Carpenter's every movement over an extensive period of time, implicated the Fourth Amendment's concern with arbitrary government power in a way that the phone numbers and bank records under review in *Miller* and *Smith* did not.[364] Moreover, Chief Justice Roberts countered Justice Alito's reliance on *Miller* and *Smith* by pointing to the Court's decision in *Riley*, in which Justice Alito concurred, explaining that "[w]hen confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents."[365]

E. Justice Thomas's Dissent

Justice Thomas's dissent castigated the majority's reliance on the *Katz* privacy test,[366] which he argued should be overruled.[367] He characterized the *Katz* test as, among other things, "foreign to the ratifiers of the Fourth Amendment,"[368] "unworkable in practice,"[369] and "a failed experiment."[370] Justice Thomas's fervent advocacy for *Katz*'s demise stems from two propositions. First, "[t]he *Katz* test has no basis in the text or history of the Fourth Amendment."[371] Second, "it invites courts to make judgments about policy, not law."[372]

F. Justice Gorsuch's Dissent

Justice Gorsuch's dissent is perhaps the most intriguing, in part because it reads more like a concurrence.[373] The thrust of his opinion is a discussion of three potential ways to deal with the problem that is the third-party doctrine:

---

364. *Id.* at 2222 (majority opinion).

365. *Id*.

366. *Id.* at 2236 (Thomas, J., dissenting).

367. *Id.* at 2246 (contending that the Court "is dutybound to reconsider" *Katz v. United States*, 389 U.S. 347 (1967)).

368. *Id.* at 2243.

369. *Id.* at 2244.

370. *Id.* at 2246.

371. *Id.* at 2236.

372. *Id.*

373. Daniel Solove, Carpenter v. United States*, Cell Phone Location Records, and the Third Party Doctrine*, TEACHPRIVACY (July 1, 2018), https://teachprivacy.com/carpenter-v-united-states-cell-phone-location-records-and-the-third-party-doctrine [https://perma.cc/8GJC-5HKL] (explaining that Justice Gorsuch's dissent "should probably be a concurring opinion").

> The first is to ignore the problem, maintain *Smith* and *Miller*, and live with the consequences. If the confluence of these decisions and modern technology means our Fourth Amendment rights are reduced to nearly nothing, so be it. The second choice is to set *Smith* and *Miller* aside and try again using the *Katz* "reasonable expectation of privacy" jurisprudence that produced them. The third is to look for answers elsewhere.[374]

As Justice Gorsuch evaluated each of these options, he went to great lengths to repudiate both the third-party doctrine and *Katz*. In his view, *Smith* and *Miller* amount to little more than a "doubtful application of *Katz* that lets the government search almost whatever it wants whenever it wants."[375] As he explained,

> [t]oday we use the Internet to do most everything. Smartphones make it easy to keep a calendar, correspond with friends, make calls, conduct banking, and even watch the game. Countless Internet companies maintain records about us and, increasingly, *for* us. Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. *Smith* and *Miller* teach that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did.[376]

Justice Gorsuch concluded his dissent by proposing that the Court jettison the third-party doctrine and resolve cases involving the compulsory production of third-party papers by "look[ing] to a more traditional Fourth Amendment approach" grounded in the positive rights that attend to property.[377] Applying that approach, he contended that it is "entirely possible a person's cell-site data could qualify as *his* papers or effects under existing law" given the positive legal rights in such data provided to customers and subscribers under the SCA.[378] He also hinted that he may have ruled in Carpenter's favor on that basis had Carpenter not waived his right to invoke positive property rights in his CSLI, which was "his most promising line of argument."[379]

---

374. *Carpenter*, 138 S. Ct. at 2262 (Gorsuch, J., dissenting).
375. *Id.* at 2264.
376. *Id.* at 2262.
377. *Id.* at 2272.
378. *Id.*
379. *Id.*

V. *CARPENTER*'S APPLICATION TO STATE PDMP HEALTH INFORMATION

The *Carpenter* decision has been heralded as a "major statement on privacy in the digital age"[380] and a "landmark privacy case."[381] As explained above, *Carpenter* held that individuals have a reasonable expectation of privacy in their physical locations and movements. The key question in analyzing the cases involving PDMP subpoenas is whether patients have a similar expectation of privacy in records that contain their sensitive health information. The remainder of this Article discusses the applicability of *Carpenter* to prescribing records stored in state PDMPs.

Carpenter analyzed the petitioner's privacy rights in his CSLI data held by a third party by looking at the "intersection of two lines of cases"[382]: (1) decisions on expectations of privacy in physical location and movements;[383] and (2) precedent on the third-party doctrine.[384] The DEA's acquisition of patient prescribing records from state PDMPs, however, implicates a person's expectation of privacy in her health-care information and not in her locations and movements. As a result, this Article first discusses an individual's right to privacy in her prescribing records and then examines the post-*Carpenter* third-party doctrine.

A. The Right to Health-Information Privacy

Carpenter held that individuals have an expectation of privacy in their physical locations. The question for PDMP data is whether they have a similar expectation of privacy in their prescribing records. While there is no on-point *Fourth* Amendment precedent that controls the PDMP-data cases, courts have long recognized that individuals have

380. Adam Liptak, *In Ruling on Cellphone Location Data, Supreme Court Makes Statement on Digital Privacy*, N.Y. TIMES (June 22, 2018), https://www.nytimes.com/2018/06/22/us/politics/supreme-court-warrants-cell-phone-privacy.html [https://perma.cc/9UZ6-53RZ].

381. Alexia Ramirez & Rachel Levinson-Waldman, *Supreme Court Strengthens Digital Privacy*, BRENNAN CTR. FOR JUST. (June 22, 2018), https://www.brennancenter.org/blog/supreme-court-strengthens-digital-privacy [https://perma.cc/E4TS-6NGX]. *But see* Amy Davidson Sorkin, *In* Carpenter*, the Supreme Court Rules, Narrowly, for Privacy*, NEW YORKER (June 22, 2018) https://www.newyorker.com/news/daily-comment/in-carpenter-the-supreme-court-rules-narrowly-for-privacy [https://perma.cc/A5LF-ZPX7] ("*Carpenter* is not quite a full manifesto for digital privacy, but it insists that there is a new discussion to be had, and it tries to set the terms.").

382. *Carpenter*, 138 S. Ct. at 2214–15.

383. *Id.* at 2215.

384. *Id.* at 2216.

significant *Fourteenth* Amendment constitutional privacy interests in their medical records. And courts and commentators have repeatedly recognized that Fourteenth Amendment privacy interests may influence or inform individuals' reasonable expectations of privacy in the Fourth Amendment context.[385] This Section provides a detailed summary of the courts' consistent treatment of health-care data as exceptionally private, beginning with applicable Fourteenth Amendment precedent. It then describes the Supreme Court's relevant commentary connecting health data and privacy. This Section concludes by summarizing other sources of federal and state law that support the contention that individuals have a reasonable expectation of privacy in their prescribing-related health information.

1. *Fourteenth Amendment Case Law*. Fourteenth Amendment precedent makes it clear that individuals have a reasonable expectation of privacy in their health-care records. The Court's decision in *Whalen v. Roe*[386] expounded on patients' privacy interests in their prescribing-related health information. At issue was a 1972 New York state statute that required physicians to report certain Schedule II drug-prescribing information to the New York State Department of Health ("DOH").[387] A group of patients and physicians challenged the statute, contending that it violated their Fourteenth Amendment rights to "nondisclosure of private information" and to make to independent health-care-related decisions.[388] The Court rejected those arguments, noting that "disclosures of private medical information to doctors, to hospital personnel, to insurance companies, and to public health agencies are often an essential part of modern medical practice even when the disclosure may reflect unfavorably on the character of the patient."[389] In addition, the Court emphasized that "[p]ublic disclosure of the identity of patients [wa]s expressly prohibited by the statute and by a [DOH] regulation."[390]

385. *See, e.g.*, Ferguson v. City of Charleston, 532 U.S. 67, 78 n.14 (2001).

386. Whalen v. Roe, 429 U.S. 589 (1977).

387. *Id.* at 593 (explaining that the statute required the physician to report "identifi[cation of] the prescribing physician"; "the dispensing pharmacy"; and "the drug and dosage" as well as "the name, address, and age of the patient" to DOH upon the prescribing of a Schedule II controlled substance).

388. *Id.* at 599–600.

389. *Id.* at 600.

390. *Id.*

Although the *Whalen* Court did not invalidate the New York statute on privacy grounds under the circumstances, it did recognize "the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files"—more than forty years ago.[391] Justice Stevens explained that

> [t]he right to collect and use [personal and potentially embarrassing] data for public purposes *is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures*. . . . New York's statutory scheme . . . evidence[s] a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data—whether intentional or unintentional—or by a system that did not contain comparable security provisions.[392]

Separately concurring in *Whalen*, Justice Brennan explained that "[b]road dissemination by state officials of [patient prescribing records] . . . would clearly implicate constitutionally protected privacy rights, and would presumably be justified only by compelling state interests."[393] He further contended that "[t]he central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information" and, as such, he was "not prepared to say that future developments will not demonstrate the necessity of some curb on such technology."[394] With regard to that concern, he concurred with the majority only because "[t]he information disclosed by the physician under this program *is made available only to a small number of public health officials with a legitimate interest in the information*."[395]

In sum, *Whalen* recognized that (1) patients and prescribers have Fourteenth Amendment privacy interests in their prescribing records; (2) patients have a constitutional privacy interest in their right to make independent health-care decisions; and (3) compulsory disclosure of prescribing-related records to a state public-health agency is constitutional under the Fourteenth Amendment so long as the disclosure scheme has safeguards in place to ensure the privacy of that state-collected information. The DEA invoked *Whalen* in both the

391. *Id.* at 605.

392. *Id.* at 605–06 (emphasis added).

393. *Id.* at 606 (Brennan, J., concurring) (citing Roe v. Wade, 410 U.S. 113, 155–56 (1973)).

394. *Id.* at 607.

395. *Id.* at 606 (emphasis added).

Oregon and Utah PDMP cases to support its argument that patients have no reasonable expectation of privacy in their prescribing records. *Whalen*, however, expressly acknowledges that both patients and doctors have a reasonable expectation of privacy in that information,[396] which the Court then balanced against the government's legitimate public-welfare interests effectuated by the challenged statutory scheme.[397] Moreover—and contrary to the DEA's position in the PDMP cases—*Whalen* presumed that the prescribing data collected by the New York DOH would be protected from disclosure by the state statute at issue and not undermined or eroded by a less protective federal statutory provision.

In addition, and unlike in *Whalen*, none of the interested parties in the PDMP cases challenged their respective state health agency's right to compel collection of their prescribing information. In fact, the PDMP cases were *instigated by the state PDMP agencies' refusal to comply with DEA subpoenas* without a warrant. Thus, *Whalen* does not answer whether the DEA is required to obtain a warrant to access PDMP data.

In another decision that advances the notion that patients have a reasonable expectation of privacy in their health-care records, the Supreme Court struck down the mandatory reporting requirements of the Pennsylvania Abortion Control Act in *Thornburgh v. American College of Obstetricians & Gynecologists.*[398] In concluding that the Pennsylvania reporting statute was unconstitutional, *Thornburgh* expressly relied on the threat of public disclosure of sensitive patient reporting information and its attendant "chilling" effect on patient behavior: "Pennsylvania's reporting requirements raise the specter of public exposure and harassment of women who choose to exercise their personal, intensely private, right, with their physician, to end a pregnancy. Thus, they pose an unacceptable danger of deterring the exercise of that right, and must be invalidated."[399]

---

396. *Id.* at 598–600 (majority opinion).

397. *Id.* at 600–04.

398. Thornburgh v. Am. Coll. of Obstetricians & Gynecologists, 476 U.S. 747, 766–68 (1986), *overruled by* Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833 (1992); *see also id*. at 765 (explaining that the Pennsylvania statute mandated that abortion providers give the state a detailed individual report on each abortion they had performed, including the physician's name and the name of the facility where the abortion was performed, the woman's age, race, marital status and number of prior pregnancies, her political party and state of residence, and method of payment).

399. *Id.* at 767–68.

Thornburgh and subsequent Supreme Court case law have challenged—if not outright rejected—the Court's reasoning in *Whalen*. *Roe v. Wade* and its progeny, for example, "ma[d]e it clear that [an individual's constitutional] right [to privacy applies to fundamental personal rights and] has some extension to activities relating to marriage, procreation, contraception, family relationships, and child rearing and education."[400] These cases, moreover, hold that the Fourteenth Amendment right to privacy "encompass[es] a woman's decision whether or not to terminate her pregnancy"[401] and her access to contraception,[402] including her right "to obtain private counseling, access to medical assistance and up-to-date information in respect to proper methods of birth control."[403]

Needless to say, a woman's prescribing history could reveal that she exercised either her right to access contraception or to terminate a pregnancy. Such information includes all medications prescribed to her for ex ante or ex post attempts to avoid conception, ranging from birth-control pills to Plan B prescriptions.[404] It also identifies her prescriber, which very well may be the only abortion provider in the area.

The majority of the federal circuit courts also have concluded that a Fourteenth Amendment right to privacy extends to medical records, prescription records, or both—often in reliance on the abortion and

400. Roe v. Wade, 410 U.S. 113, 152–53 (1973) (quotations and citations omitted); *id.* at 152 (contending that "the Court has recognized that a right of personal privacy . . . does exist under the Constitution" and has "found at least the roots of that right . . . in the Fourth and Fifth Amendments").

401. *Id.* at 153.

402. Griswold v. Connecticut, 381 U.S. 479, 484–85 (1965).

403. *Id.* at 503 (Harlan, J., concurring).

404. *See, e.g.*, KIMBERLY DANIELS, JILL DAUGHERTY, JO JONES & WILLIAM MOSHER, NAT'L HEALTH STATISTICS REPORTS, CURRENT CONTRACEPTIVE USE AND VARIATION BY SELECTED CHARACTERISTICS AMONG WOMEN AGED 15–44: UNITED STATES, 2011–2013 (Nov. 10, 2015), https://www.cdc.gov/nchs/data/nhsr/nhsr086.pdf [https://perma.cc/4MGG-GXMC] (explaining that "virtually all sexually experienced women in the United States have used contraception at some time in their lives" and that the pill was the most common method of such contraception).

contraception cases.[405] In *Douglas v. Dobbs*,[406] for instance, the Tenth Circuit had "no difficulty concluding that protection of a right to privacy in a person's prescription drug records, which contain intimate facts of a personal nature, is sufficiently similar to other areas already protected within the ambit of privacy."[407] In reaching that result, the court reasoned that "[i]nformation contained in prescription records not only may reveal other facts about what illnesses a person has, but may reveal information relating to procreation—whether a woman is taking fertility medication for example—as well as information relating to contraception."[408]

2. *Fourth Amendment Case Law*. The Supreme Court also has recognized that patients have a Fourth Amendment reasonable expectation of privacy in their health records. In *Ferguson*, for example, the Court held that patients have a reasonable expectation that their attending hospital would not share their diagnostic-test records "with nonmedical personnel without [their] consent."[409] The

405. *See, e.g.*, Kerns v. Bader, 663 F.3d 1173, 1184 (10th Cir. 2011) ("[A] patient has a privacy interest in medical records held by a third party medical services provider."); Douglas v. Dobbs, 419 F.3d 1097, 1102 (10th Cir. 2005) ("We have previously applied th[e] right [to privacy] in the context of an employer's search of an employee's medical records, and in the context of a government official's disclosure of a person's HIV status." (citation omitted)); Tucson Woman's Clinic v. Eden, 379 F.3d 531, 550 (9th Cir. 2004) ("[A]ll provision of medical services in private physicians' offices carries with it a high expectation of privacy for both physician and patient."); Doe v. Broderick, 225 F.3d 440, 451 (4th Cir. 2000) (holding that a patient had a legitimate expectation of privacy in his records on file at a methadone clinic); Herring v. Keenan, 218 F.3d 1171, 1173 (10th Cir. 2000) ("[T]here is a constitutional right to privacy that protects an individual from the disclosure of information concerning a person's health."); Doe v. Se. Pa. Transp. Auth., 72 F.3d 1133, 1137–38 (3d Cir. 1995) ("It is now possible from looking at an individual's prescription records to determine that person's illnesses, or . . . ascertain such private facts as whether a woman is attempting to conceive . . . through the use of fertility drugs. This information is precisely the sort intended to be protected by penumbras of privacy."); Doe v. City of New York, 15 F.3d 264, 267 (2d Cir. 1994) ("Extension of the right to confidentiality to personal medical information recognizes that there are few matters that are quite so personal as the status of one's health, and few matters the dissemination of which one would prefer to maintain greater control over."); *see also* Harris v. Thigpen, 941 F.2d 1495, 1513 (11th Cir. 1991) (assuming that the right exists); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980) ("Information about one's body and state of health is matter which the individual is ordinarily entitled to retain within the 'private enclave where he may lead a private life.'" (quoting United States v. Grunewald, 233 F.2d 556, 581–82 (2d Cir. 1956) (Frank, J., dissenting)). *Contra* Jarvis v. Wellman, 52 F.3d 125, 126 (6th Cir. 1995) (holding that the constitutional right of privacy does not apply to medical records).

406. Douglas v. Dobbs, 419 F.3d 1097 (10th Cir. 2005).

407. *Id.* at 1102 (citing *Griswold*, 381 U.S. at 484).

408. *Id.* (citations omitted).

409. Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001).

Ferguson Court also acknowledged that "an intrusion on that expectation [of privacy] may have adverse consequences because it may deter patients from receiving needed medical care."[410]

Although *Ferguson* is important and persuasive precedent, it is distinguishable from the PDMP cases. *Ferguson* did not involve state-sanctioned collection of health-care information because no law required the state hospital to perform the diagnostic tests at issue.[411] *Ferguson* also did not concern a law enforcement demand for sensitive health data held by a state actor pursuant to a compulsory process expressly endorsed by a federal statute, like the CSA.[412] Indeed, the state hospital in *Ferguson* voluntarily submitted its patients' diagnostic drug-test results to local law enforcement pursuant to a collaborative agreement.[413]

Notably, the Supreme Court has referenced the private nature of an individual's medical appointments and health-care-related internet searches on several occasions in its recent digital-surveillance cases. In *Carpenter*, Chief Justice Roberts pointed out that "[a] cell phone faithfully follows its owner beyond public thoroughfares and into private residences, *doctor's offices*, political headquarters, and *other potentially revealing locales*."[414] Justice Gorsuch's dissent also points out that indiscriminate application of the third-party doctrine leads to the inevitable conclusion that "the Constitution does nothing to limit investigators from searching records you've entrusted to your bank, accountant, and *maybe even your doctor*."[415]

The unanimous majority in *Riley*, which held that police are forbidden from searching an individual's cell phone incident to arrest, expressed similar concerns. There, Chief Justice Roberts pointed out that "an Internet-enabled phone . . . could reveal an individual's privacy interests or concerns—perhaps *a search for certain symptoms*

410. *Id.* at 78 n.14 (citing Whalen v. Roe, 429 U.S. 589, 599–600 (1977)).

411. *Id.* at 70–73 (explaining that the hospital decided on its own accord to conduct nonconsensual and surreptitious urine screens of pregnant women receiving prenatal treatment on the theory that there was an "apparent increase in the use of cocaine" by those patients and "such use harmed the fetus and was therefore child abuse").

412. *Id.* (providing that the hospital reached out to local law enforcement to offer its "cooperation in prosecuting mothers whose children tested positive for drugs at birth").

413. *Id.* at 71–72 (explaining that the hospital entered into a collaborative agreement with local law enforcement in which it agreed to test a patient "for cocaine through a urine drug screen if she met one or more of nine criteria" and then immediately refer any patients who tested positive while pregnant to law enforcement for arrest and prosecution).

414. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) (emphasis added).

415. *Id.* at 2261 (Gorsuch, J., dissenting) (emphasis added).

of disease, coupled with frequent visits to WebMD."[416] Justice Sotomayor likewise explained in her *Jones* concurrence that GPS data could disclose "trips the indisputably private nature of which takes little imagination to conjure: *trips to the psychiatrist, the plastic surgeon, the abortion clinic, [and] the AIDS treatment center*."[417]

The point here is a simple one: if information that reveals one's trips to a doctor's office, abortion clinic, or AIDS treatment center is of an "indisputably private nature" and cell phone searches trigger significant privacy concerns because they could disclose frequent visits to WebMD or searches for disease symptoms, then an individual has a reasonable expectation of privacy in their sensitive and often disease-identifying prescribing records. Indeed, medical prescribing records frequently expose more personal and potentially stigmatizing information than one's treatment-related travel or web searches.

3. *Other Pertinent Privacy Statutes and Regulations*. Federal statutes and regulations further support the claim that patients have a reasonable expectation of privacy in their prescribing records. For instance, HIPAA[418] and the Health Information Technology for Economic and Clinical Health Act[419] prohibit the nonconsensual disclosure of patients' protected health information to third parties by covered entities and their business associates.[420] Similarly, 42 C.F.R. § 2 protects identifying information concerning individuals in substance-abuse treatment programs.[421] Various state constitutions[422] and privacy

416. Riley v. California, 573 U.S. 373, 395–96 (2014) (emphasis added).

417. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)).

418. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

419. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 115 (2009) (enacted as part of the American Recovery and Investment Act of 2009, Pub. L. 111-5, 123 Stat. 115).

420. 42 U.S.C. §§ 17931, 17934 (2018); 45 C.F.R. § 164.512(f) (2018).

421. 42 C.F.R. § 2 (2018).

422. Manela v. Superior Court, 99 Cal. Rptr. 3d 736, 744 (Cal. Ct. App. 2009) (recognizing the California constitutional right to privacy in medical records); State v. Johnson, 814 So. 2d 390, 393 (Fla. 2002) (recognizing the Florida constitutional right to privacy in medical records); King v. State, 535 S.E.2d 492, 494–95 (Ga. 2000) (recognizing the Georgia constitutional right to privacy in medical records); Brende v. Hara, 153 P.3d 1109, 1115 (Haw. 2007) (recognizing the Hawaii constitutional right to privacy in medical records); State v. Skinner, 10 So. 3d 1212, 1218 (La. 2009) (holding that "a warrant is required to conduct an investigatory search of medical and/or prescription records" under the Louisiana Constitution); T.L.S. v. Mont. Advocacy Program, 144 P.3d 818, 824 (Mont. 2006) (recognizing the Montana constitutional right to privacy in a patient's medical history); *see also* Catherine Louisa Glenn, *Protecting Health Information Privacy: The*

statutes[423] also bolster the conclusion that individuals have privacy rights in their health-care records. And the majority of states expressly extend privacy protections to patient prescribing information in their PDMP statutes, including provisions that limit law enforcement access to PDMP data.[424] The volume of positive law providing privacy protections to patient data would go a long way to convincing a judge like Justice Gorsuch, who seemed sympathetic to such an argument in his *Carpenter* dissent.[425]

In sum, myriad sources of federal and state law indicate that patients have a reasonable expectation of privacy in their PDMP prescribing information. By comparison, the Court's holding that Carpenter had a reasonable expectation of privacy in his location and movements drew largely from two concurring opinions from a single prior Court decision—*United States v. Jones*.[426] Justice Kennedy's dissent, in fact, criticizes the majority for grounding its holding on such little support.[427] A parallel holding that individuals have reasonable expectations of privacy in their historic prescribing information would rest on a considerably more robust positive-law foundation than that which supported the Court's ruling concerning an individual's locations and movements in *Carpenter*.

Finally, the *Carpenter* majority held that the petitioner had a reasonable expectation of privacy in his CSLI even though those records largely revealed his *public* movements. The Court reasoned that "what one seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[428] The PDMP cases, however, do not involve any information that patients exposed to the public. Instead, the data at issue in the PDMP cases—patient

Case for Self-Regulation of Electronically Held Medical Records, 53 VAND. L. REV. 1605, 1609 n.25 (2000) (identifying the constitutions of Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington as protecting health-information privacy).

423. *See, e.g.*, Nicolas P. Terry, *What's Wrong with Health Privacy?*, 5 J. HEALTH & BIOMEDICAL L. 1, 6 n.19 (2009) (listing state statutes that protect health information).

424. LAW ENFORCEMENT ACCESS TO PDMP REPORTS, *supra* note 54 (demonstrating that at least twenty-eight states require law enforcement to obtain a warrant or court order to obtain PDMP data).

425. Carpenter v. United States, 138 S. Ct. 2206, 2272 (2018) (Gorsuch, J., dissenting).

426. *Id.* at 2217 (2018) (Alito, J., concurring) (first citing United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring in the judgment); then citing *id.* at 415 (Sotomayor, J., concurring)).

427. *Carpenter*, 128 S. Ct. at 2231 (Kennedy, J., concurring).

428. *Id.* at 2217 (majority opinion) (quoting Katz v. United States, 389 U.S. 347, 351–52 (1967)).

prescribing records—are generated as a result of confidential physician–patient communications for the purpose of providing health-care diagnosis and treatment. Given the Court's determination that individuals' public travel and movements "hold for many Americans the 'privacies of life[,]'"[429] it is difficult to controvert the conclusion that historic prescribing information does, too.

*B. The Post-*Carpenter *Third-Party Doctrine*

The Supreme Court refused to "mechanically apply[] the third-party doctrine" to CSLI records in *Carpenter*.[430] Instead, it explained that, while "[t]he . . . doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with [others,] . . . *Smith* and *Miller* . . . did not rely solely on the act of sharing."[431] *Smith* and *Miller*, as the Chief Justice pointed out, require courts to take into consideration the nature of the documents sought in determining whether the search target has a legitimate expectation of privacy in their contents *notwithstanding information sharing*.[432] Moreover, the third-party doctrine is rooted in the concept of *voluntary* exposure.[433] This is because the doctrine's assumption-of-the-risk rationale does not hold up absent a consensual transfer of information from the target to the third party.[434] This Section applies these dispositive third-party-doctrine limiting principles to PDMP prescribing information.

1. *The Nature of the Records Sought.* The records at issue in the PDMP cases—medical records that include patient prescribing information—are extremely revealing, often sensitive, and undoubtedly private in nature. As the Oregon district court acknowledged in its PDMP decision, "[i]t is difficult to conceive of information that is more private or more deserving of Fourth Amendment protection."[435] Indeed, knowledge of nothing more than the identity of the drug that a physician has prescribed to a patient can reveal that patient's medical condition with specificity. For example, a

429. *Id.* (quoting Riley v. California, 573 U.S. 373, 403 (2014)).

430. *Id.* at 2219.

431. *Id.*

432. *Id.*

433. *Id.*

434. *Id.* at 2220.

435. Or. Prescription Drug Monitoring Program v. U.S. Drug Enf't Admin., 998 F. Supp. 2d 957, 966 (D. Or. 2014), *rev'd*, 860 F.3d 1228 (9th Cir. 2017).

patient whose PDMP records disclosed that the patient was on a prescribed treatment regime of biweekly, self-administrated, injectable testosterone—a Schedule III controlled substance—would be exposed as having a diagnosis of gender dysphoria—a condition that has no alternative indicated pharmaceutical treatment.[436] Moreover, and as the intervenors explained in the Oregon PDMP litigation, information about the quantity and frequency of a patient's testosterone prescriptions discloses not only that the patient is transitioning from female to male, but also the precise stage of that patient's transition.[437]

In addition, and as explained above, a wide range of positive law, including the constitutional right to privacy and numerous federal and state statutes, supports the determination that patients have a reasonable expectation of privacy in their prescribing-related health records. The Oregon PDMP statute, for instance, is highly protective of patients' right to confidentiality in their prescribing information. It expressly provides that prescription monitoring data submitted to the PDMP "[i]s protected health information,"[438] and "[i]s confidential and not subject to disclosure"[439] but for a limited number of narrow exceptions. Most importantly, such data is only subject to law enforcement agency access "[p]ursuant to a valid court order based on probable cause" where such agency is engaged "in an authorized drug-related investigation involving a person to whom the requested information pertains."[440] As a result, it is easy to argue that an Oregon patient has a reasonable expectation of privacy in their prescribing information. Privacy expert Daniel Solove's recent musings about the third-party doctrine's application to medical records sum things up nicely:

> Would the Supreme Court really hold that people lack an expectation of privacy in their medical data because they convey that information to Third Parties (their physicians)? The result would strike many as absurd. The logic of the Third Party Doctrine leads to this result, which is probably why the Supreme Court has avoided taking a case

436. Plaintiff-Intervenors Complaint at 16, *Or. Prescription Drug Monitoring Program*, 998 F. Supp. 2d 957 (No. 12-2023).

437. *Id.* at 22; *see also id.* at 19 (explaining that knowledge that a patient is taking certain medication, such as clonazepam, reveals that the individual has been diagnosed with mental illness).

438. OR. REV. STAT. § 431A.865(1)(a)(A) (2017).

439. *Id.* § 431A.865(1)(a)(B).

440. *Id.* § 431A.865(2)(a)(G).

> that would result in this holding. It would be the kind of case that would lead to a public uproar.[441]

2. *The Voluntariness of the Information Conveyed.* The third-party doctrine's assumption-of-the-risk rationale rests on voluntariness: that a person does not assume the risk of third-party betrayal unless he or she voluntarily transfers information to that third party. The *Carpenter* Court relied on this fundamental limitation of the third-party doctrine in holding that the petitioner had a reasonable expectation of privacy in his CSLI.[442] As the majority reasoned, Carpenter's CSLI was "not truly 'shared' [with his wireless carrier] as one normally understands the term" for two reasons.[443] First, cell phones are pervasive to the extent that "carrying one is indispensable to participation in modern society."[444] Second, "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user besides powering up."[445]

The receipt of necessary medical treatment, including prescription-drug therapy, is similarly "indispensable to participation in modern society,"[446] particularly when such treatment is necessarily indispensable to living. And while the decision to forgo cell phone use might be debilitating, it is highly unlikely to initiate or contribute to a public-health catastrophe. But when individuals forgo treatment for communicable diseases, such as, for example, MRSA, tuberculosis, hepatitis, Ebola, HIV, influenza, and gonorrhea, public health and safety is placed in peril. Public health and safety are also implicated when individuals avoid medical treatment for mental illness, substance-use disorder, or other stigmatizing conditions.

Moreover, a patient's confidential disclosure of sensitive health information to her physician for the purposes of diagnosis and treatment does not vitiate her reasonable expectation of privacy in that data. The Supreme Court held as much in *Ferguson* when it ruled that patients had a reasonable expectation of privacy in the health-care-

---

441. Daniel Solove, *10 Reasons Why the Fourth Amendment Third Party Doctrine Should Be Overruled in* Carpenter v. US, TEACHPRIVACY (Nov. 28, 2017), https://teachprivacy.com/carpenter-v-us-10-reasons-fourth-amendment-third-party-doctrine-overruled [https://perma.cc/7N2T-E5EF].

442. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

443. *Id.*

444. *Id.*

445. *Id.*

446. *Id.*

related information they voluntarily conveyed to a state hospital for medical-treatment purposes.[447] Similarly, in *National Treasury Employees Union v. Von Raab*,[448] the Court held that employees had a reasonable expectation of privacy in the results of the urine tests that they voluntarily disclosed to a third party—their employer. As the *Von Raab* Court explained, those "[t]est results may not be used in a criminal prosecution of the employee without the employee's consent."[449]

Importantly, the Court has also "assumed . . . for many reasons, [that] physicians have an interest in keeping their prescription decisions confidential."[450] As physicians have recognized dating back to the inception of the Hippocratic Oath,[451] patient confidences "impose[] an obligation of secrecy upon [doctors], and thus prevent [their] making public what [they] cannot avoid seeing or hearing."[452] In keeping with that tradition, the American Medical Association has promulgated an ethics rule that "information disclosed to a physician during the course of the relationship between physician and patient is confidential to the greatest possible degree."[453] Consistent with this fundamental tenet of the practice of medicine, at least forty-four states, including Oregon and Utah, "have enacted physician-patient privilege statutes."[454] The purposes of the physician–patient privilege include, among other things, "further[ing] the doctor-patient relationship," "encourag[ing] unrestrained communication," and "encourag[ing]

447. Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001) ("The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent.").

448. Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656 (1989).

449. *Id.* at 666.

450. Sorrell v. IMS Health Inc., 564 U.S. 552, 572 (2011).

451. See, for example, *In re: Vioxx Products Liability Litigation*, No. MDL 1657, 2005 WL 2036797 (E.D. La. July 22, 2005), where the court wrote:

> The classical version of the Hippocratic Oath reads in pertinent part: "What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about."

Id. at *3.

452. Benjamin Rush, *On the Duties of Patients to Their Physicians*, *in* SIXTEEN INTRODUCTORY LECTURES 322 (1811).

453. COUNCIL ON ETHICAL & JUDICIAL AFFAIRS, AM. MED. ASS'N, CODE OF MEDICAL ETHICS: CURRENT OPINIONS WITH ANNOTATIONS 88 (1998).

454. Yedishtra Naidoo & J. Richard Ciccone, *The Reporting of Child Abuse Argued as an Exception to Physician–Patient Privilege in Criminal Proceedings*, 44 J. AM. ACAD. PSYCH. & L. 270, 271 (2016).

physicians to fully and accurately record their patients' confidential information."[455]

The long-standing confidentially rules that apply to physician–patient communications cut against the notion that patients voluntarily abandon the sensitive and intimate information they share with their providers in the course of diagnosis and treatment. Instead, these laws, which expressly attend heightened privacy protections to physician–patient communications, lead patients to reasonably believe that the information they convey to their health care providers is shielded from unfettered law enforcement access. Moreover and as already emphasized, patients cannot avoid sharing information with their providers unless they are willing to sacrifice their access to potentially life-saving health-care treatment. "Even compared to owning a smartphone, individuals cannot easily choose to avoid professional medical care, making the production of these records inescapable and automatic."[456]

Finally, even assuming that a patient's decision to communicate sensitive, prescribing-related information to her physician for treatment and diagnosis amounts to a "voluntary" transfer of that information for third-party doctrine purposes, it is irrelevant in the context of the PDMP cases. This is because patients never share their prescribing data with the state PDMPs—voluntarily or otherwise. And dispensers only do so involuntarily because they are mandated to transfer patient prescribing-related information to the PDMPs by state law.

*C. Potential Post-*Carpenter *Pitfalls*

This Article contends that DEA warrantless searches of PDMP prescribing information violate the Fourth Amendment under pertinent pre-*Carpenter* precedent and *Carpenter* itself. Two potential pitfalls, however, challenge these conclusions. First, certain distinctions between the type of data that the FBI sought in *Carpenter*—CSLI—and the type of data the DEA seeks from PDMPs—prescribing-related health information—could provoke a ruling that patients do not have a reasonable expectation of privacy in their PDMP records. Second, lower federal courts might uphold warrantless DEA PDMP searches pursuant to the "highly regulated industries" exception to the Fourth

455. *Id.*

456. Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357, 383 (2019).

Amendment, which is separate and distinct from the third-party doctrine. Each of these challenges is discussed, in turn, below.

1. Carpenter *May Not Apply to PDMP Databases Due to Their Lack of Sophistication and Pervasiveness*. It is possible to read *Carpenter*, alongside *Riley* and *Jones*, as little more than an extension of special or heightened Fourth Amendment protection to devices like cell phones and GPS units and the data those devices store and emit. This would make these cases inapplicable to less sophisticated, electronically stored third-party information, such as that contained in PDMPs, regardless of the significance of the privacy concerns that attend to those databases. This limited reading of *Carpenter* is provoked by at least three observations: the Court's overt refusal to overrule *Smith* and *Miller*;[457] its overriding concern about pervasive, nonstop surveillance;[458] and its emphasis on the narrowness of its decision and express refusal to extend its holding to "conventional surveillance techniques."[459] As one legal scholar has noted, *Carpenter* "evinces . . . a profound *tech exceptionalism*."[460] In fact, the Court's heavy reliance on the ever-increasing sophistication and accuracy of CSLI throughout *Carpenter*, alone, indicates that it seeks to draw a line between older digital technologies and new data-collection systems.

While it remains to be seen which side of that line the Court will deem appropriate for patient prescribing information collected by state PDMP databases, the growing sophistication of PDMP databases supports imposing a warrant requirement. PDMPs are no longer simply passive databases that store voluminous amounts of sensitive and potentially stigmatizing patient health-care data. Instead, they are "smart" databases that rely on robust data-analytics software. One such software, "NarxCare," uses black-box algorithms that mine through a patient's PDMP information to produce multiple three-digit "risk scores," including a composite overdose-risk score, collectively called "Narx Scores."[461] Moreover, the company that owns NarxCare

457. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

458. *Id.* at 2219–20.

459. *Id.* at 2220.

460. Ohm, *supra* note 456, at 360.

461. Appriss's website provides details about its PDMP software, NarxCare, stating that "NarxCare is a robust analytics tool and care management platform that helps prescribers and dispensers analyze real-time controlled substance data from Prescription Drug Monitoring Programs (PDMPs) and manage substance use disorder" and that "NarxCare automatically analyzes PDMP data and a patient's health history and provides patient risk scores and an

and controls its algorithms, Appriss Health, describes NarxCare as "a robust analytics tool and care management platform" and concedes that

> [t]he identification of patients at risk is only the beginning of a comprehensive platform needed to impact the increasing prevalence of substance use disorder. NarxCare extends beyond information and insights to provide tools and resources to enable care teams to support patient needs.[462]

Appriss also has publicly stated that it is working to gather pertinent information from patient electronic health records, including emergency-room records, court records, and other sources in order to improve and hone the precision of its predictive Narx Score algorithms. In fact, at least three states already incorporate patients' criminal histories into their PDMP databases.[463] PDMPs, therefore, are constantly evolving by collecting more and more sensitive data from an expansive number of sources and adopting smarter and smarter trade-secret-protected software, data-analytics tools, and algorithms. As a result, even assuming PDMPs are not yet sophisticated and pervasive enough to satisfy *Carpenter* today, they are swiftly—and inevitably—moving in that direction.[464]

In the age of "personalized" medicine, the growing precision and sophistication of targeted pharmaceutical treatments and pharmacogenetics presents an additional argument in response to the contention that PDMPs are not sufficiently technologically advanced to satisfy *Carpenter*. As noted earlier in this Article, PDMP data is incredibly sensitive. In fact, the development of targeted pharmaceutical treatments means not only that it is entirely possible to identify a patient's medical condition or diagnosis with the patient's prescribing data, but that it is sometimes possible to identify the stage of the patient's condition or disease with dose or quantity data. In addition, the emerging field of pharmacogenetics promises the

---

interactive visualization of usage patterns to help identify potential risk factors." *NarxCare*, APPRISS (2019), https://apprisshealth.com/solutions/narxcare [https://perma.cc/T3FS-D3MJ].

462. *Id.*

463. Beletsky, *supra* note 52, at 169 (explaining that Wisconsin, Kentucky, and Maine integrate criminal justice information into their state PDMPs).

464. Bolstering this point, the United States Court of Appeals for the Seventh Circuit recently applied *Carpenter* to conclude that government access to "smart" electric-meter data constitutes a Fourth Amendment search. *See* Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 527 (7th Cir. 2018).

development of even more sensitive and precise disease-identifying PDMP data.[465]

"The aim of pharmacogenetics is to combine targeted therapies with companion pretreatment diagnostic tests, which identify whether a person carries a gene or other biomarker that is linked with increased sensitivity to or resistance to the particular treatment."[466] This burgeoning field has already realized some measure of success in various oncological treatments. The federal Food and Drug Administration, for example, has approved the drug Herceptin to treat "HER2" positive tumors.[467] And "[o]ther molecular tests paired with appropriately targeted therapeutics are available for other cancer types including malignant melanoma, colorectal cancer, and several subtypes of leukemia and lymphoma."[468] Thus, while the PDMP databases may appear simple on initial glance, the information that populates them is incredibly revealing and constantly growing in sophistication.

Instead of relying the sophistication of PDMP-database software, analytics, and smart algorithms to contend that PDMP prescribing information should fall within the ambit of *Carpenter*, health-data advocates should consider arguing that it is the sophistication and sensitivity of the controlled-substance information *stored* in PDMPs that satisfies *Carpenter*'s implicit advanced-technology requirement. Relying on similar logic, at least one legal scholar has already contended that databases that contain genetic data are entitled to Fourth Amendment warrant protection under *Carpenter*.[469]

2. Carpenter *Does Not Address the Highly Regulated Industries Exception to the Warrant Requirement*. The Supreme Court has long held that "administrative searches conducted without a warrant . . . [violate] the Fourth Amendment guarantee[]" against unreasonable searches.[470] The Court nonetheless has created an exception to the warrant requirement for searches of "highly regulated industries." Over the past half century, the Court has identified only four

465. Dianne Nicol et al., *Precision Medicine: Drowning in a Regulatory Soup?*, 3 J.L. & BIOSCIENCES 281, 287 (2016).

466. *Id.*

467. *Id.* at 288.

468. *Id.*

469. *See generally* Natalie Ram, *Genetic Privacy After* Carpenter, 105 VA. L. REV. 1357 (2019).

470. Camara v. Mun. Court of S.F., 387 U.S. 523, 534 (1967).

industries—liquor sales,[471] firearms dealing,[472] mining,[473] and automobile junkyards[474]—that are subject to such expansive government oversight that "no reasonable expectation of privacy could exist for a proprietor over the stock of such an enterprise."[475]

Whether an industry is highly regulated depends on the "duration of the [applicable] regulation's existence, [the] pervasiveness of the regulatory scheme, and [the] regularity of the regulation's application."[476] If a court concludes that an industry is highly regulated, the court must then determine whether the warrantless search at issue is reasonable. Three criteria must be met: (1) "there must be a 'substantial' government interest that informs the regulatory scheme pursuant to which the inspection is made"; (2) "the warrantless inspections must be 'necessary to further [the] regulatory scheme'"; and (3) "the statute's inspection program . . . [must] provid[e] a constitutionally adequate substitute for a warrant."[477]

The Supreme Court grappled with the highly regulated industries exception most recently in *City of Los Angeles v. Patel*.[478] That case involved a Fourth Amendment challenge by Los Angeles hotel operators to a "provision of the Los Angeles Municipal Code that require[d] hotel operators to make their registries available to the police on demand."[479] In its analysis, the *Patel* Court explained that "*the closely regulated industry . . . is the exception*"[480] and that "classif[ication of] hotels as pervasively regulated would permit what has always been a narrow exception to swallow the rule."[481] Ultimately, the Court held that the hotel business did not constitute a highly regulated industry.

---

471. Colonnade Catering Corp. v. United States, 397 U.S. 72, 77 (1970).

472. United States v. Biswell, 406 U.S. 311, 317 (1972).

473. Donovan v. Dewey, 452 U.S. 594, 606 (1981); *see also id.* at 602 (describing the mining industry as "among the most hazardous in the country").

474. New York v. Burger, 482 U.S. 691, 703–12 (1987); *see also id.* at 709 ("Automobile junkyards and vehicle dismantlers provide the major market for stolen vehicles and vehicle parts.").

475. Marshall v. Barlow's, Inc., 436 U.S. 307, 313 (1978).

476. Free Speech Coal., Inc. v. Attorney Gen., 677 F.3d 519, 544 (3d Cir. 2012) (citing *Donovan*, 452 U.S. 594, 605–06).

477. *Burger*, 482 U.S. at 702–03 (quoting *Donovan*, 452 U.S. at 600–03).

478. City of Los Angeles v. Patel, 135 S. Ct. 2443 (2015).

479. *Id.* at 2447.

480. *Id.* at 2455 (emphasis added) (quoting *Barlow's*, 436 U.S. at 313).

481. *Id.* at 2447.

However, the Court went on to explain that "[e]ven if we were to find that hotels are pervasively regulated,"[482] the Los Angeles Municipal Code's warrantless inspection regime was nonetheless constitutionally deficient because (1) it was unnecessary to further the regulatory scheme and (2) "it fail[ed] to sufficiently constrain police officers' discretion as to which hotels to search and under what circumstances" "under the 'certainty and regularity' prong of the closely regulated industries test."[483]

The Utah district court upheld the DEA's PDMP searches, in part, on the theory that "[p]rescription drugs are a highly regulated industry in which patients and doctors do not have a reasonable expectation of privacy."[484] The court's discussion of that exception, *in toto*, was as follows:

> Prescription drugs are a highly regulated industry in which patients and doctors do not have a reasonable expectation of privacy. The Sixth Circuit has held that the pharmaceutical industry, like the mining, firearms, and liquor industries, is a pervasively regulated industry and that consequently pharmacists and distributors subject to the [CSA] have a reduced expectation of privacy in the records kept in compliance with the [CSA]. As one federal district court explained, the CSA was intended as a comprehensive federal program to place certain drugs and other substances under strict federal controls. In other words, the expectation created by the CSA is that the prescription and use of controlled substances will happen under the watchful eye of the federal government.[485]

The district court's application and limited analysis of the highly regulated industries exception in the context of warrantless PDMP searches is problematic for at least two reasons. First, DEA warrantless PDMP searches do not conform to the minimum requirements of the highly regulated industry exception. The highly "regulated industry exception applies to searches of *commercial* premises for *civil* purposes."[486] The DEA did not issue subpoenas in the PDMP litigation that sought to conduct warrantless inspections of commercial premises for such purposes. Instead, it issued subpoenas that demanded sensitive

---

482. *Id.* at 2456.

483. *Id.*

484. U.S. Dep't of Justice v. Utah Dep't of Commerce, No. 2:16-cv-611, 2017 WL 3189868, at *8 (D. Utah July 27, 2017).

485. *Id.* (quotations omitted).

486. Note, *Rethinking Closely Regulated Industries*, 129 HARV. L. REV. 797, 797 (2016).

prescribing information contained in a *state agency's* electronic database in the course of *criminal* investigations.

No other federal court has applied the highly regulated industry exception to a law enforcement search of *information held by a state agency*—as opposed to an inspection of a commercial enterprise. The Utah district court ignored the fact that the DEA's subpoenas were directed at a government entity and, instead, focused its attention on the nature of the "pharmaceutical industry." Whether the court was correct that the "pharmaceutical industry" is highly regulated, however, is of no moment because the DEA did not serve the administrative subpoenas on any "pharmaceutical industry" entity—it directed its subpoenas to the state PDMP agency.

The Utah district court's analysis is even more curious given that the CSA *expressly prohibits* the DEA from "inspecting, copying, and verifying the correctness of records, reports or other documents required to be kept" by "controlled premises"—including factories, warehouses, *pharmacies*, and other commercial establishments[487]—*without an administrative inspection warrant*.[488] The DEA, therefore, is proscribed by its own enabling statute from conducting a warrantless inspection on a pharmaceutical industry entity.[489] Indeed, the lone case that the Utah district court relied on to support its highly regulated industries ruling—*United States v. Acklen*[490]—decided "whether evidence seized [from the defendant's pharmacy] pursuant to an *administrative inspection warrant* . . . should be suppressed in a criminal trial for violations of the Controlled Substances Act if the primary purpose of the administrative inspection search was to obtain evidence for criminal prosecution."[491] Because *Acklen* involved the DEA's search of a *pharmacy*, which the CSA only permits pursuant to a court-ordered administrative-inspection warrant, it cannot support the DEA's issuance or enforcement of an administrative subpoena directed at a state PDMP agency.

Second, the Utah district court was required to assess whether the DEA's warrantless search of PDMP prescribing information was

487. 21 U.S.C. § 880(a)–(b) (2018).

488. *Id.* § 880(b)(1)–(2).

489. *Id.*; *see also id.* § 880(c) (listing the situations where the DEA is permitted to inspect books and records pursuant to an administrative subpoena, including when the owner consents or when exigent circumstances exist).

490. United States v. Acklen, 690 F.2d 70 (6th Cir. 1982).

491. *Id.* at 72 (emphasis added).

reasonable.[492] Nowhere in its decision does the court reach even a conclusory determination with regard to any of the three criteria enumerated above applicable to the constitutional reasonableness analysis. As already noted, the Utah district court's application of the highly regulated industries exception to enforce the DEA's administrative subpoenas of state PDMP databases was anomalous and likely unwarranted. If pertinent precedent is any guide, Fourth Amendment challenges to such subpoenas are likely to rise or fall on the merits of the two warrant exceptions directly addressed in *Carpenter*: the administrative-subpoena exception and the third-party doctrine.

CONCLUSION

The diversion and problematic use of prescription drugs in the United States provoked a public-health crisis and, predictably, a predominantly supply-side, law-enforcement-centric response, including the ubiquitous creation of state PDMPs. These programs collect, store, and analyze reams of highly sensitive, personal, and sometimes stigmatizing patient prescribing data. The DEA's unchecked, sweeping, and virtually instantaneous access to PDMP prescribing information—which include, among other things, diagnosis-identifying information—raises material Fourth Amendment concerns. In the apt words of one public-health scholar, "[g]overnment surveillance systems, including various electronic databases like PDMPs . . . have a sinister side."[493]

Fortunately, this "sinister" and sweeping surveillance is foreclosed both by pre-*Carpenter* precedent and *Carpenter* itself. The latter, in particular, practically demands that courts put a stop to the DEA's widespread practice of conducting dragnet-style searches of state PDMP prescribing data without judicial oversight and probable cause. Ultimately, before the government can compel the disclosure of patient prescribing information, it must abide by a "familiar" admonition—"get a warrant."[494]

492. New York v. Burger, 482 U.S. 691, 702–03 (1987).

493. Beletsky, *supra* note 52, at 142.

494. Carpenter v. United States, 138 S. Ct. 2211, 2223 (2018).