

1 **WO**

2
3
4
5
6 **IN THE UNITED STATES DISTRICT COURT**
7 **FOR THE DISTRICT OF ARIZONA**
8

9 CDK Global LLC, et al.,

10 Plaintiffs,

11 v.

12 Mark Brnovich, et al.,

13 Defendants,

14 and

15 Arizona Automobile Dealers Association,

16 Intervenor Defendant.
17

No. CV-19-04849-PHX-GMS

ORDER

18 Pending before the Court are Defendant Arizona Automobile Dealers Association
19 (“AADA”)’s Motion to Dismiss for Failure to State a Claim (Doc. 39) and Defendants
20 Mark Brnovich and John S. Halikowski’s¹ Joint Motion to Dismiss for Failure to State a
21 Claim (Doc. 40). The Motions are granted in part and denied in part.

22 **BACKGROUND**

23 Plaintiffs CDK Global LLC and Reynolds and Reynolds Company (collectively,
24 “Plaintiffs”) develop, own, and operate proprietary computer systems known as dealer
25 management systems (“DMSs”) that process vast amounts of data² sourced from various

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

28 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,

1 parties. Automotive dealerships hold licenses to DMSs to help manage their business
2 operations, including handling confidential consumer and proprietary data, processing
3 transactions, and managing data communications between dealers, customers, car
4 manufacturers, credit bureaus, and other third parties. Plaintiffs employ multiple
5 technological measures—such as secure login credentials, CAPTCHA prompts, and
6 comprehensive cybersecurity infrastructure, hardware, and software—to safeguard their
7 DMS systems from unauthorized access or breach. Plaintiffs also contractually prohibit
8 dealers from granting third parties access to their DMSs without Plaintiffs’ authorization.

9 In March 2019, the Arizona Legislature passed the Dealer Data Security Law (“the
10 Dealer Law”), A.R.S. §§ 28-4651–28-4655. The Dealer Law went into effect on August
11 27, 2019.³ The Dealer Law regulates the relationship between DMS licensers like Plaintiffs
12 and the dealerships they serve. Under the Dealer Law, DMS providers may no longer
13 “[p]rohibit[] a third party [that has been authorized by the Dealer and] that has satisfied or
14 is compliant with . . . current, applicable security standards published by the standards for
15 technology in automotive retail [(STAR standards)] . . . from integrating into the dealer’s
16 [DMS] or plac[e] an unreasonable restriction on integration” A.R.S. §§ 28-
17 4653(A)(3)(b), 28-4651(9). The Dealer Law also requires that DMS providers “[a]dopt and
18 make available a standardized framework for the exchange, integration and sharing of data
19 from [a DMS]” that is compatible with STAR standards and that they “[p]rovide access to
20 open application programming interfaces to authorized integrators.” A.R.S. § 28-4654(A).
21 Finally, a DMS provider may only use data to the extent permitted in the DMS provider’s
22 agreement with the dealer, must permit dealer termination of such agreement, and “must

23 _____
24 and Subaru. Other data in or processed by [Plaintiffs’] DMS[s] is proprietary to third-party
25 service providers, such as credit reporting bureaus like Equifax, Experian and TransUnion.
26 Still other data in the DMS[s] is [Plaintiffs’] own proprietary, copyrightable data, including
27 forms, accounting rules, tax tables, service pricing guides, and proprietary tools and data
28 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.)

1 work to ensure a secure transition of all protected dealer data to a successor dealer data
2 vendor or authorized integrator” upon termination. A.R.S. §§ 28-4654(B)(1)-(3).

3 Plaintiffs filed the underlying complaint seeking declaratory and injunctive relief
4 from the Dealer Law on July 29, 2019. These Motions to Dismiss followed on September
5 18, 2019.

6 DISCUSSION

7 I. Legal Standard

8 To survive a motion to dismiss for failure to state a claim pursuant to Federal Rule
9 of Civil Procedure 12(b)(6), a complaint must contain more than a “formulaic recitation of
10 the elements of a cause of action”; it must contain factual allegations sufficient to “raise
11 the right of relief above the speculative level.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544,
12 555 (2007) (quoting *Conley v. Gibson*, 355 U.S. 41, 47 (1957)). While “a complaint need
13 not contain detailed factual allegations . . . it must plead ‘enough facts to state a claim to
14 relief that is plausible on its face.’” *Clemens v. DaimlerChrysler Corp.*, 534 F.3d 1017,
15 1022 (9th Cir. 2008) (quoting *Twombly*, 550 U.S. at 570). “A claim has facial plausibility
16 when the plaintiff pleads factual content that allows the court to draw the reasonable
17 inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556
18 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. at 556). When analyzing a complaint for
19 failure to state a claim, “allegations of material fact are taken as true and construed in the
20 light most favorable to the non-moving party.” *Smith v. Jackson*, 84 F.3d 1213, 1217 (9th
21 Cir. 1996). In addition, the Court must assume that all general allegations “embrace
22 whatever specific facts might be necessary to support them.” *Pelozo v. Capistrano Unified*
23 *Sch. Dist.*, 37 F.3d 517, 521 (9th Cir. 1994). However, legal conclusions couched as factual
24 allegations are not given a presumption of truthfulness, and “conclusory allegations of law
25 and unwarranted inferences are not sufficient to defeat a motion to dismiss.” *Pareto v.*
26 *F.D.I.C.*, 139 F.3d 696, 699 (9th Cir. 1998).

27 ///

28 ///

1 **II. Analysis**

2 Plaintiffs’ claims concern five federal statutes and five provisions of the United
3 States Constitution. Plaintiffs “object to [the Dealer Law] not in the context of an actual
4 [prosecution], but in a facial challenge” prior to enforcement such that the State of Arizona
5 “has had no opportunity to implement [the Dealer Law], and its courts have had no occasion
6 to construe the law in the context of actual disputes . . . or to accord the law a limiting
7 construction to avoid constitutional questions.” *Washington State Grange v. Washington*
8 *State Republican Party*, 552 U.S. 442, 449–50 (2008). “Facial challenges are disfavored
9 for several reasons”:

10 Claims of facial invalidity often rest on speculation. As a consequence, they
11 raise the risk of “premature interpretation of statutes on the basis of factually
12 barebones records.” *Sabri v. United States*, 541 U.S. 600, 609 . . . (2004)
13 (internal quotation marks and brackets omitted). Facial challenges also run
14 contrary to the fundamental principle of judicial restraint that courts should
15 neither “anticipate a question of constitutional law in advance of the
16 necessity of deciding it” nor “formulate a rule of constitutional law broader
17 than is required by the precise facts to which it is to be applied.” *Ashwander*
18 *v. TVA*, 297 U.S. 288, 346–347 . . . (1936) (Brandeis, J., concurring)
19 Finally, facial challenges threaten to short circuit the democratic process by
20 preventing laws embodying the will of the people from being implemented
21 in a manner consistent with the Constitution.

22 *Id.* at 450–51.

23 **A. Ripeness**

24 To obtain relief, Plaintiffs must show “a genuine threat of imminent prosecution
25 under the challenged statute to establish a justiciable case or controversy.” (Doc. 40 at 6)
26 (quoting *Wash. Mercantile Ass’n v. Williams*, 733 F.2d 687, 688 (9th Cir. 1984)). The three
27 factors courts consider when analyzing the genuineness of a threat of prosecution include:
28 (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

1 longstanding practices. And when fear of criminal prosecution under an allegedly
2 unconstitutional statute is “not imaginary or wholly speculative,” a plaintiff need not “first
3 expose himself to actual arrest or prosecution to be entitled to challenge the statute.”
4 *Babbitt v. United Farm Workers Nat. Union*, 442 U.S. 289, 302 (1979). Here, as in *Babbitt*,
5 “the State has not disavowed any intention of invoking the criminal penalty provision”
6 against Plaintiffs, and “the positions of the parties are sufficiently adverse with respect to
7 [the Dealer Law] . . . to present a case or controversy within the jurisdiction of the District
8 Court.” *Id.* Plaintiffs’ claims present a ripe controversy.

9 **B. Federal Preemption**

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

21 On a facial preemption challenge, a plaintiff must show that “no set of
22 circumstances exists under which the Act would be valid.” *United States v. Salerno*, 481
23 U.S. 739, 746 (1987).⁴ However, the proper inquiry is not simply “whether state and local
24 law enforcement officials can apply the statute in a constitutional way,” because “there can
25 be no constitutional application of a statute that, on its face, conflicts with Congressional
26 intent and therefore is preempted by the Supremacy Clause.” *United States v. Arizona*, 641

27 _____
28 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).

1 F.3d 339, 345–46 (9th Cir. 2011), *aff'd in part, rev'd in part and remanded*, 567 U.S. 387
2 (2012). Nevertheless, “courts should assume that ‘the historic police powers of the States’
3 are not superseded ‘unless that was the clear and manifest purpose of Congress.’” *Arizona*,
4 567 U.S. at 400 (quoting *Rice v. Santa Fe Elevator Corp.*, 331 U.S. 218, 230 (1947)). And,
5 as this preemption challenge has been brought prior to enforcement and thus “without the
6 benefit of a definitive interpretation [of the Dealer Law] from the state courts,” the timing
7 of this case “counsel[s] caution in evaluating [the Dealer Law’s] validity” because “it
8 would be inappropriate to assume [the Dealer Law] will be construed in a way that creates
9 a conflict with federal law.” *Arizona*, 567 U.S. at 415.

10 1. CFAA

11 The CFAA was enacted to prevent “hackers” from “steal[ing] information or . . .
12 disrupt[ing] or destroy[ing] computer functionality” and “to penalize thefts of property via
13 computer that occur as part of a scheme to defraud.” *United States v. Nosal*, 844 F.3d 1024,
14 1032 (9th Cir. 2016). “The conduct prohibited [by the CFAA] is analogous to that of
15 ‘breaking and entering,’” H.R. Rep. No. 98-894, at 20 (1984), a comparison invoked “so
16 frequently during congressional consideration” that the Ninth Circuit found the CFAA
17 inapposite where the breaking and entering analogy “ha[d] no application,” *hiQ Labs, Inc.*
18 *v. LinkedIn Corp.*, 938 F.3d 985, 1001 (9th Cir. 2019). To those ends, the CFAA imposes
19 criminal and civil liability on anyone who “intentionally accesses a computer without
20 authorization or exceeds authorized access, and thereby obtains . . . information”
21 *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1065–66 (9th Cir. 2016). However,
22 while the CFAA criminalizes accessing information without authorization in protected
23 computers, it does not limit how access might be authorized. Rather, it leaves it to authority
24 external to the statute itself—such as state law—to determine what is authorized or not.

25 Plaintiffs contend that the Dealer Law is preempted by the CFAA because the
26 Dealer Law poses “an obstacle to” Congress’ purpose in enacting the CFAA “by requiring
27 CDK and Reynolds to allow access to their systems by any user authorized by a dealer.”
28 (Doc. 1 at 50, 51.) But Plaintiffs’ suggested interpretation ignores the authorization

1 provided by state law and would expand the CFAA beyond its “narrow” aim, *Shamrock*
2 *Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008), of “deter[ing] and punish[ing]
3 certain ‘high-tech’ crimes” and targeting “hackers who accessed computers to steal
4 information or to disrupt or destroy computer functionality,” *Nosal*, 844 F.3d at 1032. “The
5 CFAA must be interpreted in its historical context, mindful of Congress’ purpose in
6 enacting it.” *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1109 (N.D. Cal.
7 2017), *aff’d and remanded*, 938 F.3d 985 (9th Cir. 2019). A broad reading of the CFAA
8 “could stifle the dynamic evolution and incremental development of state and local laws
9 addressing the delicate balance between open access to information and privacy,” a
10 “profound consequence[] . . . Congress could not have intended . . . when it enacted the
11 CFAA in 1984 . . . before the advent of the World Wide Web.” *Id.*

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

23 **2. The Copyright Act**

24 Under the Copyright Act, copyright protection, including the “exclusive right[]” to

25 ⁵ Regarding the CFAA and at various other points in their Motion to Dismiss, Defendants
26 argue that Plaintiffs can comply with the Dealer Law by creating an application
27 programming interface (API) that would allow dealers to transfer their data to and from
28 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.

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

15 Under the Dealer Law, DMS providers like Plaintiffs may not prohibit other parties
16 that have “satisfied or [are] compliant with the star standards or other generally accepted
17 standards that are at least as comprehensive as the star standards and that the dealer has
18 identified as one of its authorized integrators from integrating into the dealer’s dealer data
19 system.” Ariz. Rev. Stat. Ann. § 28-4653. At oral argument, Defendants asserted that the
20 Dealer Law “does not say that the DMS companies must tolerate the ways in which data
21 access are currently done,” but rather that it simply requires Plaintiffs and other DMS
22 providers to “provide a way for third parties to extract the data at the dealers’ behest . . . in
23 a way that is consistent with plaintiffs’ Copyright Act rights.” Transcript of Oral Argument
24 at 34. Defendants further argue that “there is no allegation in the complaint that that is not
25 possible.” *Id.* But Plaintiffs argue that the Dealer Law conflicts with the Copyright Act
26 because “requiring [DMS providers] to allow third parties with no license agreement . . .
27 to access and use . . . copyrighted DMS software . . . necessarily entails the display,
28 distribution, and creation of copies and derivative works of . . . copyrighted DMS

1 software.” (Doc. 1 at 47) (emphasis added). “[E]ach time a user runs the DMS software,
2 that process creates a new fixed copy of the original computer program code in the
3 computer’s random access memory.” *Id.* at 47–48. The Court therefore interprets Plaintiffs
4 to be alleging exactly what Defendants have articulated—that it is not possible for Plaintiffs
5 to both comply with the Dealer Law and retain their rights under the Copyright Act.
6 Construing the facts in Plaintiffs’ favor, the Dealer Law “conflicts with Congressional
7 intent . . . on its face,” regardless of Defendants’ assertion that “the statute [can be applied]
8 in a constitutional way,” *United States v. Arizona*, 641 F.3d 339, 345–46 (9th Cir. 2011),
9 *aff’d in part, rev’d in part and remanded*, 567 U.S. 387 (2012), in cases where DMS
10 providers have not yet obtained copyright registration or where it would be possible for
11 third parties to access DMSs without copying DMS providers’ proprietary software.

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

15 (1) the purpose and character of the use, including whether such use is of a
16 commercial nature or is for nonprofit educational purposes; (2) the nature of
17 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.

18 *Id.*

19 In *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 596 (9th Cir.
20 2000), the Ninth Circuit held that Connectix’s intermediate copying of Sony’s software to
21 create software allowing Connectix customers to play Sony PlayStation games on their
22 computers was a fair use. In analyzing the “nature of the copyrighted work,” the court noted
23 that Sony’s software warranted a “lower degree of protection than more traditional literary
24 works” because it “contain[ed] unprotected aspects that [could not] be examined without
25 copying.” *Id.* at 603. Thus, the court determined, in to order to constitute fair use,
26 “Connectix’s copying of [Sony’s software] *must have been ‘necessary.’*” *Id.* (emphasis
27 added). Similarly, in *Assessment Technologies of Wisconsin, LLC v. WIREdata, Inc.*, 350
28 F.3d 640, 645 (7th Cir. 2003), the Seventh Circuit held that if the *only way* WIREdata, the

1 entity seeking to extract data from the plaintiff’s database, could obtain the public-domain
2 data it sought would be by “copying [the plaintiff’s] compilation and not just the compiled
3 data . . . because the data and the format in which they were organized could not be
4 disentangled, [WIREdata] would be privileged to make such a copy.”

5 Here, Reynolds has alleged that, even if third parties do not have access to their
6 DMS, “dealership customers can use dealer-driven data export tools to send their
7 operational and inventory data to application providers or other third parties, as the dealer
8 deems appropriate.” (Doc. 1 at 29.) Thus, unlike in *Sony* and *WIREdata*, third parties’
9 copying of Plaintiffs’ software would presumably not be necessary to obtain dealer data
10 and thus would presumably not qualify as “fair use.” The Motion is accordingly denied as
11 to the Copyright Act claim at this stage of the litigation.

12 3. DMCA

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

22 There is nothing about the Dealer Data Security Law on its face that violates the
23 DMCA. Like the CFAA, the purpose of the DMCA is “to ensure the integrity of the
24 electronic marketplace by preventing fraud and misinformation,” *ITC Textile, Ltd. v. Wal-*
25 *Mart Stores, Inc.*, No. 208CV07422FMCJCX, 2009 WL 10671458, at *5 (C.D. Cal. Mar.
26 31, 2009), and to provide copyright owners “reasonable assurance that they will be
27 protected against massive piracy,” S. Rep. No. 105–190, at 8 (May 11, 1998). And like the
28 CFAA, the DMCA does not address the issue of state statutes requiring those who hold

1 dealer protected data to provide access to it. The DMCA is concerned with preventing
2 unauthorized access to copyrighted works by “pirates who aim to destroy the value of
3 American intellectual property,” H.R. Rep. No. 105–551, pt. 1, at 9–10 (May 22, 1998)—
4 not defining what access is legally authorized in the first place. Presumably, were Plaintiffs
5 able to show that dealers or authorized third parties were pirating or otherwise fraudulently
6 using their copyrighted material, the DMCA might provide them with a private right of
7 action against such persons. But this does not mean that the DMCA preempts the Dealer
8 Law. Defendants’ Motion is granted as to this claim.

9 4. DTSA

10 The DTSA prohibits “economic espionage” and “theft of trade secrets.” 18 U.S.C.
11 §§ 1831–1839. The statute imposes criminal and civil liability on individuals who access
12 protected information “without authorization” or by “improper means,” 18 U.S.C. §§
13 1831–1832, exempting “reverse engineering, independent derivation, or any other lawful
14 means of acquisition,” 18 U.S.C. §§ 1839. In drafting the DTSA, “Congress borrowed
15 heavily from . . . the states’ trade secrets law . . .” *Yeiser Research & Dev., LLC v. Teknor*
16 *Apex Co.*, No. 17-CV-1290-BAS-MSB, 2019 WL 2177658, at *4 (S.D. Cal. May 20,
17 2019). Like the CFAA, the DTSA relies on other law to determine what “other lawful
18 means of acquisition” might be. It thus does not preempt state laws that provide other
19 lawful means of access.

20 In a preemption analysis, “courts should assume that ‘the historic police powers of
21 the States’ are not superseded ‘unless that was the clear and manifest purpose of
22 Congress.’” *Arizona*, 567 U.S. at 400 (quoting *Rice*, 331 U.S. at 230). As with the CFAA
23 and the DMCA addressed above, Plaintiffs have cited nothing in the DTSA or its legislative
24 history indicating that Congress intended this statute to prevent states from authorizing
25 lawful transfers of otherwise protected information. Were the Dealer Law to be
26 implemented, to the extent Plaintiffs could show that dealers or authorized third parties
27 were exploiting access to protected dealer data as a means to steal Plaintiffs’ trade secrets
28 (a claim Plaintiffs have not asserted here), they might have a cause of action under the

1 DTSA. But this does not mean that the DTSA preempts the Dealer Law. Even construing
2 the facts in the light most favorable to Plaintiffs, Plaintiffs' claim fails as a matter of law.
3 The DTSA claim is accordingly dismissed.

4 **5. GLBA**

5 The GLBA imposes on "each financial institution" an "affirmative and continuing
6 obligation to respect the privacy of its customers and to protect the security and
7 confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a).
8 In connection with this requirement, the FTC promulgated a rule requiring financial
9 institutions to "implement information safeguards to control" any "reasonably foreseeable
10 . . . risks to the security, confidentiality, and integrity of customer information." 16 C.F.R.
11 § 314.4.5.

12 The GLBA does not preempt the Dealer Law. Plaintiffs assert that the Dealer Law
13 "prevents dealers from fulfilling their obligations under the GLBA by preventing Plaintiffs,
14 the dealers' service providers, from adequately securing the data they store." (Doc. 50 at
15 25.) But this theory assumes that dealers are incapable of complying with their own GLBA
16 obligations if they retain control of their data. Plaintiffs have not remotely plausibly alleged
17 that this is the case; Plaintiffs have not cited any specific requirement under the GLBA
18 with which dealers cannot comply. Moreover, the Dealer Law provides several provisions
19 designed to ensure compliance with GLBA requirements, including that protected dealer
20 data only be used subject to a dealer's express written consent, that third party integrators
21 comply with the STAR standards or other generally accepted standards that are at least as
22 comprehensive as the STAR standards, and that Plaintiffs are not precluded from
23 "discharging" any federal legal duties "to protect and secure protected dealer data." A.R.S.
24 § 28-4653. This claim is dismissed.

25 **C. Constitutional Violations**

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

1 **1. Vagueness**

2 “It is a basic principle of due process that an enactment is void for vagueness if its
3 prohibitions are not clearly defined.” *Grayned v. City of Rockford*, 408 U.S. 104, 108
4 (1972). At the same time, “we can never expect mathematical certainty from our language.”
5 *Id.* at 110. Thus, while statutes must “give the person of ordinary intelligence a reasonable
6 opportunity to know what is prohibited” and “provide explicit standards for those who
7 apply them,” *Grayned*, 408 U.S. at 108–09; *see also Guerrero v. Whitaker*, 908 F.3d 541,
8 543 (9th Cir. 2018) (a criminal statute violates due process if it is “so vague that it fails to
9 give ordinary people fair notice of the conduct it punishes, or so standardless that it invites
10 arbitrary enforcement”), “uncertainty does not mean that a statute is unconstitutionally
11 vague. Many statutes provide uncertain standards and, so long as those standards are
12 applied to real-world facts . . . engage[d in] on a particular occasion” rather than to an
13 “idealized crime,” “the statutes are almost certainly constitutional,” *Guerrero*, 908 F.3d at
14 545.

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

- 16 (a) Whether contractually agreed dealer access restrictions violate the law;
17 (b) Whether hosting encrypted data for a fee is prohibited cyber-ransom;
18 (c) Whether they are required to facilitate or prevent one dealer from
19 accessing another dealer’s data;
20 (d) Whether any or all of their dealer charges are prohibited fees;
21 (e) Which of their restrictions on access by authorized integrators are
22 “unreasonable”;
23 (f) What subset of dealer data is actually subject to the law; or even
24 (g) Whether, in light of conflicting federal obligations, the law applies to
25 Plaintiffs or their core conduct at all.

26 (Doc. 1 at 53–54.) But a “person of ordinary intelligence” would not interpret a prohibition
27 against “cyber ransom,” defined as encrypting, restricting or prohibiting, or threatening to
28 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

1 that this definition created a right for a dealer to access another dealer’s DMS, let alone a
2 duty for Plaintiffs to facilitate that access. These provisions are not unconstitutionally
3 vague.

4 Plaintiffs allege they do not know “[w]hether any or all of their dealer charges are
5 prohibited fees.” (Doc. 1 at 53.) In the Dealer Law, “[f]ee” means “a charge for allowing
6 access to protected dealer data beyond any direct costs incurred by the dealer data vendor
7 in providing protected dealer data access to an authorized integrator or allowing an
8 authorized integrator to write data to a dealer data system.” Ariz. Rev. Stat. Ann. § 28-
9 4651. The Dealer Law makes clear, to a person of ordinary intelligence, what kinds of fees
10 are prohibited by explicitly stating it in § 28-4653:

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

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

25 Next, Plaintiffs argue that they do not know “[w]hich of their restrictions on access
26 by authorized integrators are ‘unreasonable.’” (Doc. 1 at 53.) A statute “need not be prolix
27 to avoid impermissible vagueness.” *Am. Coal Co. v. Fed. Mine Safety & Health Review*
28 *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

1 practical guide to permissible conduct.”). Even with regulations “provid[ing] limited
2 direction,” courts have found the terms “reasonable” and “unreasonable” to be adequately
3 specific when the parties subject to the regulation were “experienced in the industry and
4 well-schooled in the characteristics” of the item being regulated, as is the case here. *Id.* “A
5 reasonableness standard is found throughout the statutory and common law, and legal
6 standards such as an ‘unreasonably low price for the purpose of destroying competition or
7 eliminating a competitor,’ generally withstand an ambiguity challenge.” *Monarch Content*
8 *Mgmt. LLC v. Arizona Dep’t of Gaming*, No. CV-19-04928-PHX-JJT, 2019 WL 7019416,
9 at *6 (D. Ariz. Dec. 20, 2019) (quoting *United States v. Nat’l Dairy Prods. Corp.*, 372 U.S.
10 29, 34 (1963)) (finding that a statutory provision stating that an agreement would be
11 approved if it “is reasonable and complies with the requirements of this subsection” and
12 prohibiting charging an “excessive or unreasonable rate” was not impermissibly vague).
13 Moreover, the fact that the Dealer Law provides six examples of what constitutes an
14 unreasonable restriction makes this case different from one in which a law provides “no
15 objective standards for enforcement.” *St. Mark Roman Catholic Par. Phoenix v. City of*
16 *Phoenix*, No. CV 09-1830-PHX-SRB, 2010 WL 11519169, at *8 (D. Ariz. Mar. 3, 2010).

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

1 as addressed in the preemption analysis above, the Court disagrees that the Dealer Law
2 wholly prohibits Plaintiffs from fulfilling their federal, state or local obligations to protect
3 and secure dealer data.

4 The Dealer Law “give[s] the person of ordinary intelligence a reasonable
5 opportunity to know what is prohibited.” *Grayned*, 408 U.S. at 108–09. Moreover, it does
6 not require courts to apply the Dealer Law to an “idealized crime” but rather “to real-world
7 facts . . . engage[d in] on a particular occasion.” *Guerrero*, 908 F.3d at 545. Finally,
8 “speculation about possible vagueness in hypothetical situations not before us will not
9 support a facial attack on a statute when it is surely valid in the vast majority of its intended
10 applications.” *California Hotels & Lodging Ass’n v. City of Oakland*, 393 F. Supp. 3d 817,
11 833 (N.D. Cal. 2019). Claim Six is accordingly dismissed.

12 **2. Takings Clause**

13 Determining what constitutes a “taking” for purposes of the Fifth Amendment “has
14 proved to be a problem of considerable difficulty”; the inquiry is “essentially ad hoc” and
15 “factual.” *Penn Cent. Transp. Co. v. City of New York*, 438 U.S. 104, 123–24 (1978). “The
16 paradigmatic taking requiring just compensation is a direct government appropriation or
17 physical invasion of private property.” *Lingle v. Chevron U.S.A. Inc.*, 544 U.S. 528, 537
18 (2005). However, mere *regulation* of private property may also be “so onerous that its
19 effect is tantamount to a direct appropriation or ouster.” *Id.* For instance, where the
20 government “requires an owner to suffer a permanent physical invasion of her property—
21 however minor—it must provide just compensation.” *Id.* at 38. In addition, the government
22 must pay for regulations that completely deprive an owner of “all economically beneficial
23 us[e]” of her property. *Id.* Beyond these “two relatively narrow categories,” *id.*, regulatory
24 takings challenges are governed by “several factors that have particular significance,”
25 including the economic impact of the regulation on the claimant, the extent to which the
26 regulation has interfered with investment-backed expectations, and the character of the
27 governmental action (for instance, a taking “may more readily be found when the
28 interference with property can be characterized as a physical invasion by government”),

1 *Penn Cent.*, 438 U.S. at 124.

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

12 3. Contracts Clause

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

17 To determine when such a law crosses the constitutional line, this Court has
18 long applied a two-step test. The threshold issue is whether the state law has
19 “operated as a substantial impairment of a contractual relationship.” *Allied*
20 *Structural Steel Co. [v. Spannaus]*, 438 U.S. 234, 244 (1978).] In answering
21 that question, the Court has considered the extent to which the law
22 undermines the contractual bargain, interferes with a party’s reasonable
23 expectations, and prevents the party from safeguarding or reinstating his
24 rights. . . . If such factors show a substantial impairment, the inquiry turns to
25 the means and ends of the legislation. In particular, the Court has asked
26 whether the state law is drawn in an “appropriate” and “reasonable” way to
27 advance “a significant and legitimate public purpose.” *Energy Reserves*
28 *Group, Inc. v. Kansas Power & Light Co.*, 459 U.S. 400, 411–412 . . . (1983).

24 *Sveen v. Melin*, 138 S. Ct. 1815, 1821–22 (2018).

25 Plaintiffs argue that the Dealer Law “substantially impairs Plaintiffs’ existing

26
27 ⁶ At various points, Plaintiffs allege “physical” (Doc. 1 at 55), “regulatory,” *id.*, and “*per*
28 *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.

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

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

22 **4. Dormant Commerce Clause**

23 The Commerce Clause provides Congress with the power to “regulate
24 Commerce . . . among the several States” U.S. Const. art. I, § 8, cl. 3. A state statute
25 violates the so-called Dormant Commerce Clause if it “directly regulates or discriminates

26 ⁷ Defendants assert that if Plaintiffs “want to challenge whether the law can be
27 constitutionally applied to an existing contract, that would require a specific challenge to a
28 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.”

1 against interstate commerce,” *Brown-Forman Distillers Corp. v. N.Y. State Liquor Auth.*,
2 476 U.S. 573, 579 (1986), or, if a statute has only indirect effects on interstate commerce
3 and is non-discriminatory, if “the burdens of the statute so outweigh the putative benefits
4 as to make the statute unreasonable or irrational,” *UFO Chuting of Haw., Inc. v. Smith*, 508
5 F.3d 1189, 1196 (9th Cir. 2007).

6 Plaintiffs allege that the Dealer Law “imposes an undue and substantial burden on
7 interstate commerce” by requiring Plaintiffs to “change their products specifically for the
8 Arizona market” even though “DMSs are sold nationwide, and indeed some dealers have
9 operations in more than one State.” (Doc. 1 at 56.) Moreover, they argue that there is no
10 “legitimate public purpose justifying the DMS Law’s burden on interstate commerce
11 because the law inures to the sole benefit of a small class of private parties.” *Id.* But courts
12 do not engage in any “assessment of the benefits of a state law and the wisdom in adopting”
13 it until a party has shown that a state statute discriminates in favor of in-state commerce or
14 imposes a significant burden on interstate commerce. *Chinatown Neighborhood Ass’n v.*
15 *Harris*, 794 F.3d 1136, 1146 (9th Cir. 2015).

16 Plaintiffs have made no plausible allegation that the Dealer Law is discriminatory
17 in favor of Arizona commerce. As to whether the Dealer Law imposes a significant burden
18 on interstate commerce, “only a small number of cases invalidating laws under the dormant
19 Commerce Clause have involved laws that were genuinely nondiscriminatory.” *Id.*
20 Generally, such cases involve “inconsistent regulations of activities that are inherently
21 national or require a uniform system of regulation,” *Nat’l Ass’n of Optometrists &*
22 *Opticians v. Harris*, 682 F.3d 1144, 1148 (9th Cir. 2012), such as transportation or sports
23 leagues, *Chinatown*, 794 F.3d at 1146. Moreover, “Supreme Court precedent establishes
24 that there is not a significant burden on interstate commerce merely because a non-
25 discriminatory regulation precludes a preferred, more profitable method of operating in a
26 retail market”; the dormant Commerce Clause “protects the interstate market, not particular
27 interstate firms, from prohibitive or burdensome regulations.” *Nat’l Ass’n of Optometrists*,

28

1 682 F.3d at 1154, 1152. Plaintiffs have not shown that the Dealer Law regulates activities
2 that are “inherently national.” Plaintiffs Motion to Dismiss is granted as to Claim Nine.

3 **5. First Amendment Freedom of Speech**

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

5 First, Plaintiffs contend that because they are “not merely conduits facilitating the
6 transmission of information between dealers and third-party integrators,” but rather
7 “*organize[rs of]* information belonging to dealers and others in their proprietary DMSs,”
8 the Dealer Law violates the First Amendment by requiring Plaintiffs to share “information,
9 as they have organized it, with third parties.” (Doc. 50 at 36) (emphasis added). Plaintiffs
10 describe this information sharing as “compelled . . . communicat[ion].” *Id.* To the extent
11 that Plaintiffs seek protection for any copyright they have in the organization of their DMS
12 information, they have stated a claim to such protection that survives, as addressed in the
13 above Copyright Act section. However, Plaintiffs have provided no relevant authority to
14 support the claim that organization of otherwise unprotected information is subject to *First*
15 *Amendment* protection. At oral argument, Plaintiffs cited *Arkansas Educational Television*
16 *Commission v. Forbes*, 523 U.S. 666 (1998), for the provision that the First Amendment
17 protects the organization of material. *Forbes* held that a public broadcaster “engages in
18 speech activity” when it “exercises editorial discretion in the selection and presentation of
19 its programming”; however, that case is inapposite here, where, unlike the broadcaster in
20 *Forbes*, Plaintiffs’ organizational decisions do *not* result in a decision by Plaintiff as to
21 what speech to disseminate. *Forbes* dealt with the organizing broadcaster’s right to exclude
22 a candidate for federal office from a televised debate—in other words, allowing the
23 broadcaster the freedom to “speak” by running programming that did not include the
24 candidate. Here, Plaintiffs’ seek First Amendment protection not to “speak,” but to protect
25 information stored within the DMS from access by any others, relief more appropriately
26 provided—if at all—through statute. Plaintiffs’ first free speech arguments fails.

27 Plaintiffs’ second First Amendment argument is that because they will be
28 “compelled to write computer code if the Dealer Law goes into effect” and “the computer

1 code Plaintiffs must write falls within the First Amendment’s protection,” the Dealer Law
2 violates the First Amendment because it “necessarily alters the content of [Plaintiffs’]
3 speech,” demanding “exacting First Amendment scrutiny.” (Doc. 50 at 36.) Plaintiffs
4 complaint does not sufficiently allege how writing code to make unprotected information
5 accessible to third parties is subject to First Amendment scrutiny. Computer code and
6 computer programs constructed from code can constitute speech warranting First
7 Amendment protection. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449 (2d Cir.
8 2001); *see also United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1127 (N.D. Cal. 2002)
9 (“[c]omputer software is . . . speech that is protected at some level by the First
10 Amendment”). However, whether code rises to the level of speech under the First
11 Amendment depends on whether “a programmer might be said to communicate through
12 code to the user of the program (not necessarily protected)” or only “to the computer (never
13 protected).” *Corley*, 273 F.3d at 449. And even when software communicates to a user,
14 where it is “mechanical[.]” and does not involve “second-guessing” or “intercession of the
15 mind or the will of the recipient,” such code is devoid of any constitutionally protected
16 speech. *Id.* (describing the holding of *Commodity Futures Trading Comm’n v. Vartuli*, 228
17 F.3d 94 (2d Cir. 2000)).

18 The Dealer Law does not in fact mandate that a DMS provider write code. It only
19 mandates that owners of DMS systems “[a]dopt and make available a standardized
20 framework for the exchange, integration and sharing of data from [a DMS],” Ariz. Rev.
21 Stat. Ann. § 28-4654, “[p]rovide access to open application programming interfaces to
22 authorized integrators,” *id.*, and allow “third part[ies] that ha[ve] satisfied or [are]
23 compliant with the star standards or other generally accepted standards that are at least as
24 comprehensive as the star standards and that the dealer has identified as one of its
25 authorized integrators [to] integrat[e] into the dealer’s dealer data system,” Ariz. Rev. Stat.
26 Ann. § 28-4653. Given the nature of existing DMSs, it would not be surprising if the
27 implementation of these provisions required DMS providers to write code. Nevertheless,
28 as the statute makes plain, the purpose of the Dealer Law—and thus any such code—is

1 merely to facilitate the sharing of the otherwise unprotected underlying information in the
2 DMS. To the extent Plaintiffs comply with the Dealer Law by creating code, that code only
3 tells a computer how to function; it has no other expressive purpose.

4 *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000), is not to the contrary. In that case,
5 the plaintiff sought to distribute encryption source code to demonstrate how computers
6 work—code that qualified as speech because it was “an expressive means for the exchange
7 of information and ideas about computer programming.” 209 F.3d at 485. Nor is this case
8 like *Bernstein v. U.S. Dep’t of State*, 922 F. Supp. 1426, 1429 (N.D. Cal. 1996), in which
9 the regulation at issue prohibited the plaintiff’s publication of code “articulat[ing] . . .
10 mathematical ideas” so substantive they were also published in an academic paper.
11 Plaintiffs cannot plausibly argue that the Dealer Law’s regulation of Plaintiffs’ code goes
12 beyond the code’s capacity “to instruct a computer” to give third parties access to dealer
13 data, just as the *Corley* court held that the DMCA’s prohibition on posting technology for
14 circumventing DVD encryption on the internet was a functional and not a speech
15 regulation. 273 F.3d at 454. The allegations of Plaintiffs’ complaint establish that, unlike
16 in *Junger*, *Bernstein*, and *Corley*, any code Plaintiffs create pursuant to the Dealer Law
17 only instructs a computer to provide access to unprotected information contained in
18 Plaintiffs’ DMSs. Thus, as alleged in the complaint, the Dealer Law does not regulate
19 speech under the First Amendment. Plaintiffs First Amendment claim is therefore
20 dismissed. This claim is dismissed with leave to amend, if Plaintiffs wish to do so, within
21 30 days.

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

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

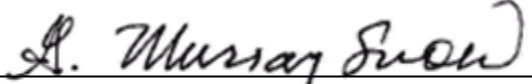
27 ///

28 ///

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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.

Dated this 20th day of May, 2020.



G. Murray Snow
Chief United States District Judge