of GED and paralegal courses, and his family situation. His attorney argued that his pre-existing medical conditions, which include diabetes, hypertension and gout, increases his risk of having a very serious illness if he contracted Covid 19. He has a viable home plan.

The concerns expressed by Littrell's counsel about the risk of contracting Covid 19 in prison were well founded, as he now has tested positive for the disease. Although I have not received any information about the seriousness of his condition or his current medical treatment, I believe that keeping him in the Bureau of Prisons at this time is not warranted. The facility in which he is confined, FCI Forrest City Low, has one of the highest incidences of Covid 19 cases in any of the Bureau of Prisons facilities.[10]

The extraordinary and compelling circumstances resulting from the change in sentencing law, together with Littrell's lack of prior serious criminal history and his stable home plan, would justify my reducing his sentence to 240 months even if he had not contracted Covid 19. But because that sentence would require him to serve a few more months in jail and because he has now been diagnosed with Covid 19, I agree that a reduction of sentence to time served is appropriate. The Bureau of Prisons may delay implementation of this sentence for not more than fourteen days from today, but only if necessary to arrange for appropriate medical treatment or quarantine.

Accordingly,

IT IS HEREBY ORDERED that defendant's latest Motions to Reduce Sentence [87, 91, 102] are granted and defendant Anthony Littrell's sentence is reduced to time served. The Bureau of Prisons may delay implementation of this sentence for not more than fourteen days from today, but only if necessary to arrange for appropriate medical treatment or quarantine.

An amended judgment in accord with this Memorandum and Order is entered this same date.

10. *Federal Bureau of Prisons, Covid-19 Coronavirus,* https://www.bop.gov/coronavirus (last accessed May 19, 2020).

CDK GLOBAL LLC, et al., Plaintiffs,

v.

Mark BRNOVICH, et al., Defendants,

and

Arizona Automobile Dealers Association, Intervenor Defendant.

No. CV-19-04849-PHX-GMS

United States District Court, D. Arizona.

Signed 05/20/2020

Background: Dealer management system (DMS) providers brought action against state and trade organization representing automobile dealerships, seeking declaratory and injunctive relief from Dealer Data Security Law, which allegedly was preempted by federal law and violated the Takings Clause, Contracts Clause, Due Process Clause, Commerce Clause, and First Amendment. Defendants moved to dismiss.

Holdings: The District Court, G. Murray Snow, Chief Judge, held that:

(1) Dealer Law was not preempted by the Computer Fraud and Abuse Act (CFAA);

(2) Copyright Act did not preempt the Dealer Law;

(3) Dealer Law was not void for vagueness under the Due Process Clause;

(4) plaintiffs sufficiently alleged that Dealer Law constituted a taking under the Fifth Amendment;

(5) plaintiffs sufficiently alleged that Dealer Law violated the Contracts Clause of the Constitution;

(6) Dealer Law did not violate dormant Commerce Clause; and

(7) Dealer Law did not abridge plaintiffs' freedom of speech.

Motion granted in part and denied in part.

1. Constitutional Law ⚿656, 969, 975

Facial challenges to constitutionality of law are disfavored for several reasons, including that such challenges often rest on speculation, and that they also run contrary to fundamental principle of judicial restraint, under which courts should neither anticipate question of constitutional law in advance of necessity of deciding it nor formulate rule of constitutional law broader than is required by precise facts to which it is to be applied.

2. Constitutional Law ⚿978

Action brought by dealer management system (DMS) providers, asserting facial constitutional challenge prior to enforcement of Arizona's Dealer Data Security Law that made it illegal for DMS providers to prevent third party authorized by an automotive dealer from accessing dealer's DMS, was ripe for judicial review; providers plausibly pled that the Dealer Law criminalized their current and longstanding practices, fear of criminal prosecution was not imaginary or wholly speculative, since state had not disavowed any intention of invoking criminal penalty provision against them, and positions of providers and state were sufficiently adverse with respect to the Dealer Law to present a case or controversy. U.S. Const. art. 3, § 2, cl. 1; Ariz. Rev. Stat. Ann. § 28-4651 et seq.

3. Federal Courts ⚿2103

Three factors courts consider when analyzing genuineness of a threat of prosecution, for purposes of determining whether requisite "case or controversy" exists for federal jurisdiction, include: (1) whether the plaintiffs have articulated a concrete plan to violate the law in question, (2) whether the prosecuting authorities have communicated a specific warning or threat to initiate proceedings, and (3) the history of past prosecution or enforcement under the challenged statute. U.S. Const. art. 3, § 2, cl. 1.

4. States ⚿18.5

On a facial preemption challenge, a plaintiff must show that no set of circumstances exists under which the law would be valid; however, the proper inquiry is not simply whether state and local law enforcement officials can apply the statute in a constitutional way, because there can be no constitutional application of a statute that, on its face, conflicts with Congressional intent and therefore is preempted by the Supremacy Clause. U.S. Const. art. 6, cl. 2.

5. States ⚿18.13

In preemption analysis, courts should assume that the historic police powers of the states are not superseded unless that was the clear and manifest purpose of Congress.

6. Telecommunications ⚿1342

Computer Fraud and Abuse Act (CFAA) was enacted to prevent hackers from stealing information or disrupting or destroying computer functionality and to

penalize thefts of property via computer that occur as part of a scheme to defraud. 18 U.S.C.A. § 1030 et seq.

7. Telecommunications ⚿1342, 1348

Computer Fraud and Abuse Act (CFAA) imposes criminal and civil liability on anyone who intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information. 18 U.S.C.A. § 1030 et seq.

8. Antitrust and Trade Regulation ⚿269(3)

States ⚿18.84

Given the stated purpose of the Computer Fraud and Abuse Act (CFAA), Arizona's Dealer Data Security Law did not pose an obstacle to CFAA, and thus, Dealer Law was not preempted by CFAA; Dealer Law required dealer management system (DMS) providers to allow access to their systems by any user authorized by automotive dealership holding license to the DMS, while CFAA had narrow aim of deterring and punishing certain high-tech crimes and targeting hackers who accessed computers to steal information or to disrupt or destroy computer functionality. 18 U.S.C.A. § 1030 et seq.; Ariz. Rev. Stat. Ann. § 28-4651 et seq.

9. Copyrights and Intellectual Property ⚿75.5

Although an author gains exclusive rights in her work immediately upon the work's creation, a civil action for copyright infringement cannot be instituted until the copyright has been duly registered. 17 U.S.C.A. § 411(a).

10. Copyrights and Intellectual Property ⚿75.5

Upon registration of the copyright, a copyright owner can recover for infringement that occurred both before and after registration. 17 U.S.C.A. § 411(a).

11. Copyrights and Intellectual Property ⚿109

States ⚿18.87

Copyright Act did not preempt Arizona's Dealer Data Security Law, which required dealer management system (DMS) providers to allow third parties with no license agreement to access and use copyrighted DMS software; Dealer Law could be applied in constitutional way in cases where DMS providers had not yet obtained copyright registration or where it would be possible for third parties to access DMSs without copying providers' proprietary software, and where copyright registration has been obtained, third parties' copying of providers' software would not be necessary to obtain dealer data and thus would presumably not qualify as "fair use" under the Copyright Act. 17 U.S.C.A. §§ 106(1), 107; Ariz. Rev. Stat. Ann. § 28-4653.

12. Copyrights and Intellectual Property ⚿109

States ⚿18.87

Arizona's Dealer Data Security Law, which required dealer management system (DMS) providers to allow access to their systems by any user authorized by automotive dealership, was not preempted by the Digital Millennium Copyright Act (DMCA), since DMCA was concerned with preventing unauthorized access to copyrighted works by pirates who aimed to destroy the value of American intellectual property, not defining what access was legally authorized in the first place. 17 U.S.C.A. §§ 1201(a)(1)(A), 1203, 1204; Ariz. Rev. Stat. Ann. § 28-4651 et seq.

13. Antitrust and Trade Regulation ⚿269(3)

States ⚿18.84

Arizona's Dealer Data Security Law, which required dealer management system (DMS) providers to allow access to their

systems by any user authorized by automotive dealership, was not preempted by the Defend Trade Secrets Act (DTSA), since nothing in the DTSA or its legislative history indicated that Congress intended the statute to prevent states from authorizing lawful transfers of otherwise protected information. 18 U.S.C.A. § 1831 et seq.; Ariz. Rev. Stat. Ann. § 28-4651 et seq.

14. Antitrust and Trade Regulation ⚿269(3)

States ⚿18.84

Gramm-Leach-Bliley Act (GLBA) did not preempt Arizona's Dealer Data Security Law, which required dealer management system (DMS) providers to allow access to their systems by any user authorized by automotive dealership; Dealer Law provided several provisions designed to ensure compliance with GLBA requirements, including that protected dealer data only be used subject to a dealer's express written consent, and providers were not precluded from discharging any federal legal duties to protect and secure protected dealer data. 15 U.S.C.A. § 6801(a); Ariz. Rev. Stat. Ann. § 28-4651 et seq.

15. Constitutional Law ⚿3905

It is a basic principle of due process that an enactment is void for vagueness if its prohibitions are not clearly defined. U.S. Const. Amend. 14.

16. Constitutional Law ⚿3905, 4506

While statutes must give the person of ordinary intelligence a reasonable opportunity to know what is prohibited and provide explicit standards for those who apply them, uncertainty does not mean that a statute is vague in violation of due process; as long as uncertain standards are applied to real-world facts engaged in on a particular occasion rather than to an idealized crime, the statutes are almost certainly constitutional. U.S. Const. Amend. 14.

17. Antitrust and Trade Regulation ⚿269(3)

Constitutional Law ⚿4267

Copyrights and Intellectual Property ⚿2

Arizona's Dealer Data Security Law, which made it illegal for dealer management system (DMS) providers to prevent third party authorized by an automotive dealer from accessing dealer's DMS, was not void for vagueness under the Due Process Clause, since the Dealer Law gave the person of ordinary intelligence a reasonable opportunity to know what was prohibited and did not require courts to apply the Dealer Law to an idealized crime but rather to real-world facts engaged in on a particular occasion. U.S. Const. Amend. 14; Ariz. Rev. Stat. Ann. § 28-4651 et seq.

18. Constitutional Law ⚿3905

Speculation about possible vagueness in hypothetical situations not before the court will not support a facial attack on a statute on vagueness grounds under the Due Process Clause when it is surely valid in the vast majority of its intended applications. U.S. Const. Amend. 14.

19. Eminent Domain ⚿2.1

Inquiry into what constitutes a "taking" for purposes of the Fifth Amendment is essentially ad hoc and factual. U.S. Const. Amend. 5.

20. Eminent Domain ⚿2.1

Paradigmatic Fifth Amendment taking requiring just compensation is a direct government appropriation or physical invasion of private property; however, mere regulation of private property may also be so onerous that its effect is tantamount to a direct appropriation or ouster. U.S. Const. Amend. 5.

21. Eminent Domain ⚿2.1, 69

Under the Fifth Amendment's Takings Clause, the government must pay for

regulations that completely deprive an owner of all economically beneficial use of her property. U.S. Const. Amend. 5.

22. Eminent Domain ⚿2.1

Regulatory takings challenges are governed by several factors that have particular significance, including the economic impact of the regulation on the plaintiff, the extent to which the regulation has interfered with investment-backed expectations, and the character of the governmental action. U.S. Const. Amend. 5.

23. Eminent Domain ⚿2.34

Dealer management system (DMS) providers sufficiently alleged that Arizona's Dealer Data Security Law, which required them to allow third parties with no license agreement to access and use copyrighted DMS software if authorized to do so by an automotive dealership, constituted a taking under the Fifth Amendment; providers alleged that permitting third parties to use their proprietary systems without their permission constituted an interference with their property, amounting to a physical invasion by government, and they argued that Dealer Law would have significant economic impact on them and substantially interfere with their reasonable investment-backed expectations because they had invested heavily to maintain and enhance their proprietary systems and charged fees to authorized users to recoup the investment. U.S. Const. Amend. 5.

24. Constitutional Law ⚿2671

The threshold issue in determining if state law violates the Contracts Clause is whether the state law has operated as a substantial impairment of a contractual relationship. U.S. Const. art. 1, § 10, cl. 1.

25. Constitutional Law ⚿2671

Total destruction of contractual expectations is not necessary for a finding of substantial impairment, for purposes of the Contracts Clause. U.S. Const. art. 1, § 10, cl. 1.

26. Antitrust and Trade Regulation ⚿269(3)

Constitutional Law ⚿2757

Copyrights and Intellectual Property ⚿2

Dealer management system (DMS) providers sufficiently alleged that Arizona's Dealer Data Security Law, which required them to allow third parties with no license agreement to access and use copyrighted DMS software if authorized to do so by an automotive dealership, violated the Contracts Clause of the Constitution; providers alleged that enforcement of Dealer Law would substantially impair their contracts, and that Dealer Law was not appropriate and reasonable means of serving any legitimate interest because, for instance, it placed consumer data at risk to provide economic benefit to car dealers. U.S. Const. art. 1, § 10, cl. 1; Ariz. Rev. Stat. Ann. § 28-4651 et seq.

27. Commerce ⚿12

Statute violates the so-called Dormant Commerce Clause if it directly regulates or discriminates against interstate commerce, or, if a statute has only indirect effects on interstate commerce and is nondiscriminatory, if the burdens of the statute so outweigh the putative benefits as to make the statute unreasonable or irrational. U.S. Const. art. 1, § 8, cl. 3.

28. Commerce ⚿12, 54.1

In evaluating dormant Commerce Clause challenges, courts may not assess state law's benefits or wisdom in adopting it unless law either discriminates in favor of in-state commerce or imposes significant burden on interstate commerce. U.S. Const. art. 1, § 8, cl. 3.

29. Commerce ⚿62.12

Copyrights and Intellectual Property ⚿2

Arizona's Dealer Data Security Law, which required dealer management system (DMS) providers to allow third parties with no license agreement to access and use copyrighted DMS software if authorized to do so by an automotive dealership, did not violate the dormant Commerce Clause, where there was no plausible allegation that Dealer Law was discriminatory in favor of Arizona commerce or that it regulated activities that were inherently national. U.S. Const. art. 1, § 8, cl. 3; Ariz. Rev. Stat. Ann. § 28-4651 et seq.

30. Constitutional Law ⚿2147

Whether computer code rises to the level of speech under the First Amendment depends on whether a programmer might be said to communicate through code to the user of the program, which is not necessarily protected, or only to the computer, which is never protected; even when software communicates to a user, where it is mechanical and does not involve second-guessing or intercession of the mind or the will of the recipient, such code is devoid of any constitutionally protected speech. U.S. Const. Amend. 1.

31. Antitrust and Trade Regulation ⚿269(3)

Constitutional Law ⚿2147

Copyrights and Intellectual Property ⚿2

Arizona's Dealer Data Security Law, which required dealer management system (DMS) providers to allow third parties with no license agreement to access and use copyrighted DMS software if authorized to do so by an automotive dealership, did not abridge providers' freedom of speech in violation of the First Amendment; purpose of Dealer Law was to facilitate sharing of otherwise unprotected underlying information in the DMS, and to extent that providers complied with the Dealer Law by creating code, that code only told a computer how to function and had no other expressive purpose. U.S. Const. Amend. 1; Ariz. Rev. Stat. Ann. § 28-4651 et seq.

Andrew Tauber, Mark William Ryan, Pro Hac Vice, Mayer Brown LLP, Washington, DC, Brett E. Legner, Pro Hac Vice, Britt M. Miller, Pro Hac Vice, Daniel T. Fenske, Pro Hac Vice, Michael Anthony Scodro, Pro Hac Vice, Mayer Brown LLP, Chicago, IL, Brian Alexander Howie, Lauren Elliott Stine, Quarles & Brady LLP, Phoenix, AZ, for Plaintiff CDK Global LLC.

Amar Shrinivas Naik, Pro Hac Vice, Molly C. Lorenzi, Pro Hac Vice, Sheppard Mullin Richter & Hampton LLC, San Francisco, CA, Aundrea K. Gulley, Pro Hac Vice, Brice A. Wilkinson, Pro Hac Vice, Denise L. Drake, Pro Hac Vice, Gibbs & Bruns LLP, Houston, TX, Brian Alexander Howie, Lauren Elliott Stine, Quarles & Brady LLP, Phoenix, AZ, Jonathan Richard DeFosse, Pro Hac Vice, Thomas J. Dillickrath, Pro Hac Vice, Sheppard Mullin Richter & Hampton LLP, Mark William Ryan, Pro Hac Vice, Mayer Brown LLP, Washington, DC, for Plaintiff Reynolds and Reynolds Company.

Brunn Wall Roysden, III, Rusty Duane Crandell, Office of the Attorney General, William DeWitt Furnish, Mary Ruth OGrady, Osborn Maledon PA, Phoenix, AZ, for Defendant Mark Brnovich.

Bethan R. Jones, Pro Hac Vice, Brendan J. Crimmins, Pro Hac Vice, Christine Bonomo, Pro Hac Vice, Collin R. White, Pro Hac Vice, Daniel V. Dorris, Pro Hac Vice, David L. Schwarz, Pro Hac Vice, Derek T. Ho, Pro Hac Vice, Jayme Louise Weber, Joshua Hafenbrack, Pro Hac Vice, Michael

N. Nemelka, Pro Hac Vice, Kellogg Hansen Todd Figel & Frederick PLLC, Washington, DC, Jeffrey Dale Gardner, Jimmie W. Pursell, Jr., John C. Norling, Jennings Strouss & Salmon PLC, Phoenix, AZ, for Intervenor Defendant.

ORDER

G. Murray Snow, Chief United States District Judge

Pending before the Court are Defendant Arizona Automobile Dealers Association ("AADA")'s Motion to Dismiss for Failure to State a Claim (Doc. 39) and Defendants Mark Brnovich and John S. Halikowski's [1] Joint Motion to Dismiss for Failure to State a Claim (Doc. 40). The Motions are granted in part and denied in part.

BACKGROUND

Plaintiffs CDK Global LLC and Reynolds and Reynolds Company (collectively, "Plaintiffs") develop, own, and operate proprietary computer systems known as dealer management systems ("DMSs") that process vast amounts of data [2] sourced from various parties. Automotive dealerships hold licenses to DMSs to help manage their business operations, including handling confidential consumer and proprietary data, processing transactions, and managing data communications between dealers, customers, car manufacturers, credit bureaus, and other third parties. Plaintiffs employ multiple technological measures—such as secure login credentials, CAPTCHA prompts, and comprehensive cybersecurity infrastructure, hardware, and software—to safeguard their DMS systems from unauthorized access or breach. Plaintiffs also contractually prohibit dealers from granting third parties access to their DMSs without Plaintiffs' authorization.

In March 2019, the Arizona Legislature passed the Dealer Data Security Law ("the Dealer Law"), A.R.S. §§ 28-4651–28-4655. The Dealer Law went into effect on August 27, 2019.[3] The Dealer Law regulates the relationship between DMS licensers like Plaintiffs and the dealerships they serve. Under the Dealer Law, DMS providers may no longer "[p]rohibit[ ] a third party [that has been authorized by the Dealer and] that has satisfied or is compliant with ... current, applicable security standards published by the standards for technology in automotive retail [(STAR standards)] ... from integrating into the dealer's [DMS] or plac[e] an unreasonable restriction on integration ...." A.R.S. §§ 28-4653(A)(3)(b), 28-4651(9). The Dealer Law also requires that DMS providers "[a]dopt and make available a standardized framework for the exchange, integration and sharing of data from [a DMS]" that is compatible with STAR standards and that they "[p]rovide access to open application

1. While Docs. 39 and 40 were pending, Defendant Halikowski's Motion to Dismiss for Lack of Jurisdiction (Doc. 38) was granted. He is therefore no longer a party to this case.

2. "Such data belongs to several types of entities. Some data, such as prices and part numbers for replacement parts, labor rates, and rebate, incentive, and warranty information, is proprietary to OEMs [Original Equipment Manufacturers] such as General Motors, Ford, and Subaru. Other data in or processed by [Plaintiffs'] DMS[s] is proprietary to third-party service providers, such as credit reporting bureaus like Equifax, Experian and TransUnion. Still other data in the DMS[s] is [Plaintiffs'] own proprietary, copyrightable data, including forms, accounting rules, tax tables, service pricing guides, and proprietary tools and data compilations. And while some data 'belongs' to the dealers, in the sense that dealers enter the data into the system, that use [Plaintiffs'] DMS[s], much of that is consumer data." (Doc. 1 at 11.)

3. However, Defendants stipulated on September 4, 2019 that they would "take no action to enforce Arizona House Bill 2418 (2019) for the pendency of Plaintiffs' Motion for Preliminary Injunction in this Court." (Doc. 28 at 2.)

programming interfaces to authorized integrators." A.R.S. § 28-4654(A). Finally, a DMS provider may only use data to the extent permitted in the DMS provider's agreement with the dealer, must permit dealer termination of such agreement, and "must work to ensure a secure transition of all protected dealer data to a successor dealer data vendor or authorized integrator" upon termination. A.R.S. §§ 28-4654(B)(1)-(3).

Plaintiffs filed the underlying complaint seeking declaratory and injunctive relief from the Dealer Law on July 29, 2019. These Motions to Dismiss followed on September 18, 2019.

DISCUSSION

I. Legal Standard

To survive a motion to dismiss for failure to state a claim pursuant to Federal Rule of Civil Procedure 12(b)(6), a complaint must contain more than a "formulaic recitation of the elements of a cause of action"; it must contain factual allegations sufficient to "raise the right of relief above the speculative level." *Bell Atl. Corp. v. Twombly,* 550 U.S. 544, 555, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007) (quoting *Conley v. Gibson*, 355 U.S. 41, 47, 78 S.Ct. 99, 2 L.Ed.2d 80 (1957)). While "a complaint need not contain detailed factual allegations ... it must plead 'enough facts to state a claim to relief that is plausible on its face.'" *Clemens v. DaimlerChrysler Corp.*, 534 F.3d 1017, 1022 (9th Cir. 2008) (quoting *Twombly*, 550 U.S. at 570, 127 S.Ct. 1955). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009) (citing *Twombly*, 550 U.S. at 556, 127 S.Ct. 1955). When analyzing a complaint for failure to state a claim, "allegations of material fact are taken as true and construed in the light most favorable to the non-moving party." *Smith v. Jackson*, 84 F.3d 1213, 1217 (9th Cir. 1996). In addition, the Court must assume that all general allegations "embrace whatever specific facts might be necessary to support them." *Peloza v. Capistrano Unified Sch. Dist.*, 37 F.3d 517, 521 (9th Cir. 1994). However, legal conclusions couched as factual allegations are not given a presumption of truthfulness, and "conclusory allegations of law and unwarranted inferences are not sufficient to defeat a motion to dismiss." *Pareto v. F.D.I.C.*, 139 F.3d 696, 699 (9th Cir. 1998).

II. Analysis

[1] Plaintiffs' claims concern five federal statutes and five provisions of the United States Constitution. Plaintiffs "object to [the Dealer Law] not in the context of an actual [prosecution], but in a facial challenge" prior to enforcement such that the State of Arizona "has had no opportunity to implement [the Dealer Law], and its courts have had no occasion to construe the law in the context of actual disputes ... or to accord the law a limiting construction to avoid constitutional questions." *Washington State Grange v. Washington State Republican Party*, 552 U.S. 442, 449–50, 128 S.Ct. 1184, 170 L.Ed.2d 151 (2008). "Facial challenges are disfavored for several reasons":

> Claims of facial invalidity often rest on speculation. As a consequence, they raise the risk of "premature interpretation of statutes on the basis of factually barebones records." *Sabri v. United States*, 541 U.S. 600, 609 [124 S.Ct. 1941, 158 L.Ed.2d 891] ...(2004) (internal quotation marks and brackets omitted). Facial challenges also run contrary to the fundamental principle of judicial restraint that courts should neither "anticipate a question of constitutional law in advance of the necessity of deciding it"

> nor "formulate a rule of constitutional law broader than is required by the precise facts to which it is to be applied." *Ashwander v. TVA*, 297 U.S. 288, 346–347 [56 S.Ct. 466, 80 L.Ed. 688] . . . (1936) (Brandeis, J., concurring) . . . . Finally, facial challenges threaten to short circuit the democratic process by preventing laws embodying the will of the people from being implemented in a manner consistent with the Constitution.

Id. at 450–51, 128 S.Ct. 1184.

A. Ripeness

[2, 3] To obtain relief, Plaintiffs must show "a genuine threat of imminent prosecution under the challenged statute to establish a justiciable case or controversy." (Doc. 40 at 6) (quoting *Wash. Mercantile Ass'n v. Williams*, 733 F.2d 687, 688 (9th Cir. 1984)). The three factors courts consider when analyzing the genuineness of a threat of prosecution include: (1) "whether the plaintiffs have articulated a concrete plan to violate the law in question," (2) "whether the prosecuting authorities have communicated a specific warning or threat to initiate proceedings," and (3) "the history of past prosecution or enforcement under the challenged statute." *Stormans, Inc. v. Selecky*, 586 F.3d 1109, 1122 (9th Cir. 2009). Although Defendants have not communicated a specific warning or threat against Plaintiffs, Plaintiffs have plausibly pled that the Dealer Law criminalizes their current and longstanding practices. And when fear of criminal prosecution under an allegedly unconstitutional statute is "not imaginary or wholly speculative," a plaintiff need not "first expose himself to actual arrest or prosecution to be entitled to challenge the statute." *Babbitt v. United Farm Workers Nat. Union*, 442 U.S. 289, 302, 99 S.Ct. 2301, 60 L.Ed.2d 895 (1979). Here, as in *Babbitt*, "the State has not disavowed any intention of invoking the criminal penalty provision" against Plaintiffs, and "the positions of the parties are sufficiently adverse with respect to [the Dealer Law] . . . to present a case or controversy within the jurisdiction of the District Court." *Id.* Plaintiffs' claims present a ripe controversy.

B. Federal Preemption

Plaintiffs argue that the Dealer Law is preempted by the Computer Fraud and Abuse Act (CFAA), the Copyright Act, the Digital Millennium Copyright Act (DMCA), the Defend Trade Secrets Act (DTSA), and the Gramm-Leach-Bliley Act (GLBA) because the Dealer Law "conflicts with, or poses an obstacle to, the purposes sought to be achieved" by these statutes. (Doc. 1 at 44.) Broadly, Plaintiffs assert that the Dealer Law conflicts with these statutes because "DMSs house both 'protected dealer data' as defined by the DMS Law and other proprietary data, including Plaintiffs' intellectual property," and the Dealer Law's ban on Plaintiffs "tak[ing] any action by contract, technical means or otherwise to prohibit or limit a dealer's ability to protect, store, copy, share or use protected dealer data" effectively "grants third parties access to that other proprietary data as well." (Doc. 1 at 31.)

[4, 5] On a facial preemption challenge, a plaintiff must show that "no set of circumstances exists under which the Act would be valid." *United States v. Salerno*, 481 U.S. 739, 746, 107 S.Ct. 2095, 95 L.Ed.2d 697 (1987).[4] However, the proper inquiry is not simply "whether state and local law enforcement officials can apply the statute in a constitutional way," because "there can be no constitutional application of a statute that, on its face,

4. *"Salerno's* applicability in preemption cases is not entirely clear, however . . . . [w]ithout more direction, we have chosen to continue applying *Salerno*." *Puente Arizona v. Arpaio*, 821 F.3d 1098, 1104 (9th Cir. 2016).

conflicts with Congressional intent and therefore is preempted by the Supremacy Clause." *United States v. Arizona*, 641 F.3d 339, 345–46 (9th Cir. 2011), *aff'd in part, rev'd in part and remanded*, 567 U.S. 387, 132 S.Ct. 2492, 183 L.Ed.2d 351 (2012). Nevertheless, "courts should assume that 'the historic police powers of the States' are not superseded 'unless that was the clear and manifest purpose of Congress.' " *Arizona*, 567 U.S. at 400, 132 S.Ct. 2492 (quoting *Rice v. Santa Fe Elevator Corp.*, 331 U.S. 218, 230, 67 S.Ct. 1146, 91 L.Ed. 1447 (1947)). And, as this preemption challenge has been brought prior to enforcement and thus "without the benefit of a definitive interpretation [of the Dealer Law] from the state courts," the timing of this case "counsel[s] caution in evaluating [the Dealer Law's] validity" because "it would be inappropriate to assume [the Dealer Law] will be construed in a way that creates a conflict with federal law." *Arizona*, 567 U.S. at 415, 132 S.Ct. 2492.

1. CFAA

[6, 7] The CFAA was enacted to prevent "hackers" from "steal[ing] information or ... disrupt[ing] or destroy[ing] computer functionality" and "to penalize thefts of property via computer that occur as part of a scheme to defraud." *United States v. Nosal*, 844 F.3d 1024, 1032 (9th Cir. 2016). "The conduct prohibited [by the CFAA] is analogous to that of 'breaking and entering,' " H.R. Rep. No. 98-894, at 20 (1984), a comparison invoked "so frequently during congressional consideration" that the Ninth Circuit found the CFAA inapposite where the breaking and entering analogy "ha[d] no application," *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1001 (9th Cir. 2019). To those ends, the CFAA imposes criminal and civil liability on anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information ...." *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1065–66 (9th Cir. 2016). However, while the CFAA criminalizes accessing information without authorization in protected computers, it does not limit how access might be authorized. Rather, it leaves it to authority external to the statute itself—such as state law—to determine what is authorized or not.

Plaintiffs contend that the Dealer Law is preempted by the CFAA because the Dealer Law poses "an obstacle to" Congress' purpose in enacting the CFAA "by requiring CDK and Reynolds to allow access to their systems by any user authorized by a dealer." (Doc. 1 at 50, 51.) But Plaintiffs' suggested interpretation ignores the authorization provided by state law and would expand the CFAA beyond its "narrow" aim, *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008), of "deter[ing] and punish[ing] certain 'high-tech' crimes" and targeting "hackers who accessed computers to steal information or to disrupt or destroy computer functionality," *Nosal*, 844 F.3d at 1032. "The CFAA must be interpreted in its historical context, mindful of Congress' purpose in enacting it." *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1109 (N.D. Cal. 2017), *aff'd and remanded*, 938 F.3d 985 (9th Cir. 2019). A broad reading of the CFAA "could stifle the dynamic evolution and incremental development of state and local laws addressing the delicate balance between open access to information and privacy," a "profound consequence[ ] ... Congress could not have intended ... when it enacted the CFAA in 1984 ... before the advent of the World Wide Web." *Id.*

[8] Plaintiffs have cited no authority to the contrary. The cases in Plaintiffs' Response in Opposition involve users attempting to access information from opera-

tors' sites after those users have been denied, or never received, access. They certainly do not involve cases in which state law explicitly authorized access. *See, e.g.*, *Nosal*, 844 F.3d at 1031 (employees acted "without authorization" when they downloaded information and source lists from their company's confidential internal database to launch a competitor firm). Further, to hold, as Plaintiffs request, that the CFAA preempts any state law that allows others to access their own information held in Plaintiffs' computer system cuts too broadly. Indeed, Plaintiffs have cited no evidence that the CFAA has preempted any state statute in its 35-year history. Given the stated purpose of the CFAA, the Dealer Law does not "pose an obstacle to" the CFAA. This claim is accordingly dismissed.[5]

2. The Copyright Act

[9, 10] Under the Copyright Act, copyright protection, including the "exclusive right[ ]" to "reproduce," "distribute copies" of, and "prepare derivative works based upon" the owner's "copyrighted work," 17 U.S.C. § 106(1)–(3), attaches to "original works of authorship fixed in any tangible medium of expression," 17 U.S.C. § 102(a). Although an author gains "exclusive rights" in her work immediately upon the work's creation, a civil action for copyright infringement cannot be instituted until the copyright has been duly registered. *Fourth Estate Pub. Benefit Corp. v. Wall-Street.com, LLC*, —— U.S. ——, 139 S. Ct. 881, 887, 203 L.Ed.2d 147 (2019). However, "[u]pon registration of the copyright . . . a copyright owner can recover for infringement that occurred both before and after registration." *Id.* at 886–87. Here, CDK has not asserted that its material is copyrighted, merely "copyrightable." Nor have Plaintiffs collectively made any assertions as to the copyright registrations of other DMS providers. However, Reynolds has asserted that its "software program that runs on dealer computers," including "its source and object code; distinctive screen layouts; graphical content; text; arrangement, organization, and display of information; and dynamic user experience," is an "original copyrighted work." (Doc. 1 at 13.)

Under the Dealer Law, DMS providers like Plaintiffs may not prohibit other parties that have "satisfied or [are] compliant with the star standards or other generally accepted standards that are at least as comprehensive as the star standards and that the dealer has identified as one of its authorized integrators from integrating into the dealer's dealer data system." Ariz. Rev. Stat. Ann. § 28-4653. At oral argument, Defendants asserted that the Dealer Law "does not say that the DMS companies must tolerate the ways in which data access are currently done," but rather that it simply requires Plaintiffs and other DMS providers to "provide a way for third parties to extract the data at the dealers' behest . . . in a way that is consistent with plaintiffs' Copyright Act rights." Transcript of Oral Argument at 34. Defendants further argue that "there is no allegation in the complaint that that is not possible." *Id.* But Plaintiffs argue that the Dealer Law conflicts with the Copyright Act because "requiring [DMS providers] to allow

5. Regarding the CFAA and at various other points in their Motion to Dismiss, Defendants argue that Plaintiffs can comply with the Dealer Law by creating an application programming interface (API) that would allow dealers to transfer their data to and from third-party partners without requiring integration into the DMS. Plaintiffs argue that Defendants are "wrong to say that use of an API involves 'no third-party access to the DMS.' " (Doc. 50 at 10.) As such, this is a disputed factual question inappropriate for resolution through a motion to dismiss. The Court will therefore not address this argument in this order.

third parties with no license agreement ... to access and use ... copyrighted DMS software .... *necessarily* entails the display, distribution, and creation of copies and derivative works of ... copyrighted DMS software." (Doc. 1 at 47) (emphasis added). "[E]ach time a user runs the DMS software, that process creates a new fixed copy of the original computer program code in the computer's random access memory." *Id.* at 47–48. The Court therefore interprets Plaintiffs to be alleging exactly what Defendants have articulated—that it is not possible for Plaintiffs to both comply with the Dealer Law and retain their rights under the Copyright Act. Construing the facts in Plaintiffs' favor, the Dealer Law "conflicts with Congressional intent ... on its face," regardless of Defendants' assertion that "the statute [can be applied] in a constitutional way," *United States v. Arizona*, 641 F.3d 339, 345–46 (9th Cir. 2011), *aff'd in part, rev'd in part and remanded*, 567 U.S. 387, 132 S.Ct. 2492, 183 L.Ed.2d 351 (2012), in cases where DMS providers have not yet obtained copyright registration or where it would be possible for third parties to access DMSs without copying DMS providers' proprietary software.

Notwithstanding the provisions of the Copyright Act, "the fair use of a copyrighted work ... is not an infringement of copyright." 17 U.S.C. § 107. In determining whether a particular use is a "fair use," courts must consider:

> (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.

Id.

In *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 596 (9th Cir. 2000), the Ninth Circuit held that Connectix's intermediate copying of Sony's software to create software allowing Connectix customers to play Sony PlayStation games on their computers was a fair use. In analyzing the "nature of the copyrighted work," the court noted that Sony's software warranted a "lower degree of protection than more traditional literary works" because it "contain[ed] unprotected aspects that [could not] be examined without copying." *Id.* at 603. Thus, the court determined, in to order to constitute fair use, "Connectix's copying of [Sony's software] *must have been 'necessary.'*" *Id.* (emphasis added). Similarly, in *Assessment Technologies of Wisconsin, LLC v. WIREdata, Inc.*, 350 F.3d 640, 645 (7th Cir. 2003), the Seventh Circuit held that if the *only way* WIREdata, the entity seeking to extract data from the plaintiff's database, could obtain the public-domain data it sought would be by "copying [the plaintiff's] compilation and not just the compiled data ... because the data and the format in which they were organized could not be disentangled, [WIREdata] would be privileged to make such a copy."

[11] Here, Reynolds has alleged that, even if third parties do not have access to their DMS, "dealership customers can use dealer-driven data export tools to send their operational and inventory data to application providers or other third parties, as the dealer deems appropriate." (Doc. 1 at 29.) Thus, unlike in *Sony* and *WIREdata*, third parties' copying of Plaintiffs' software would presumably not be necessary to obtain dealer data and thus would presumably not qualify as "fair use." The Motion is accordingly denied as to the

Copyright Act claim at this stage of the litigation.

3. DMCA

The DMCA prohibits both the "circumvention" of "technological measure[s] that effectively control[ ] access to a [copyrighted] work" and the manufacture or sale of technologies and services that are "primarily designed or produced for the purpose of circumventing" such measures. 17 U.S.C. §§ 1201(a)(1)(A), (a)(2)(A). Circumvention in this context "means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure." 17 U.S.C. § 1201(a)(3)(A). The DMCA imposes criminal sanctions and gives copyright owners a private right of action against those who unlawfully access their copyrighted works. *See* 17 U.S.C. §§ 1203, 1204.

[12] There is nothing about the Dealer Data Security Law on its face that violates the DMCA. Like the CFAA, the purpose of the DMCA is "to ensure the integrity of the electronic marketplace by preventing fraud and misinformation," *ITC Textile, Ltd. v. Wal-Mart Stores, Inc.*, No. 208CV07422FMCJCX, 2009 WL 10671458, at *5 (C.D. Cal. Mar. 31, 2009), and to provide copyright owners "reasonable assurance that they will be protected against massive piracy," S. Rep. No. 105–190, at 8 (May 11, 1998). And like the CFAA, the DMCA does not address the issue of state statutes requiring those who hold dealer protected data to provide access to it. The DMCA is concerned with preventing unauthorized access to copyrighted works by "pirates who aim to destroy the value of American intellectual property," H.R. Rep. No. 105–551, pt. 1, at 9–10 (May 22, 1998)—not defining what access is legally authorized in the first place. Presumably, were Plaintiffs able to show that dealers or authorized third parties were pirating or otherwise fraudulently using their copyrighted material, the DMCA might provide them with a private right of action against such persons. But this does not mean that the DMCA preempts the Dealer Law. Defendants' Motion is granted as to this claim.

4. DTSA

The DTSA prohibits "economic espionage" and "theft of trade secrets." 18 U.S.C. §§ 1831–1839. The statute imposes criminal and civil liability on individuals who access protected information "without authorization" or by "improper means," 18 U.S.C. §§ 1831–1832, exempting "reverse engineering, independent derivation, or any other lawful means of acquisition," 18 U.S.C. §§ 1839. In drafting the DTSA, "Congress borrowed heavily from . . . the states' trade secrets law . . . ." *Yeiser Research & Dev., LLC v. Teknor Apex Co.*, No. 17-CV-1290-BAS-MSB, 2019 WL 2177658, at *4 (S.D. Cal. May 20, 2019). Like the CFAA, the DTSA relies on other law to determine what "other lawful means of acquisition" might be. It thus does not preempt state laws that provide other lawful means of access.

[13] In a preemption analysis, "courts should assume that 'the historic police powers of the States' are not superseded 'unless that was the clear and manifest purpose of Congress.' " *Arizona*, 567 U.S. at 400, 132 S.Ct. 2492 (quoting *Rice*, 331 U.S. at 230, 67 S.Ct. 1146). As with the CFAA and the DMCA addressed above, Plaintiffs have cited nothing in the DTSA or its legislative history indicating that Congress intended this statute to prevent states from authorizing lawful transfers of otherwise protected information. Were the Dealer Law to be implemented, to the extent Plaintiffs could show that dealers or authorized third parties were exploiting access to protected dealer data as a means to steal Plaintiffs' trade secrets (a claim

Plaintiffs have not asserted here), they might have a cause of action under the DTSA. But this does not mean that the DTSA preempts the Dealer Law. Even construing the facts in the light most favorable to Plaintiffs, Plaintiffs' claim fails as a matter of law. The DTSA claim is accordingly dismissed.

5. GLBA

The GLBA imposes on "each financial institution" an "affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a). In connection with this requirement, the FTC promulgated a rule requiring financial institutions to "implement information safeguards to control" any "reasonably foreseeable ... risks to the security, confidentiality, and integrity of customer information." 16 C.F.R. § 314.4.5.

[14] The GLBA does not preempt the Dealer Law. Plaintiffs assert that the Dealer Law "prevents dealers from fulfilling their obligations under the GLBA by preventing Plaintiffs, the dealers' service providers, from adequately securing the data they store." (Doc. 50 at 25.) But this theory assumes that dealers are incapable of complying with their own GLBA obligations if they retain control of their data. Plaintiffs have not remotely plausibly alleged that this is the case; Plaintiffs have not cited any specific requirement under the GLBA with which dealers cannot comply. Moreover, the Dealer Law provides several provisions designed to ensure compliance with GLBA requirements, including that protected dealer data only be used subject to a dealer's express written consent, that third party integrators comply with the STAR standards or other generally accepted standards that are at least as comprehensive as the STAR standards, and that Plaintiffs are not precluded from "discharging" any federal legal duties "to protect and secure protected dealer data." A.R.S. § 28-4653. This claim is dismissed.

C. Constitutional Violations

Plaintiffs also bring five constitutional claims. Plaintiffs argue that the Dealer Law is void for vagueness under the Due Process Clause and that it violates the Takings Clause, the Contracts Clause, the Dormant Commerce Clause, and the First Amendment.

1. Vagueness

[15, 16] "It is a basic principle of due process that an enactment is void for vagueness if its prohibitions are not clearly defined." *Grayned v. City of Rockford*, 408 U.S. 104, 108, 92 S.Ct. 2294, 33 L.Ed.2d 222 (1972). At the same time, "we can never expect mathematical certainty from our language." *Id.* at 110, 92 S.Ct. 2294. Thus, while statutes must "give the person of ordinary intelligence a reasonable opportunity to know what is prohibited" and "provide explicit standards for those who apply them," *Grayned*, 408 U.S. at 108–09, 92 S.Ct. 2294; *see also Guerrero v. Whitaker*, 908 F.3d 541, 543 (9th Cir. 2018) (a criminal statute violates due process if it is "so vague that it fails to give ordinary people fair notice of the conduct it punishes, or so standardless that it invites arbitrary enforcement"), "uncertainty does not mean that a statute is unconstitutionally vague. Many statutes provide uncertain standards and, so long as those standards are applied to real-world facts ... engage[d in] on a particular occasion" rather than to an "idealized crime," "the statutes are almost certainly constitutional," *Guerrero*, 908 F.3d at 545.

Plaintiffs argue that the Dealer Law is vague because they cannot determine:

(a) Whether contractually agreed dealer access restrictions violate the law;

(b) Whether hosting encrypted data for a fee is prohibited cyber-ransom;

(c) Whether they are required to facilitate or prevent one dealer from accessing another dealer's data;

(d) Whether any or all of their dealer charges are prohibited fees;

(e) Which of their restrictions on access by authorized integrators are "unreasonable";

(f) What subset of dealer data is actually subject to the law; or even

(g) Whether, in light of conflicting federal obligations, the law applies to Plaintiffs or their core conduct at all.

(Doc. 1 at 53–54.) But a "person of ordinary intelligence" would not interpret a prohibition against "cyber ransom," defined as encrypting, restricting or prohibiting, or threatening to encrypt, restrict or prohibit a "dealer's or a dealer's authorized integrator's access to protected dealer data for monetary gain," A.R.S. § 28-4651, as a prohibition against money exchanged for encrypting data *at a dealer's request.* Nor would a reasonable person interpret "[p]rotected dealer data" as anything other than "data ... stored in [*that*] dealer's dealer data system." A.R.S. § 28-4651. A person of ordinary intelligence would not assume that this definition created a right for a dealer to access another dealer's DMS, let alone a duty for Plaintiffs to facilitate that access. These provisions are not unconstitutionally vague.

Plaintiffs allege they do not know "[w]hether any or all of their dealer charges are prohibited fees." (Doc. 1 at 53.) In the Dealer Law, "[f]ee" means "a charge for allowing access to protected dealer data beyond any direct costs incurred by the dealer data vendor in providing protected dealer data access to an authorized integrator or allowing an authorized integrator to write data to a dealer data system." Ariz. Rev. Stat. Ann. § 28-4651. The Dealer Law makes clear, to a person of ordinary intelligence, what kinds of fees are prohibited by explicitly stating it in § 28-4653:

> A third party may not ... [t]ake any action by contract, technical means or otherwise to prohibit or limit a dealer's ability to protect, store, copy, share or use protected dealer data, including ... [i]mposing any fee or other restriction on the dealer or an authorized integrator for accessing or sharing protected dealer data or for writing data to a dealer data system, including any fee on a dealer that chooses to submit or push data or information to the third party as prescribed in § 28-4652. A third party must disclose a charge to the dealer and justify the charge by documentary evidence of the costs associated with access or the charge will be deemed to be a fee pursuant to this subdivision.

As with other sections of the Dealer Law Plaintiffs allege are vague, "the general class of offenses to which [this section] is directed is plainly within its terms"; thus, "the statute will not be struck down as vague even though marginal cases could be put where doubts might arise." *United States v. Harriss*, 347 U.S. 612, 618, 74 S.Ct. 808, 98 L.Ed. 989 (1954).

Next, Plaintiffs argue that they do not know "[w]hich of their restrictions on access by authorized integrators are 'unreasonable.' " (Doc. 1 at 53.) A statute "need not be prolix to avoid impermissible vagueness." *Am. Coal Co. v. Fed. Mine Safety & Health Review Comm'n*, 796 F.3d 18, 28 (D.C. Cir. 2015). Instead, it must merely "provide sufficient guidance so that reasonable regulated parties, aware of the goal the regulation seeks to accomplish, have 'fair warning' of what the regulation requires." *Id.*; *see also Edwards v. Swarthout*, No. C 10-4923 PJH, 2012 WL 2277926, at *9 (N.D. Cal. June 18, 2012), *aff'd*, 552 F. App'x 715 (9th Cir. 2014) ("[T]he fact

that a penal statute requires ... upon occasion [a] determin[ation] ... of reasonableness is not sufficient to make it too vague to afford a practical guide to permissible conduct."). Even with regulations "provid[ing] limited direction," courts have found the terms "reasonable" and "unreasonable" to be adequately specific when the parties subject to the regulation were "experienced in the industry and well-schooled in the characteristics" of the item being regulated, as is the case here. *Id.* "A reasonableness standard is found throughout the statutory and common law, and legal standards such as an 'unreasonably low price for the purpose of destroying competition or eliminating a competitor,' generally withstand an ambiguity challenge." *Monarch Content Mgmt. LLC v. Arizona Dep't of Gaming*, No. CV-19-04928-PHX-JJT, 2019 WL 7019416, at *6 (D. Ariz. Dec. 20, 2019) (quoting *United States v. Nat'l Dairy Prods. Corp.*, 372 U.S. 29, 34, 83 S.Ct. 594, 9 L.Ed.2d 561 (1963)) (finding that a statutory provision stating that an agreement would be approved if it "is reasonable and complies with the requirements of this subsection" and prohibiting charging an "excessive or unreasonable rate" was not impermissibly vague). Moreover, the fact that the Dealer Law provides six examples of what constitutes an unreasonable restriction makes this case different from one in which a law provides "no objective standards for enforcement." *St. Mark Roman Catholic Par. Phoenix v. City of Phoenix*, No. CV 09-1830-PHX-SRB, 2010 WL 11519169, at *8 (D. Ariz. Mar. 3, 2010).

Finally, Plaintiffs argue that they cannot discern "[w]hat subset of dealer data is actually subject to the law" or "even [w]hether, in light of conflicting federal obligations, the law applies to Plaintiffs or their core conduct at all," given that "the law does not prevent third parties (including Plaintiffs) from discharging their obligations, as service providers or otherwise, under federal, state or local law to protect and secure protected dealer data," and, in Plaintiffs' view, "the entire purpose of the DMS Law is to prohibit Plaintiffs from implementing the technological and operational measures that Plaintiffs have developed based on their understanding of their legal obligations to protect and secure protected dealer data." (Doc. 1 at 54, 43.) "Protected dealer data" is explicitly and clearly defined in § 28-4651 of the Dealer Law. And Plaintiffs clearly fall within the definition of "third party" in that section, and thus within the purview of the Dealer Law, given that "third parties" are "any other person other than the dealer." A.R.S. § 28-4651. Moreover, as addressed in the preemption analysis above, the Court disagrees that the Dealer Law wholly prohibits Plaintiffs from fulfilling their federal, state or local obligations to protect and secure dealer data.

[17, 18] The Dealer Law "give[s] the person of ordinary intelligence a reasonable opportunity to know what is prohibited." *Grayned*, 408 U.S. at 108–09, 92 S.Ct. 2294. Moreover, it does not require courts to apply the Dealer Law to an "idealized crime" but rather "to real-world facts ... engage[d in] on a particular occasion." *Guerrero*, 908 F.3d at 545. Finally, "speculation about possible vagueness in hypothetical situations not before us will not support a facial attack on a statute when it is surely valid in the vast majority of its intended applications." *California Hotels & Lodging Ass'n v. City of Oakland*, 393 F. Supp. 3d 817, 833 (N.D. Cal. 2019). Claim Six is accordingly dismissed.

2. Takings Clause

[19–22] Determining what constitutes a "taking" for purposes of the Fifth Amendment "has proved to be a problem of considerable difficulty"; the inquiry is "essentially ad hoc" and "factual." *Penn*

Cent. Transp. Co. v. City of New York, 438 U.S. 104, 123–24, 98 S.Ct. 2646, 57 L.Ed.2d 631 (1978). "The paradigmatic taking requiring just compensation is a direct government appropriation or physical invasion of private property." *Lingle v. Chevron U.S.A. Inc.*, 544 U.S. 528, 537, 125 S.Ct. 2074, 161 L.Ed.2d 876 (2005). However, mere *regulation* of private property may also be "so onerous that its effect is tantamount to a direct appropriation or ouster." *Id.* For instance, where the government "requires an owner to suffer a permanent physical invasion of her property—however minor—it must provide just compensation." *Id.* at 538, 125 S.Ct. 2074. In addition, the government must pay for regulations that completely deprive an owner of "all economically beneficial us[e]" of her property. *Id.* Beyond these "two relatively narrow categories," *id.*, regulatory takings challenges are governed by "several factors that have particular significance," including the economic impact of the regulation on the claimant, the extent to which the regulation has interfered with investment-backed expectations, and the character of the governmental action (for instance, a taking "may more readily be found when the interference with property can be characterized as a physical invasion by government"), *Penn Cent.*, 438 U.S. at 124, 98 S.Ct. 2646.

[23] Plaintiffs allege the Dealer Law constitutes a taking because "permitting third parties to use Plaintiffs' hardware and software to access and rewrite their DMSs without Plaintiffs' permission" constitutes an "interference" with Plaintiffs' property amounting to "a physical invasion by government."[6] (Doc. 50 at 31.) Plaintiffs also argue that the Dealer Law "will have a significant economic impact on Plaintiffs and substantially interfere with their reasonable investment-backed expectations" because "Plaintiffs have invested heavily to maintain and enhance their proprietary systems" and "charge fees to authorized users to recoup" this investment. *Id.* at 32. Plaintiffs have pled a takings violation sufficient to survive at this stage of the proceedings, given that the takings inquiry is particularly fact dependent. The Motion is denied as to Claim Seven.

3. Contracts Clause

[24] The Contracts Clause restricts the power of States to disrupt contractual arrangements, mandating that "[n]o state shall ... pass any ... Law impairing the Obligation of Contracts." U.S. Const., Art. I, § 10, cl. 1. However, not all laws affecting pre-existing contracts are unconstitutional under the Contracts Clause:

> To determine when such a law crosses the constitutional line, this Court has long applied a two-step test. The threshold issue is whether the state law has "operated as a substantial impairment of a contractual relationship." *Allied Structural Steel Co.* [*v. Spannaus*, 438 U.S. 234, 244, 98 S.Ct. 2716, 57 L.Ed.2d 727 (1978).] In answering that question, the Court has considered the extent to which the law undermines the contractual bargain, interferes with a party's reasonable expectations, and prevents the party from safeguarding or reinstating his rights.... If such factors show a substantial impairment, the inquiry turns to the means and ends of the legislation. In particular, the Court has asked whether the state law is drawn in an "appropriate" and "reasonable" way

6. At various points, Plaintiffs allege "physical" (Doc. 1 at 55), "regulatory," *id.*, and "*per se*" (Doc. 50 at 31) takings. However, as Plaintiffs do not argue a "paradigmatic" physical taking in their Response, and instead rely on language from *Lingle* used to describe regulatory takings, the Court will assume Plaintiffs are asserting only regulatory takings claims.

to advance "a significant and legitimate public purpose." *Energy Reserves Group, Inc. v. Kansas Power & Light Co.*, 459 U.S. 400, 411–412, 103 S.Ct. 697, 74 L.Ed.2d 569 (1983).

Sveen v. Melin, —— U.S. ——, 138 S. Ct. 1815, 1821–22, 201 L.Ed.2d 180 (2018).

[25] Plaintiffs argue that the Dealer Law "substantially impairs Plaintiffs' existing contractual relationships with dealers" because their existing contracts "prohibit dealers from granting third parties access to Plaintiffs' DMSs," while the Dealer Law "require[s] that any agreement regarding access to, sharing or selling of, copying, using or transmitting dealer data is terminable upon 90 days' notice from the dealer."[7] (Doc. 1 at 55.) "Total destruction of contractual expectations is not necessary for a finding of substantial impairment," *Energy Reserves Grp., Inc. v. Kansas Power & Light Co.*, 459 U.S. 400, 411, 103 S.Ct. 697, 74 L.Ed.2d 569 (1983); moreover, at this stage, the Court must construe the facts in the light most favorable to Plaintiffs. Plaintiffs have adequately pled that the Dealer Law would substantially impair their contracts.

[26] As to the second inquiry, Plaintiffs allege that "the Law's purpose [i]s to provide an economic benefit to a narrow class of private actors—the car dealers," and that the Dealer Law "is not an appropriate and reasonable means of serving any legitimate interest because, for instance ... it places consumer data at risk to provide an economic benefit to car dealers." (Doc. 50 at 34.) While courts "generally defer to the judgment of state legislatures as to both necessity and reasonableness so long as the state itself is not a contracting party," *Lazar v. Kroncke*, 862 F.3d 1186, 1199 (9th Cir. 2017), the determination of whether the Dealer Law is drawn in an "appropriate" and "reasonable" way to advance "a significant and legitimate public purpose" is not appropriate at this stage of the proceedings where Plaintiffs have not had a chance to develop the record. Construing all facts in Plaintiffs' favor, the Court cannot say at the motion to dismiss stage that the Dealer Law does not violate the Contracts Clause. The Motion is denied as to Claim Eight.

4. Dormant Commerce Clause

[27] The Commerce Clause provides Congress with the power to "regulate Commerce ... among the several States ...." U.S. Const. art. I, § 8, cl. 3. A state statute violates the so-called Dormant Commerce Clause if it "directly regulates or discriminates against interstate commerce," *Brown-Forman Distillers Corp. v. N.Y. State Liquor Auth.*, 476 U.S. 573, 579, 106 S.Ct. 2080, 90 L.Ed.2d 552 (1986), or, if a statute has only indirect effects on interstate commerce and is non-discriminatory, if "the burdens of the statute so outweigh the putative benefits as to make the statute unreasonable or irrational," *UFO Chuting of Haw., Inc. v. Smith*, 508 F.3d 1189, 1196 (9th Cir. 2007).

[28] Plaintiffs allege that the Dealer Law "imposes an undue and substantial burden on interstate commerce" by requiring Plaintiffs to "change their products specifically for the Arizona market" even though "DMSs are sold nationwide, and indeed some dealers have operations in more than one State." (Doc. 1 at 56.) More-

7. Defendants assert that if Plaintiffs "want to challenge whether the law can be constitutionally applied to an existing contract, that would require a specific challenge to a specific contract," (Doc. 54 at 8); however, they provide no authority for this assertion. Nor do they explain how Plaintiffs' description of their existing contracts with dealerships as alleged in their complaint, *see, e.g.*, Doc. 1 at 23, is insufficient to constitute a "specific challenge."

over, they argue that there is no "legitimate public purpose justifying the DMS Law's burden on interstate commerce because the law inures to the sole benefit of a small class of private parties." *Id.* But courts do not engage in any "assessment of the benefits of a state law and the wisdom in adopting" it until a party has shown that a state statute discriminates in favor of in-state commerce or imposes a significant burden on interstate commerce. *Chinatown Neighborhood Ass'n v. Harris*, 794 F.3d 1136, 1146 (9th Cir. 2015).

[29] Plaintiffs have made no plausible allegation that the Dealer Law is discriminatory in favor of Arizona commerce. As to whether the Dealer Law imposes a significant burden on interstate commerce, "only a small number of cases invalidating laws under the dormant Commerce Clause have involved laws that were genuinely nondiscriminatory." *Id.* Generally, such cases involve "inconsistent regulations of activities that are inherently national or require a uniform system of regulation," *Nat'l Ass'n of Optometrists & Opticians v. Harris*, 682 F.3d 1144, 1148 (9th Cir. 2012), such as transportation or sports leagues, *Chinatown*, 794 F.3d at 1146. Moreover, "Supreme Court precedent establishes that there is not a significant burden on interstate commerce merely because a non-discriminatory regulation precludes a preferred, more profitable method of operating in a retail market"; the dormant Commerce Clause "protects the interstate market, not particular interstate firms, from prohibitive or burdensome regulations." *Nat'l Ass'n of Optometrists*, 682 F.3d at 1154, 1152. Plaintiffs have not shown that the Dealer Law regulates activities that are "inherently national." Plaintiffs Motion to Dismiss is granted as to Claim Nine.

5. First Amendment Freedom of Speech

Plaintiffs allege the Dealer Law abridges their freedom of speech in two ways.

First, Plaintiffs contend that because they are "not merely conduits facilitating the transmission of information between dealers and third-party integrators," but rather "*organize*[*rs of*] information belonging to dealers and others in their proprietary DMSs," the Dealer Law violates the First Amendment by requiring Plaintiffs to share "information, as they have organized it, with third parties." (Doc. 50 at 36) (emphasis added). Plaintiffs describe this information sharing as "compelled ... communicat[ion]." *Id.* To the extent that Plaintiffs seek protection for any copyright they have in the organization of their DMS information, they have stated a claim to such protection that survives, as addressed in the above Copyright Act section. However, Plaintiffs have provided no relevant authority to support the claim that organization of otherwise unprotected information is subject to *First Amendment* protection. At oral argument, Plaintiffs cited *Arkansas Educational Television Commission v. Forbes*, 523 U.S. 666, 118 S.Ct. 1633, 140 L.Ed.2d 875 (1998), for the provision that the First Amendment protects the organization of material. *Forbes* held that a public broadcaster "engages in speech activity" when it "exercises editorial discretion in the selection and presentation of its programming"; however, that case is inapposite here, where, unlike the broadcaster in *Forbes*, Plaintiffs' organizational decisions do *not* result in a decision by Plaintiff as to what speech to disseminate. *Forbes* dealt with the organizing broadcaster's right to exclude a candidate for federal office from a televised debate—in other words, allowing the broadcaster the freedom to "speak" by running programming that did not include the candidate. Here, Plaintiffs' seek First Amend-

ment protection not to "speak," but to protect information stored within the DMS from access by any others, relief more appropriately provided—if at all—through statute. Plaintiffs' first free speech arguments fails.

[30] Plaintiffs' second First Amendment argument is that because they will be "compelled to write computer code if the Dealer Law goes into effect" and "the computer code Plaintiffs must write falls within the First Amendment's protection," the Dealer Law violates the First Amendment because it "necessarily alters the content of [Plaintiffs'] speech," demanding "exacting First Amendment scrutiny." (Doc. 50 at 36.) Plaintiffs complaint does not sufficiently allege how writing code to make unprotected information accessible to third parties is subject to First Amendment scrutiny. Computer code and computer programs constructed from code can constitute speech warranting First Amendment protection. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449 (2d Cir. 2001); *see also United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1127 (N.D. Cal. 2002) ("[c]omputer software is . . . speech that is protected at some level by the First Amendment"). However, whether code rises to the level of speech under the First Amendment depends on whether "a programmer might be said to communicate through code to the user of the program (not necessarily protected)" or only "to the computer (never protected)." *Corley*, 273 F.3d at 449. And even when software communicates to a user, where it is "mechanical[ ]" and does not involve "second-guessing" or "intercession of the mind or the will of the recipient," such code is devoid of any constitutionally protected speech. *Id.* (describing the holding of *Commodity Futures Trading Comm'n v. Vartuli*, 228 F.3d 94 (2d Cir. 2000)).

The Dealer Law does not in fact mandate that a DMS provider write code. It only mandates that owners of DMS systems "[a]dopt and make available a standardized framework for the exchange, integration and sharing of data from [a DMS]," Ariz. Rev. Stat. Ann. § 28-4654, "[p]rovide access to open application programming interfaces to authorized integrators," *id.*, and allow "third part[ies] that ha[ve] satisfied or [are] compliant with the star standards or other generally accepted standards that are at least as comprehensive as the star standards and that the dealer has identified as one of its authorized integrators [to] integrat[e] into the dealer's dealer data system," Ariz. Rev. Stat. Ann. § 28-4653. Given the nature of existing DMSs, it would not be surprising if the implementation of these provisions required DMS providers to write code. Nevertheless, as the statute makes plain, the purpose of the Dealer Law—and thus any such code—is merely to facilitate the sharing of the otherwise unprotected underlying information in the DMS. To the extent Plaintiffs comply with the Dealer Law by creating code, that code only tells a computer how to function; it has no other expressive purpose.

[31] *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000), is not to the contrary. In that case, the plaintiff sought to distribute encryption source code to demonstrate how computers work—code that qualified as speech because it was "an expressive means for the exchange of information and ideas about computer programming." 209 F.3d at 485. Nor is this case like *Bernstein v. U.S. Dep't of State*, 922 F. Supp. 1426, 1429 (N.D. Cal. 1996), in which the regulation at issue prohibited the plaintiff's publication of code "articulat[ing] . . . mathematical ideas" so substantive they were also published in an academic paper. Plaintiffs cannot plausibly argue that the Dealer Law's regulation of Plaintiffs' code goes beyond the code's capacity "to instruct a

computer" to give third parties access to dealer data, just as the *Corley* court held that the DMCA's prohibition on posting technology for circumventing DVD encryption on the internet was a functional and not a speech regulation. 273 F.3d at 454. The allegations of Plaintiffs' complaint establish that, unlike in *Junger*, *Bernstein*, and *Corley*, any code Plaintiffs create pursuant to the Dealer Law only instructs a computer to provide access to unprotected information contained in Plaintiffs' DMSs. Thus, as alleged in the complaint, the Dealer Law does not regulate speech under the First Amendment. Plaintiffs First Amendment claim is therefore dismissed. This claim is dismissed with leave to amend, if Plaintiffs wish to do so, within 30 days.

IT IS THEREFORE ORDERED that Arizona Automobile Dealers Association's Motion to Dismiss for Failure to State a Claim (Doc. 39) and Defendants Mark Brnovich and John S. Halikowski's Joint Motion to Dismiss for Failure to State a Claim (Doc. 40) are **GRANTED IN PART** and **DENIED IN PART** as follows:

1. Claims One, Three, Four, Five, Six, Nine, and Ten are dismissed.

2. Claim Ten *only* is dismissed with leave to amend. Plaintiffs shall have **30 days** from the date of this Order to file an amended complaint, if they wish to do so.

TAPESTRY ON CENTRAL CONDOMINIUM ASSOCIATION, Plaintiff,

v.

LIBERTY INSURANCE UNDERWRITERS INCORPORATED, Defendant.

No. CV-18-04857-PHX-JJT

United States District Court, D. Arizona.

Signed 02/13/2020

Background: Condominium association filed suit against its liability insurer for breach of policy, based on assertion that insurer owed duty to defend association in underlying suit against association for breach of contract. Insurer filed motion for summary judgment and insurer filed cross-motion.

Holdings: The District Court, John J. Tuchi, J., held that:

(1) single action brought against association presented two "claims," and not one single claim, thus requiring determination whether each claim fell within exclusion from coverage for claims based on construction defects;

(2) architect's claims for breach of contract fell within exclusion from coverage for claims "based upon, arising from, or in any way related to any construction defect";

(3) insurer was not relieved of duty to defend association on claim brought by construction company; and

(4) mixed-action rule did not apply to require insurer to defend condominium association on both claims.

Insurer's motion to summary judgment granted in part and denied in part; association's cross-motion for summary judgment granted in part and denied in part.