VERMONT SUPERIOR COURT
CHITTENDEN UNIT
CIVIL DIVISION

STATE OF VERMONT, Plaintiff v. CLEARVIEW AI, INC., Defendant	Docket No. 226-3-20 Cncv

RULING ON DEFENDANT'S MOTION TO DISMISS

The State brings this consumer fraud action concerning facial recognition technology developed by Defendant Clearview AI, Inc. In this three-count complaint, the State alleges that Clearview has engaged in unfair acts and practices by collecting billions of photographs and making them available for its customers to search using facial recognition technology without the consent of those depicted, engaged in deceptive acts and practices by making material misrepresentations about its product, and fraudulently acquired brokered personal information (i.e., biometric data used to identify a consumer). The State claims that Clearview's actions violate the Vermont Consumer Protection Act (9 V.S.A. § 2453(a)) (Counts I and II) and Vermont's Fraudulent Acquisition of Data law (9 V.S.A. § 2431(a)(1)) (Count III). Clearview moves to dismiss on various grounds. Ryan Kriger, Justin Kolber, and Jill Abrams, Esqs., represent the State. Timothy Doherty, Tristram Coffin, and Tor Ekeland, Esqs. represent Clearview.[1]

[1] The State has requested oral argument on this motion. State's Opp'n at 78. Given that the State has largely prevailed on this motion, and in the interest of resolving this motion prior to the undersigned's rotation to another court, the court denies that request.

Facts

The following facts are alleged in the complaint. The court makes no finding as to their accuracy for purposes of this motion to dismiss.

Clearview, a Delaware corporation with its principle place of business in New York, is engaged in the business of identifying individuals using facial recognition technology applied to photographs. Clearview is also registered as a data broker in Vermont's Data Broker Registry. *See* 9 V.S.A. § 2446. A data broker is "a business . . . that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship." 9 V.S.A. § 2430(4).

As a small start-up company, Clearview developed facial recognition technology and, using "screen scraping" technology, amassed a database of three billion photographs. Facial recognition technology involves using computers to extract biometric identifiers from photographs based on specific features of an individual's face like relative position, size, or shape of the eyes, nose, cheekbones, and jaw. These identifiers are stored as digital "hashes" in a searchable database to quickly identify an individual based on a photograph or video. A biometric identifier is a piece of information used to authenticate an individual that is based on that person's physical or behavioral traits, for example, a fingerprint, DNA mapping, ocular scan, or an analysis of the way someone walks. Facial recognition extracts a unique, instantly searchable biometric identifier for a person, which that person cannot change absent extreme efforts. Once entered into a facial recognition database, that individual can then be picked out of a crowd by anyone using the technology.

Businesses and policy makers have been particularly cautious regarding the implementation of facial recognition technology because of the potential for misuse and

its consequences. Easily accessible facial recognition would permit governments, stalkers, predators, con artists, and others to instantly identify any stranger and, combined with other readily available data sources, know extensive details about their family, address, workplace, and other characteristics. For example, large technology companies such as Google and Facebook have declined to make a facial recognition tool commercially available, though they have the capability to do so.

Clearview collected the billions of photographs by scouring millions of websites through a process called "screen scraping." Screen scraping is a term for sending automated scripts or other processes, sometimes called "spiders," "web scrapers," or "crawlers," to collect information throughout the Internet, such as downloading photographs. It has commercialized these photographs via a service that allows the customer to upload a photograph in order to instantly identify an individual through facial recognition matching. The general public first learned of Clearview through a January 18, 2020 article in the New York Times.

The State alleges in Count I (Compl. ¶ 78) that Clearview has engaged in unfair acts and practices in commerce, in violation of the Consumer Protection Act, through the following acts:

- screen scraping billions of photographs without the consent of their owners, many of which had been uploaded subject to terms of service of web sites which limited their use;
- collecting, storing, analyzing, and distributing the photographs of minors without the consent of their parents or guardians;
- invading the privacy of consumers;
- failing to provide adequate data security for the data collected;

- exposing consumers' sensitive personal data to theft by foreign actors and criminals;
- violating consumers' civil rights by chilling their freedoms of assembly and political expression;
- violating consumers' rights as to the display and distribution of their photographs and other property rights; and
- exposing citizens to the threat of surveillance, stalking , harassment, and fraud.

In Count 2 (Compl. ¶ 81), the State alleges that Clearview has engaged in deceptive acts and practices, in violation of the CPA, by making materially false or misleading statements regarding:

- the ways that Vermont consumers can assert their privacy rights to opt out of its product;
- that Clearview's processing of consumers' personal data does not unduly affect their interests or fundamental rights and freedoms;
- the strength of its data security;
- that the product is only used by law enforcement agencies and is not publicly available;
- that it removes consumers from its database to comply with relevant laws;
- the accuracy of its facial recognition matching product; and
- its success in assisting law enforcement investigations.

Finally, in Count 3, the State alleges that Clearview's use of screen scraping technology constitutes fraudulent acquisition of brokered personal information in violation of Vermont's Fraudulent Acquisition of Data Law. Compl. ¶ 86.[2]

Discussion

Clearview's motion to dismiss is based on several grounds: (1) improper venue; (2) preemption by the federal Communications Decency Act; (3) the First Amendment; (4) that the claims are void for vagueness under the Fifth and Fourteenth Amendments; (5) failure to state a claim for a CPA violation; and (6) lack of standing. Clearview also appears to assert a Fourth Amendment argument, but the basis for that argument is unclear. Clearview's Mot. to Dismiss at 2. Clearview incorporated its memorandum opposing the State's motion for a preliminary injunction into its motion to dismiss (filed Apr. 9, 2020), making its arguments for dismissal less than crystal clear. The court uses "Clearview's Mem." to refer to that memorandum throughout this ruling.

I. Venue

Clearview contends that this case cannot be brought in Chittenden County under 9 V.S.A. § 2458(a) because it does not reside in, have a place of business in, or do business in Chittenden County. However, the State has pled that venue is proper because Clearview

[2] Clearview asks the court to disregard several paragraphs from the Complaint that, it asserts, are conclusory allegations or legal conclusions masquerading as facts. Clearview's Reply at 35–38 & n.135. The court observes that most of the cited paragraphs are proper factual allegations but, to the extent they are not, the court does not assume their truth for purposes of this motion to dismiss. Clearview also asks the court to disregard numerous paragraphs "which appear to be drawn from newspaper articles and other news reports without independent investigation as required by Rule 11." Id. at 38–41 & n.141. All statements in a pleading "shall be made subject to the obligations set forth in Rule 11." V.R.C.P. 8(e)(2). Rule 11 requires that "to the best of the person's knowledge, information, and belief, formed after an inquiry reasonable under the circumstances . . . the allegations and other factual contentions have evidentiary support . . . ." V.R.C.P. 11(b)(3). The court has no reason to believe there was a Rule 11 violation here. In any event, Clearview has not properly initiated a Rule 11 motion. *See* V.R.C.P. 11(c)(1).

does business in Chittenden County. Compl. ¶ 9. That is sufficient to survive a motion to dismiss.

II. Communications Decency Act § 230

Clearview next contends that it is protected from liability for the State's claims under section 230 of the federal Communications Decency Act, which provides in pertinent part: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1). Section 230 further provides that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." Id. § 230(e)(3).

Generally, section 230 bars plaintiffs from holding internet service providers and web hosts legally responsible for information that third parties created and developed. Johnson v. Arden, 614 F.3d 785, 791 (8th Cir. 2010); *see also* Fed. Trade Comm'n v. LeadClick Media, LLC, 838 F.3d 158, 173 (2d Cir. 2016) (noting that section 230 was enacted in response to inconsistent district court rulings concerning liability for publishing or censoring third-party defamatory statements, and "intended to . . . provide immunity for 'interactive computer service[s]' that make 'good faith' efforts to block and screen offensive content"). "Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum." Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997). "[T]he application of Section 230(c)(1) is appropriate at the pleading stage when . . . the statute's barrier to suit is evident from the face of [the] complaint." Force v. Facebook, Inc., 934 F.3d 53, 63 n.15 (2d Cir. 2019).

"In applying the statute, courts have broken [it] down into three component parts, finding that [i]t shields conduct if the defendant (1) is a provider or user of an interactive computer service, (2) the claim is based on information provided by another information content provider and (3) the claim would treat [the defendant] as the publisher or speaker of that information." Fed. Trade Comm'n v. LeadClick Media, LLC, 838 F.3d 158, 173 (2d Cir. 2016) (quotations omitted). The parties agree that Clearview is a provider or user of an "interactive computer service" under that term's broad statutory definition. *See* id. at 174; 47 U.S.C. § 230(f)(2).

However, the State's claims are not based on information provided by another information content provider. "Information content provider" means "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." 47 U.S.C. § 230(f)(3). The statute's "grant of immunity" applies "only if the interactive service provider is not also an 'information content provider' of the content which gives rise to the underlying claim." LeadClick, 838 F.3d at 174. This definition of information content provider "cover[s] even those who are responsible for the development of content only in part," FTC v. Accusearch Inc., 570 F.3d 1187, 1197 (10th Cir. 2009), however, a defendant "will not be held responsible unless it assisted in the development of what made the content unlawful." Id. at 1201; *see also, e.g.*, id. at 1199 (a defendant who paid researchers to uncover confidential phone records protected by law, and then provided that information to paying customers, fell within the definition because he did not merely act as a neutral intermediary, but instead "specifically encourage[d] development of what [was] offensive about the content"); Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1167–68 (9th Cir. 2008) (holding defendant liable

for developing content by "not merely . . . augmenting the content generally, but . . . materially contributing to its alleged unlawfulness" by requiring subscribers to provide information which enabled site users to unlawfully discriminate in selecting a roommate).

Importantly, the basis for the State's claims is not merely the photographs provided by third-party individuals and entities, or that Clearview makes those photographs available to its consumers. Instead, the claims are based on the means by which Clearview acquired the photographs, its use of facial recognition technology to allow its users to easily identify random individuals from photographs, and its allegedly deceptive statements regarding its product. *See* LeadClick, 838 F.3d at 176 (defendant "not entitled to immunity because it participated in the development of the deceptive content posted on fake news pages"). This is not simply a case of Clearview republishing offensive photographs provided by someone else, and the State seeking liability because those photographs are offensive. *See, e.g.*, Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1103 (9th Cir. 2009) (no liability for failure to "remov[e] . . . indecent profiles that [plaintiff's] former boyfriend posted on Yahoo!'s website"). Indeed, whether the photographs themselves are offensive or defamatory is immaterial to the State's claims.

Moreover, the State's claims do not treat Clearview as the publisher or speaker of the third-party photographs. "At its core, § 230 bars lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content." LeadClick, 838 F.3d at 174 (quotation omitted); *see also* Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1102 (9th Cir. 2009) ("To put it another way, courts must ask whether the duty that the plaintiff alleges the defendant violated derives from the defendant's status or conduct as a 'publisher or speaker.' If it does, section 230(c)(1) precludes liability."). Instead, the claims here

attempt to hold Clearview "accountable for its *own* unfair or deceptive acts or practices," such as screen-scraping photographs without the owners' consent and in violation of the source's terms of service, providing inadequate data security for consumers' data, applying facial recognition technology to allow others to easily identify persons in the photographs, and making material false or misleading statements about its product. LeadClick, 838 F.3d at 176 (emphasis in original); *see also* Accusearch, 570 F.3d at 1204–05 (Tymkovitch, *J.*, concurring) (noting that "the FTC sought and ultimately held [defendant] liable for its *conduct* rather than for the *content* of the information it was offering on [its] website" and arguing that there should be no immunity because "Section 230 only immunizes publishers or speakers for the *content* of the information from other providers that they make public") (emphasis in original).

The complaint here simply does not fall into the category of cases relied upon by Clearview where § 230 precluded liability. *See, e.g.*, Barnes, 570 F.3d at 1103; Marshall's Locksmith Serv. Inc. v. Google, LLC, 925 F.3d 1263, 1269 (D.C. Cir. 2019) (holding that § 230 immunized search engine for publishing false information provided by third parties); Bennett v. Google, LLC, 882 F.3d 1163, 1167–68 (D.C. Cir. 2018) (Google immune from liability under § 230 for failure to remove offensive third-party blog post); Parker v. Google, Inc., 242 F. App'x 833, 838 (3d Cir. 2007) (immunity under § 230 for linking to defamatory third-party posts); Zeran v. Am. Online, Inc., 129 F.3d 327, 332 (4th Cir. 1997) (AOL immune from liability for defamatory third-party posts on its message board service). The Communications Decency Act is not grounds for dismissal.

III. First Amendment

Clearview's next ground for dismissal is that its app (and the computer code used to write it) is protected First Amendment speech, and that the State's action amounts to

an unconstitutional regulation of that speech. The State contends that many of its claims are unrelated to speech, that the First Amendment does not protect deceptive statements, and that the Clearview app is not protected speech and, even if it were, it would survive whatever First Amendment scrutiny applied.

The First Amendment guarantees an individual the right to free speech, "a term necessarily comprising the decision of both what to say and what not to say." Riley v. National Fed'n of the Blind of North Carolina, Inc., 487 U.S. 781, 796–97 (1988). Generally, this means that "government has no power to restrict expression because of its message, its ideas, its subject matter, or its content." Bolger v. Youngs Drug Prod. Corp., 463 U.S. 60, 65 (1983) (quotation omitted). "Even dry information, devoid of advocacy, political relevance, or artistic expression, has been accorded First Amendment protection." Universal City Studios, Inc. v. Corley, 273 F.3d 429, 446 (2d Cir. 2001) (collecting cases).

Content-based speech restrictions—i.e., "those that target speech based on its communicative content"—are "presumptively unconstitutional" and subject to strict scrutiny. Reed v. Town of Gilbert, Ariz., 576 U.S. 155, 163 (2015). Content-neutral regulations that incidentally restrict speech—i.e., a law that targets the non-communicative component of conduct that includes both communicative and non-communicative elements—are subject to intermediate scrutiny. United States v. O'Brien, 391 U.S. 367, 376 (1968); City of Erie v. Pap's A.M., 529 U.S. 277, 289 (2000); Vermont Soc. of Ass'n Executives v. Milne, 172 Vt. 375, 390 (2001); City of Burlington v. New York Times Co., 148 Vt. 275, 278 (1987). However, a restriction on nonspeech or nonexpressive conduct does not implicate the First Amendment and receives only

rational basis scrutiny. *See* Arcara v. Cloud Books, Inc., 478 U.S. 697, 706–07 (1986); Sorrell v. IMS Health Inc., 564 U.S. 552, 567 (2011).

Preliminarily, the court agrees with the State that the First Amendment does not protect the alleged deceptive statements in Count II. "The First Amendment, as applied to the States through the Fourteenth Amendment, protects commercial speech from unwarranted governmental regulation." Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York, 447 U.S. 557, 561 (1980). Commercial speech is defined as "expression related *solely* to the economic interests of the speaker and its audience." Id. (emphasis added); *see also* United States v. United Foods, Inc., 533 U.S. 405, 409 (2001) (stating that commercial speech is "usually defined as speech that does no more than propose a commercial transaction"). The alleged deceptive statements in Count II are advertisement, and are therefore properly categorized as commercial speech.

However, the First Amendment does not protect false or deceptive commercial speech. "[T]he government may freely regulate commercial speech that concerns unlawful activity or is misleading." Fla. Bar v. Went For It, Inc., 515 U.S. 618, 623–24 (1995); *see also* In re Deyo, 164 Vt. 613, 614 (1995) ("For commercial speech to come within that provision, it must at least concern lawful activity and not be misleading.") (quotation omitted). Therefore, the alleged deceptive statements in Count II are not protected by the First Amendment.

The court next observes that at least some of the conduct alleged in Counts I and III is largely nonexpressive in nature. The allegations that Clearview provided inadequate data security and exposed consumers' information to theft, security breaches, and surveillance lack a communicative element. The First Amendment does not protect such conduct. *See* Nat'l Rifle Ass'n of Am. v. City of Los Angeles, 441 F. Supp. 3d 915, 928–29

(C.D. Cal. 2019) (summarizing different categories of speech and corresponding levels of scrutiny).

Whether Clearview's app is First Amendment speech presents a harder question. Courts have considered whether other forms of electronic media constitute First Amendment speech. For instance, the U.S. Supreme Court has recognized that video games are protected speech because they "communicate ideas—and even social messages—through many familiar literary devices (such as characters, dialogue, plot, and music) and through features distinctive to the medium (such as the player's interaction with the virtual world)" like the "protected books, plays, and movies that preceded them . . . ." Brown v. Entm't Merchants Ass'n, 564 U.S. 786, 790 (2011).

However, Brown does not state that all software applications are speech, and Clearview's app is not like a video game. A better analogy is found in a pair of Second Circuit cases: Commodity Futures Trading Comm'n v. Vartuli, 228 F.3d 94 (2d Cir. 2000) and Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001). In Corley, the Second Circuit considered whether posting a DVD decryption code and links to other DVD decryption codes on a website was protected First Amendment speech. The court recognized that "computer code, and computer programs constructed from code *can* merit First Amendment protection " because they have the capacity to communicate to other programmers reading the code. Id. at 449 (emphasis added). The court held that the regulation sought was content-neutral because it targeted only the code's nonspeech, functional component (i.e., its "capacity to instruct a computer to decrypt" DVDs), not its speech component (i.e., its capacity to convey information to a human being). Id. at 454, 456. The court went on to hold that the regulation survived intermediate scrutiny. Id. at 454–57. Vartuli involved a software program that told users when to buy or sell currency

futures contracts if their computers were fed currency market rates. Because this program was sold and marketed as an automatic trading system generating buy and sell instructions "in an entirely mechanical way," and to "induce action without the intercession of the mind or the will of the recipient," the court held that it was not protected speech and accordingly did not apply even intermediate scrutiny to the government's regulation. Vartuli, 228 F.3d at 111.

Because the Clearview app's raw code is not at issue here as in Corley, the app arguably has no expressive speech component and is more similar to the "entirely mechanical" automatic trading system in Vartuli that "induce[d] action without the intercession of the mind or the will of the recipient." Vartuli, 228 F.3d at 111. The user simply inputs a photograph of a person, and the app automatically displays other photographs of that person with no further interaction required from the human user. In that sense, the app might not be entitled to any First Amendment protection. Complicating matters, however, is the fact that Clearview's app is similar to a search engine, and some courts have generally recognized First Amendment protection for search engines, at least to the extent that the display and order of search results involve a degree of editorial discretion. *See* Dreamstime.com, LLC v. Google, LLC, No. C 18-01910 WHA, 2019 WL 2372280, at *2 (N.D. Cal. June 5, 2019) (collecting cases). The State would confine those cases to search engine results for text rather than photos, and also contends that Clearview's app goes far beyond what any other search engines have done.

The court need not decide whether the Clearview app is speech, however. Assuming without deciding that it is speech or at least contains a speech component, the State's attempted regulation of Clearview through this enforcement action is a permissible content-neutral regulation that survives intermediate scrutiny.

"[G]overnment regulation of expressive activity is 'content neutral' if it is justified without reference to the content of regulated speech." Hill v. Colorado, 530 U.S. 703, 720 (2000). "The government's purpose is the controlling consideration. A regulation that serves purposes unrelated to the content of expression is deemed neutral, even if it has an incidental effect on some speakers or messages but not others." Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989). "The Supreme Court's approach to determining content-neutrality appears to be applicable whether what is regulated is expression, conduct, or any 'activity' that can be said to combine speech and non-speech elements." Corley, 273 F.3d at 450 (citations omitted).

The State does not justify its action against Clearview based on the content of Clearview's speech, for example, the order of its search results or whether the photographs displayed are offensive. Instead, its purpose is based purely on the alleged function of the Clearview app in allowing users to easily identify Vermonters through photographs obtained unfairly and without consent, thereby resulting in privacy invasions and unwarranted surveillance. Presumably, the State has no problem with Clearview operating its app so long as the Vermonters depicted in its photograph database have fully consented. The regulation sought by the State here is content-neutral and, accordingly, subject to intermediate scrutiny.

Clearview maintains that the State's attempted regulation is nevertheless subject to strict scrutiny because it is "speaker-based," relying on Sorrell v. IMS Health Inc., 564 U.S. 552, 563–64 (2011) ("On its face, Vermont's law enacts content-and speaker-based restrictions on the sale, disclosure, and use of prescriber-identifying information."); *see also* Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 340–41 (2010). Clearview's reliance on Sorrell is misplaced. The statute there specifically prohibited pharmaceutical

manufacturers from using prescriber-identifying information for marketing, but allowed other speakers to obtain and use such information. Sorrell, 564 U.S. at 564. Here, the Consumer Protection Act is obviously not facially speaker-based, but Clearview complains of discriminatory enforcement. Clearview contends that the State is targeting only Clearview and none of the other search engines, and asserts that Google has also developed and patented facial-recognition technology. *See* Clearview's Reply at 41, 53. However, the State alleges that Google has not actually used that technology, Compl. ¶¶ 16–17, and that Google's image search does not display photographs from websites with terms of service that prohibit screen scraping. Id. ¶ 39. There is no basis to conclude that the State's action is a speaker-based restriction on speech.

A content-neutral restriction is permissible if it serves a substantial governmental interest, the interest is unrelated to the suppression of free expression, and the regulation is narrowly tailored, which "in this context requires . . . that the means chosen do not 'burden substantially more speech than is necessary to further the government's legitimate interests.'" Turner Broadcasting System, Inc. v. FCC, 512 U.S. 622, 662 (1994) (quoting Ward v. Rock Against Racism, 491 U.S. 781, 799 (1989)). The State plainly has a substantial governmental interest in maintaining a fair and honest commercial marketplace, and in protecting the health, welfare, and privacy of its citizens. *See* 9 V.S.A. § 2451 (stating that purposes of the Consumer Protection Act are "to protect the public and to encourage fair and honest competition"); Rubin v. Coors Brewing Co., 514 U.S. 476, 485 (1995) ("the Government . . . has a significant interest in protecting the health, safety, and welfare of its citizens"); Edenfield v. Fane, 507 U.S. 761, 769 (1993) (protecting individual privacy is a "substantial state interest"); State v. VanBuren, 2018 VT 95, ¶ 57, as

supplemented (June 7, 2019) ("The government's interest in preventing any intrusions on individual privacy is substantial.").

This interest is unrelated to the suppression of free expression. The injunction the State seeks would require Clearview to remove all images of Vermonters from its facial recognition database in order to protect their privacy and welfare, regardless of the content of those images or what information they convey. *See* Corley, 273 F.3d at 454. The State also seeks civil penalties for Clearview's allegedly unfair and deceptive acts, as permitted by the Consumer Protection Act. *See* 9 V.S.A. §§ 2431(b), 2458(a)–(b). The State seeks those penalties because of the app's function in invading Vermonters' privacy, not because of disagreement with the app's content.

Furthermore, any incidental restriction on speech imposed by the State's action would not burden substantially more speech than is necessary to further the State's interest in protecting privacy. The State estimates that the relief it requests will leave more than 99 percent of Clearview's database intact. Moreover, an injunction would presumably allow Clearview the option of obtaining affirmative consent in order to add Vermonters' images to its database. In any event, the court might need to take evidence on whether there are other, substantially less burdensome ways to further the State's interest here. Any remedies could accordingly be further tailored in light of such evidence.

Clearview also advances a slightly different First Amendment theory—that this action violates its right to access public data on the web. *See* Clearview's Mem. at 37–42; *see also* Packingham v. North Carolina, 137 S. Ct. 1730, 1732 (2017) (holding that restricting sex offenders from accessing social media sites violates First Amendment). The court finds this theory unpersuasive. None of the relief sought by the State would prohibit Clearview from accessing and viewing any particular website. Instead, the claims derive

from what Clearview does with that information, and the theory that Clearview's actions constitute unfair trade practices.

Clearview relatedly relies on a trio of federal court decisions discussing the application of the federal Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(a)(2)(C), to data scraping. *See* hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019) (involving data analytics company scraping LinkedIn's data and selling to employers interested in retaining employees); Sandvig v. Barr, No. CV 16-1368 (JDB), 2020 WL 1494065 (D.D.C. Mar. 27, 2020) (Sandvig II) (involving academic researchers' intended conduct of violating employment websites' terms of service to research whether sites discriminated based on race or gender); Sandvig v. Sessions, 315 F. Supp. 3d 1 (D.D.C. 2018) (Sandvig I). These decisions are inapposite. While those courts suggested that criminalizing data scraping and website terms of service violations might implicate the First Amendment, the decisions ultimately turned on a statutory interpretation of the CFAA, which is not at issue here. *See* hiQ Labs, 938 F.3d at 999–1004; Sandvig II, 2020 WL 1494065, at *14 ("[T]he Court concludes that plaintiffs' research plans do not violate the Access Provision of the CFAA. . . . [T]he Court need not wade into the question whether plaintiffs' proposed conduct should receive First Amendment protection."). The same is true for the other federal cases cited by Clearview. *See* Clearview's Mem. at 42 n.146 (listing cases); *see also* United States v. Valle, 807 F.3d 508, 524 (2d Cir. 2015) (explaining circuit split on CFAA statutory interpretation issue).

Moreover, dicta by the Ninth Circuit further undermines Clearview's argument. *See* hiQ Labs, 938 F.3d at 1004 ("We note that entities that view themselves as victims of data scraping are not without resort, even if the CFAA does not apply: state law trespass to chattels claims may still be available. And other causes of action, such as copyright

infringement, misappropriation, unjust enrichment, conversion, breach of contract, or *breach of privacy*, may also lie.") (emphasis added) (footnote omitted). The First Amendment does not provide grounds for dismissal here at the pleading stage.

IV. Vagueness

Clearview next argues that the Consumer Protection Act as applied here is unconstitutionally vague. "A statute is void for vagueness when it 'either forbids or requires the doing of an act in terms so vague that [persons] of common intelligence must necessarily guess at its meaning and differ as to its application.'" Kimbell v. Hooper, 164 Vt. 80, 88 (1995) (quoting Zwickler v. Koota, 389 U.S. 241, 249 (1967)); *see also* Rutherford v. Best, 139 Vt. 56, 60 (1980) (due process requires that person have fair warning of what conduct is prohibited). However, "a statute need not detail every circumstance that would amount to a violation." Kimbell, 164 Vt. at 89; *see also* State v. Pecora, 2007 VT 41, ¶ 11, 181 Vt. 627 ("the fact that the statute does not enumerate 'every act that might constitute a violation' does not render it unconstitutionally vague.") (quoting In re Illuzzi, 160 Vt. 474, 481 (1993)).

The vagueness doctrine is "based on the rationale that persons should not be chilled in their exercise of constitutional rights because of their fear of criminal sanctions." Kimbell, 164 Vt. at 88 (quotation omitted). Thus, generally, the U.S. Supreme Court has "expressed greater tolerance of enactments with civil rather than criminal penalties because the consequences of imprecision are qualitatively less severe." Sessions v. Dimaya, 138 S. Ct. 1204, 1212–13 (2018) (quotation omitted). Moreover, the court generally presumes statues to be constitutional. In re LaBerge NOV, 2016 VT 99, ¶ 18, 203 Vt. 98. A proponent of a constitutional vagueness challenge "has a very weighty burden to overcome." Id. (quotation omitted).

In prohibiting the acts of screen scraping individuals' photographs without consent and allowing users to search those photographs through facial recognition technology as unfair, the Consumer Protection Act is not unconstitutionally vague. Clearview complains that "privacy" is the primary basis for the State's action. However, the Vermont Supreme Court has at least implicitly recognized a tort for invasion of privacy, based upon "intrusion upon seclusion" and the applicable standards set forth in the Restatement. *See, e.g.*, Denton v. Chittenden Bank, 163 Vt. 62, 68–69 (1994) (supervisor's questions of employee about his illness and absence from work, although "unusual and possibly rude," were not "substantial" or "an intrusion that would be highly offensive to a reasonable person"); Hodgdon v. Mt. Mansfield Co., 160 Vt. 150, 162 (1992) ("the single letter from defendant threatening termination, although perhaps insensitive under the circumstances in this case, was insufficient to constitute an invasion of privacy") (citing Restatement (Second) of Torts § 652A).

Moreover, as stated above, a statute need not enumerate every single act that might constitute a violation. Rather, "[s]tatutory language that conveys a definite warning as to proscribed conduct when measured by common understanding and practices will satisfy due process." In re Palmer, 171 Vt. 464, 472 (2000) (quoting Brody v. Barasch, 155 Vt. 103, 111 (1990)). Clearview suggests that it lacked fair warning without a specific statute or regulation prohibiting screen scraping and applying facial recognition technology to those photos. This court rejected a similar argument earlier this year, in a case alleging price-gouging of personal protective equipment:

> The fact that there is not a precise statute or declaration directly discussing PPEs is not relevant. If a separate law or executive order was required to find a particular practice unfair under the Act, the Act would have little meaning. Moreover, the Sperry case expressly rejected the argument,

> concluding that in determining what is "unfair" the FTC may "consider[] public values beyond simply those enshrined in the letter or encompassed in the spirit of" other laws.

State v. Big Brother Security Programs, No. 326-4-20 Cncv, slip copy at 12 (Apr. 27, 2020) (Ex. A to Pl.'s Opp'n to Def.'s Mot. to Dismiss) (quoting F.T.C. v. Sperry & Hutchinson Co., 405 U.S. 233, 244 (1972)).

As the State recognizes, consumer protection statutes have been applied to numerous specific behaviors that are not specifically enumerated in a particular statute or regulation. *See, e.g.*, McDonald v. Kiloo ApS, 385 F. Supp. 3d 1022, 1029 (N.D. Cal. 2019) (gaming app collecting user data for geo-targeted advertising). It would make no sense for the legislature to have to pass a new law as soon as any new technology is invented and brought to market. Such a requirement would defeat the broad, proscriptive purpose of the Consumer Protection Act. *See* Fed. Trade Comm'n v. Raladam Co., 316 U.S. 149, 152 (1942) ("One of the objects of the Act creating the Federal Trade Commission was to prevent potential injury by stopping unfair methods of competition in their incipiency."). Clearview had fair notice that its alleged conduct implicates privacy interests and might reasonably be considered "unfair" under the Act. Clearview has not met its "very weighty burden" to demonstrate that the Act as applied is unconstitutionally vague.

V. Vermont Consumer Protection Act and Fraudulent Acquisition of Data Law

Clearview contends that the complaint fails to state a claim under the Consumer Protection Act and the Fraudulent Acquisition of Data law pursuant to V.R.C.P. 12(b)(6). Both laws prohibit "unfair or deceptive acts or practices in commerce." 9 V.S.A. § 2453(a); id. § 2431(b)(1). Essentially, Clearview argues that the conduct alleged in Count I is not

"unfair," that the conduct alleged in Count II is not "deceptive," and that the conduct alleged in Count III does not constitute a fraudulent acquisition of brokered personal information and, consequently, is not an unfair or deceptive act or practice.[3]

A. Unfairness

There are three factors courts generally consider in deciding whether a practice is unfair under the Consumer Protection Act:

> (1) whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise whether, in other words, it is within at least the penumbra of some common-law, statutory, or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive or unscrupulous; (3) whether it causes substantial injury to consumers . . . .

Christie v. Dalmig, Inc., 136 Vt. 597, 601 (1979) (quoting F.T.C. v. Sperry & Hutchinson Co., 405 U.S. 233, 244 n.5 (1972)). To the extent Clearview argues that all three factors must be satisfied or that the "substantial injury" factor in particular must be satisfied in all cases, this court has already concluded in a previous case that the factors are independent. *See* State v. Big Brother Security Programs, No. 326-4-20 Cncv, slip copy at 9–10 (Apr. 27, 2020) (Ex. A to Pl.'s Opp'n to Def.'s Mot. to Dismiss). Moreover, numerous other courts have concluded similarly. *See, e.g.*, Wendorf v. Landers, 755 F. Supp. 2d 972, 979 (N.D. Ill. 2010) ("The Illinois Supreme Court has interpreted Sperry to impose only a factor-based framework, not a three-part conjunctive test"); Ramirez v. Health Net of Ne., Inc, 938 A.2d 576, 589 (Conn. 2008) ("All three criteria do not need to be satisfied to support a finding of unfairness. A practice may be unfair because of the degree to which

[3] To the extent it is relevant to the motion to dismiss, the court rejects as entirely unpersuasive Clearview's suggestion that the State's action is preempted by 23 V.S.A. § 634(c). *See* Clearview's Mem. at 67–68.

it meets one of the criteria or because to a lesser extent it meets all three."); Morrison v. Toys "R" Us, Inc., 806 N.E.2d 388, 392 (Mass. 2004) (same); Rohrer v. Knudson, 203 P.3d 759, 764 (Mont. 2009) ("We hold as a matter of law that an unfair act or practice is one which offends established public policy and which is either immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers.").

Here, the State has adequately alleged, at the very least, the first two factors. It alleges that Clearview's acts offend public policy as it relates to the privacy of Vermont consumers. Compl. ¶ 77. As to the public policy factor, the FTC specified that

> the policies relied upon "should be clear and well-established"—that is, "declared or embodied in formal sources such as statutes, judicial decisions, or the Constitution as interpreted by the courts, rather than being ascertained from the general sense of the national values." Put another way, an act or practice's "unfairness" must be grounded in statute, judicial decisions—*i.e.*, the common law—or the Constitution.

LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1229 (11th Cir. 2018) (citation omitted). Privacy as a public policy is embodied in numerous Vermont and non-Vermont judicial decisions. As noted above, the Vermont Supreme Court has at least implicitly recognized a tort for invasion of privacy, based upon "intrusion upon seclusion" and the applicable standards set forth in the Restatement. *See, e.g.*, Denton v. Chittenden Bank, 163 Vt. 62, 68–69 (1994) (supervisor's questions of employee about his illness and absence from work, although "unusual and possibly rude," were not "substantial" or "an intrusion that would be highly offensive to a reasonable person"); Hodgdon v. Mt. Mansfield Co., 160 Vt. 150, 162 (1992) ("the single letter from defendant threatening termination, although perhaps insensitive under the circumstances in this case, was insufficient to constitute an invasion of privacy") (citing Restatement (Second) of Torts § 652A). The Court has also recognized that "[t]he government's interest in preventing

any intrusions on individual privacy is substantial." State v. VanBuren, 2018 VT 95, ¶ 57, as supplemented (June 7, 2019).[4]

As the cases cited by the State amply demonstrate, many courts outside of Vermont have recognized privacy rights in the context of emerging technology. "Technological advances provide access to a category of information otherwise unknowable, and implicate privacy concerns in a manner as different from traditional intrusions as a ride on horseback is different from a flight to the moon." Patel v. Facebook, Inc., 932 F.3d 1264, 1272–73 (9th Cir. 2019) (collecting recent U.S. Supreme Court cases recognizing privacy implications of sense-enhancing thermal imaging, GPS monitoring, cell phone storage of personal information, and tracking of cell-site location information). *See also, e.g.*, id. at 1273 ("We conclude that the development of a face template using facial-recognition technology without consent (as alleged here) invades an individual's private affairs and concrete interests. Similar conduct is actionable at common law."); Opperman v. Path, Inc., 84 F. Supp. 3d 962, 992–93 (N.D. Cal. 2015) (accessing and misusing phone and app purchasers' address and contacts lists without consent); McDonald v. Kiloo ApS, 385 F. Supp. 3d 1022, 1029 (N.D. Cal. 2019) (gaming app covertly collecting user data for

[4] Clearview contends that VanBuren undermines the State's privacy argument. Clearview's Mem. at 48–51. VanBuren involved a criminal prosecution for the unconsented disclosure of an intimate image of the complainant under Vermont's relatively new "revenge porn" statute. The Court affirmed the dismissal of the charge because "the State has not established that it has evidence showing that complainant had a reasonable expectation of privacy in the images she sent to" the intended recipient, necessary to prove an element of the crime. VanBuren, 2018 VT 95, ¶ 97. Clearview's argument about VanBuren is unpersuasive. First, VanBuren was a criminal case, deciding whether the State could prove an element of the charged crime (beyond a reasonable doubt). It did not hold that individuals have no privacy interests whatsoever in photos they post on any digital platform. Second, VanBuren involved merely republishing a photo, while Clearview's alleged conduct (extracting biometric data and adding the photos to a searchable database for easy identification) goes beyond mere republication. Finally, whereas the VanBuren Court noted that the State offered no "evidence of any promise by [intended recipient], or even express request by complainant, to keep the photos confidential," or any other basis from which the complainant could "reasonably assume that he would not share the photos she sent with others," id. ¶ 106, many social media sites to which consumers post photos have terms of service policies that expressly prohibit screen scraping. Compl. ¶¶ 38–39, 43. Those terms of service provide a reasonable basis for consumers to assume that their photos would not be scraped and used in a facial recognition search engine without their consent.

geo-targeted advertising). The invasion of privacy alleged here is "within at least the penumbra of some common-law, statutory, or other established concept of unfairness." Christie, 136 Vt. at 601; *see also* LabMD, 894 F.3d 1221, 1229 ("an act or practice's 'unfairness' must be grounded in . . . judicial decisions—i.e., the common law").

The State also sufficiently alleges that Clearview's conduct is "immoral, unethical, oppressive or unscrupulous." Christie, 136 Vt. at 601; *see also* Compl. ¶ 77. Courts have described such conduct as that which "imposes a lack of meaningful choice," Centerline Equip. Corp. v. Banner Pers. Serv., Inc., 545 F. Supp. 2d 768, 780 (N.D. Ill. 2008), or that involves a lack of consent. Votto v. Am. Car Rental, Inc., 871 A.2d 981, 985 (Conn. 2005) ("The defendant's use of the plaintiff's signature on a blank credit card slip to charge the plaintiff more than twice the amount of the estimated cost of repair to the vehicle was without question unscrupulous, immoral and oppressive."). Clearview's alleged collection of and application of facial recognition technology to Vermonters' photographs without their consent plainly falls within this standard. While it remains to be seen whether the State can prove unfairness at trial, the allegations in the complaint are sufficient to survive a motion to dismiss.

Even assuming the State also had to allege substantial injury, the complaint would still suffice to move past the pleading stage. Clearview correctly observes that, in deciding whether an act or practice is "unfair or deceptive" under the Consumer Protection Act, "the courts of this State will be guided by the construction of similar terms contained in Section 5(a)(1) of the Federal Trade Commission Act [9 U.S.C. § 45] as from time to time amended by the Federal Trade Commission and the courts of the United States." 9 V.S.A. § 2453(b). Notably, however, the provision of the FTC Act on which Clearview relies provides in part:

> The Commission shall have no authority under this section . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes *or is likely to cause substantial injury* to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

15 U.S.C. § 45(n) (emphasis added). Based on a fair reading of the complaint, the State alleges that Clearview's conduct is at least "likely to cause substantial injury" by exposing Vermonters to unwanted surveillance and through Clearview's marketing of its product to law enforcement. Clearview's argument that consumers can reasonably avoid such injury by not uploading photographs of themselves online is spurious at best. It is a matter of common knowledge that a significant portion of the population has uploaded photographs or (often unwittingly) appeared in photographs uploaded by others. *See* Compl. ¶ 45. Further, the court cannot conclude from the complaint alone whether such injury is "outweighed by countervailing benefits to consumers." 15 U.S.C. § 45(n).

B. Deception

Count II alleges several deceptive statements by Clearview. To establish a "deceptive act or practice" under the Consumer Protection Act requires three elements: "(1) there must be a representation, omission, or practice likely to mislead consumers; (2) the consumer must be interpreting the message reasonably under the circumstances; and (3) the misleading effects must be material, that is, likely to affect the consumer's conduct or decision regarding the product." Carter v. Gugliuzzi, 168 Vt. 48, 56 (1998). "Deception is measured by an objective standard, looking to whether the representation or omission had the capacity or tendency to deceive a reasonable consumer; actual injury need not be shown." Id. at 56 (quotation omitted).

Clearview first argues that Vermonters are not "consumers" since they did not purchase the app, and that only law enforcement, financial institutions, and security companies are purchasers and, thus, consumers in this context. Because the users of the app are not the people allegedly harmed—the Vermont public whose photos are used—Clearview contends that the Act is inapplicable. Therefore, Clearview asserts, the deception claim fails. The court rejects this argument. First, the Act includes a specific definition of "consumer" that is limited to purchasers, 9 V.S.A. § 2451a(a), but that applies to private actions brought by individuals under § 2461(b); it does not somehow limit the State's enforcement rights under § 2458. No Vermont cases say that, to be actionable, deceptive statements must have caused direct harm to an actual or would-be *purchaser* of the product or service in question.

Second, the FTC has brought actions against companies whose deceptive conduct allegedly misled non-purchasers of those companies' products or services, indicating that the FTC does not interpret the FTC Act to include such a "purchaser" requirement. *See, e.g.*, In re Epic Marketplace, No. C-4389 (F.T.C. Mar. 13, 2013), available at https://www.ftc.gov/enforcement/cases-proceedings/112-3182/epic-marketplace-inc (online advertising company used "history sniffing" to secretly and illegally gather data from millions of consumers' web-browsing histories); FTC v. Equifax, No. 1:19-cv-03297-TWT (N.D. Ga. July 23, 2019), available at: https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc (credit reporting agency failed to secure personal information of millions of consumers stored on its network, leading to security breach that exposed information to identify theft and fraud).

Moreover, the Consumer Protection Act is to be construed "liberally . . . in light of its remedial purposes." Anderson v. Johnson, 2011 VT 17, ¶ 7, 189 Vt. 603. It is "designed

not merely to compensate consumers for actual monetary losses resulting from fraudulent or deceptive practices in the marketplace, but more broadly to protect citizens from unfair or deceptive acts in commerce, and to encourage a commercial environment highlighted by integrity and fairness." Id. (citation and quotations omitted). Under Clearview's logic, the State could never enforce the Act against patently false advertising so long as no person had yet been duped into buying the advertised product or service. Such a result is untenable, especially since "actual injury need not be shown." Carter, 168 Vt. at 56.

Next, Clearview contends that the State has not adequately pled that each of the alleged statements in Count II were deceptive and material, and that some of those statements are mere opinion or commercial puffery rather than objective fact. The complaint lists seven allegedly deceptive statements.

1. Opt-Out Rights

In the privacy policy on its website, Clearview makes the following statement concerning consumers' privacy rights: "Users and members of the public are entitled to . . . The right to erasure – You have the right to request that we erase your personal data under certain conditions." Compl. ¶ 56. The policy goes on to clarify that this right is "subject to limitations that vary by jurisdiction. We will honor such requests . . . as required under applicable data protection rules but these rights are not absolute: they do not always apply and exemptions may be engaged." Id. The State alleges that the data protection rights listed are actually from the European Union's General Data Protection Regulation, which is not applicable to U.S. citizens, and that the only state law that comes close to this is California's consumer privacy act. Id. ¶ 58. Clearview argues that this statement is technically accurate, but the State alleges that this policy "creates a

reasonable belief in any Vermont consumer who is not a privacy law scholar that they can take some action to protect their privacy" concerning data stored by Clearview. Id. ¶ 58.

The Vermont Supreme Court has "distinguished statements of fact from statements of opinion in the consumer-fraud context, holding that misrepresentations of the former may constitute fraud while misrepresentations of the latter cannot." Heath v. Palmer, 2006 VT 125, ¶ 14, 181 Vt. 545. Representations about the status of the law are generally considered nonactionable, but the Court has recognized that "[a]n important distinction must be made between representations of legal *opinions* and representations of *fact* relating to the law as it exists." Winton v. Johnson & Dix Fuel Corp., 147 Vt. 236, 240 (1986) (emphasis in original). Legal opinions "involve[] the legal meaning and effect of a statute, court ruling, document, instrument or other source of law," while factual representations about the law "involve[] statements that imply the existence of accurate and readily ascertainable facts that either concern the law or have legal significance, but which are not part of the law themselves." Id. at 240. Such legal facts "may imply the existence or non-existence of an applicable statute, regulation, or judicial decision, and this is one kind of external fact which may seem very important to the person addressed by the statement." Id. at 241 (statements in hot water heater advertisement that emphasized availability of state energy tax credit were "fashioned as facts, rather than opinions about the application of the law" and therefore actionable under Consumer Fraud Act); *see also* Webb v. Leclair, 2007 VT 65, ¶ 22, 182 Vt. 559.

The alleged statement involves an "objectively verifiable statement of fact," that is, whether consumers have a right to have their data erased, rather than a subjective "opinion." Heath, 2006 VT 125, ¶ 14. To the extent it involves a component of legal status, it is a representation of fact regarding the law as it exists, rather than a legal opinion.

Winton, 147 Vt. at 240. While the policy's statements might not be literally false and might not be so clear as the statement in Winton, Clearview could have presented the policy in a less misleading manner, for example, by making it clear that these opt-out "rights" in fact do not apply to most U.S. citizens. The complaint sufficiently alleges that these statements could mislead a reasonable consumer regarding their ability to opt out of Clearview's product.

2. Affect on Consumers' Interests or Fundamental Rights and Freedoms

Clearview's privacy policy also states: "We are not allowed to process personal data if we do not have a valid legal ground. Therefore, we will only process personal data if . . . the processing is necessary for the legitimate interests of Clearview, and does not unduly affect your interests or fundamental rights and freedoms." Compl. ¶ 59. The State alleges that this statement is false because "Clearview's processing does very much unduly affect consumers' interests and fundamental rights and freedoms." Id. ¶ 60. Essentially, this statement amounts to a legal conclusion or opinion about whether Clearview's alleged unfair acts as stated in Count I implicate consumers' privacy rights. It goes far beyond a mere assertion that a particular statute does or does not exist or apply. *See* Winton, 147 Vt. at 240–41. Moreover, as it would require a resolution on the merits of Count I, it was not objectively verifiable at the time the statement was made. Consequently, this statement does not constitute a deceptive act under the Consumer Protection Act. *See generally* Heath, 2006 VT 125, ¶ 14.

3. Strength of Data Security

Clearview's privacy policy also includes a paragraph with assertions about the strength of the data security technology it uses to protect personal information. Compl. ¶ 61. While parts of this paragraph undoubtedly constitute vague commercial puffery, other parts plainly consist of facts capable of objective analysis, likely by computer security experts. This statement could lead a reasonable consumer to believe that Clearview's stored personal data is completely secure. Id. ¶ 62. The complaint sufficiently alleges a deceptive statement regarding the strength of Clearview's data security. Compl. ¶¶ 63–68.

4. Use by Law Enforcement and Public Availability

In its "User Code of Conduct," Clearview states that users may use its app for only "legitimate law enforcement and security purposes," and not for "personal purposes." Compl. ¶ 69. Clearview also states on its website that its app is not available to the public. Id. ¶ 30. However, the State alleges that this is not true because Clearview has provided access to its app to numerous for-profit corporations, universities, investors, reporters, and governments in dozens of countries, and has not limited its use to authorized users even in the law enforcement context. Id. ¶¶ 31–32. Furthermore, in private marketing statements, Clearview has allegedly told users to use the app on friends and family and to "feel free to run wild with your searches." Id. ¶¶ 33, 70. The complaint fairly alleges that Clearview's statements about law enforcement use and the public availability of its app are deceptive.

5. Removal of Consumer Data from Database

Clearview has allegedly claimed or implied that it removes consumer data from its database to comply with existing law. Compl. ¶¶ 50, 56, 81(e). However, the State alleges

that Clearview does not yet have the capability to remove individuals by geographic region or age. Id. ¶ 51. This plainly states a claim for a deceptive act.

6. Accuracy of Matching Technology

According to the State's allegations, Clearview has claimed (1) an accuracy rate of 98.6% to 99.6% for its photograph matching technology without providing any evidence or a standard benchmark, and (2) an accuracy rate of 100% according to the ACLU's methodology which it then retracted after the ACLU complained that Clearview had not properly applied its technology and called Clearview's claim "absurd." Compl. ¶¶ 71–72. Clearview also has allegedly not provided its matching algorithm for testing to the only entity that provides public testing of facial recognition technology. Id. ¶ 73. These allegations state a claim for deceptive statements regarding the accuracy of Clearview's matching technology. Clearview provides an affidavit asserting that it has tested its technology's accuracy using the Megaface benchmark test. Clearview's Mem. at 66 n.231. That may be so, but the court cannot consider an affidavit on a motion to dismiss.

7. Success in Assisting Law Enforcement Investigations

According to the complaint, Clearview claimed to have assisted the NYPD in solving several cases, but the NYPD denied that Clearview was used in any of those cases. Compl. ¶¶ 74–75. This also is sufficient to survive a motion to dismiss.

Moreover, all of the alleged statements described above are material in that they are "likely to affect [a] consumer's conduct or decision regarding the product," Carter, 168 Vt. at 56, at least for purposes of the motion to dismiss. The State does not allege a de minimus misrepresentation such as, for example, if Clearview claimed to have a 95.3% accuracy rate when the actual rate was 95.2%. Such an insignificant deception would not reasonably affect a consumer's conduct regarding the product. The alleged deceptions

here, however, are significant, and are reasonably likely to affect the conduct of either law enforcement or the general public with respect to Clearview's app.

C. Vermont's Fraudulent Acquisition of Data Law

Vermont's Fraudulent Acquisition of Data law prohibits the acquisition of "brokered personal information through fraudulent means." 9 V.S.A. § 2431(a)(1). A violation of this law constitutes "an unfair and deceptive act in commerce in violation of [9 V.S.A. §] 2453." Id. § 2431(b)(1). "Brokered personal information" means "computerized data elements about a consumer, if categorized or organized for dissemination to third parties," including "unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data." Id. § 2430(1)(A)(vi).[5] For purposes of this statute, "consumer" means "an individual residing in this State." Id. § 2430(3).

Clearview asserts that this law does not apply because the data it acquires is "not brokered" and "not acquired by fraud." Clearview's Mem. at 68. The data it acquires plainly falls within the statutory definition of "brokered personal information." 9 V.S.A. § 2430(1)(A)(vi). However, the complaint does not adequately allege that the data was acquired by fraudulent means. The court disagrees with the State's contention that, in this context, "fraud" refers to consumer fraud, i.e., an unfair or deceptive act or practice in commerce. While the statute does not explicitly define "fraud," and the legislature's

[5] The definition also includes "other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty." 9 V.S.A. § 2430(a)(ix).

statement of findings and intent unsurprisingly provides little assistance in that regard, *see* 2017, No. 171, § 1, the court concludes that "fraud" here means fraud in the traditional or common law sense, rather than in the "consumer fraud" sense. The statute would simply make no sense otherwise. That a fraudulent acquisition of brokered personal information constitutes "an unfair and deceptive act in commerce in violation of" the Consumer Protection Act does not also mean that any variation of "consumer fraud" necessarily constitutes acquisition of "brokered personal information through fraudulent means." Id. § 2431(a)(1).[6] That is circular reasoning that would render the Fraudulent Acquisition of Data law meaningless. Under that logic, the law would proscribe virtually no conduct beyond that also proscribed by the Consumer Protection Act.[7]

Fraud traditionally requires some form of misrepresentation. Ianelli v. U.S. Bank, 2010 VT 34, ¶ 14 n.*, 187 Vt. 644 (mem.). The complaint, however, alleges no such misrepresentation with respect to Clearview's acquisition of the data. The State argues in its memorandum that Clearview's "indiscriminate screen-scraping . . . involved using spiders that misrepresented their purpose in accessing websites," State's Opp'n at 71, yet alleges nowhere in the complaint that Clearview's "spiders" actually misrepresented their purpose. It argues that Clearview violated the terms of service of the websites it scraped, yet the complaint is devoid of any allegation that Clearview actually misrepresented its

---

[6] Notably, several years before the Fraudulent Acquisition of Data law was added in 2018, the legislature changed the title of the "Consumer Fraud Act" to "Consumer Protection Act" in 2012. *See* 2011, No. 109, § 3 ("Redesignation of term 'consumer fraud' to read 'consumer protection'"); McKinstry v. Fecteau Residential Homes, Inc., 2015 VT 125, ¶ 4 n.1, 200 Vt. 392. This makes it even less likely that the legislature's intent behind using the term "fraud" in section 2431(a)(1) was to refer to "consumer fraud" rather than common law fraud.

[7] The Attorney General's own guidance about this law suggests that acquisition by "fraudulent means" refers to common law fraud. *See* Vermont Office of the Attorney General, Guidance on Vermont's Act 171 of 2018 Data Broker Regulation at 11 (Dec. 11, 2018) ("The concepts of fraud, stalking and harassing, identity theft, and unlawful discrimination are addressed in the common law and other statutes.") (available at: https://perma.cc/BK6G-YBHH).

purpose in accessing the websites rather than merely contravening the terms of service. The State also argues that Clearview collected personal photos without consumers' knowledge or consent "in order to turn those photographs against their owners through the use of facial recognition." Id. Again, no allegation of misrepresentation in the complaint supports this argument. Clearview's actions in acquiring the photos is akin to someone walking into a store and surreptitiously stealing an item. In that example, the person's action might be larceny and it might violate the store's posted rules, but it is not fraud because it does not involve a misrepresentation. Moreover, the post-acquisition use of those photographs is immaterial to Count III, which asserts that Clearview acquired brokered personal information by fraudulent means under 9 V.S.A. § 2431(a)(1), not that it "acquire[d] or use[d] brokered personal information for the purpose of" stalking, harassment, committing a fraud, or engaging in unlawful discrimination under § 2431(a)(2).

The court could imagine how the deceptive statements alleged in Count II might support the alleged fraudulent acquisition of data in Count III by inducing someone to continue posting photographs on social media, or to refrain from deleting their photographs from social media. However, that would depend on the deceptive statements being presented before the screen scraping began, so that consumers would have time to act on those statements. There is no such information in the complaint concerning the dates the deceptive statements were made and when the screen scraping began, nor does the State allege that a Clearview misrepresentation induced anyone to make their photographs available for Clearview's acquisition.

It appears that this is the first time the Fraudulent Acquisition of Data Law—which went into effect in 2019 and is apparently the first of its kind in the country—has been

discussed or construed in a court decision. *See generally* Note, The Federalist Regulation of Privacy: The Happy Incidents of State Regulatory Activity and Costs of Preemptive Federal Action, 84 Mo. L. Rev. 1055, 1073–75 and nn.130, 138–43 (2019). As this court has recognized many times, "[a] motion to dismiss . . . is not favored and [is] rarely granted[,] . . . especially . . . when the asserted theory of liability is novel or extreme," as such cases "should be explored in the light of facts as developed by the evidence, and, generally, not dismissed before trial because of the mere novelty of the allegations." Alger v. Dep't of Labor & Indus., 2006 VT 115, ¶ 12, 181 Vt. 309 (citation and quotations omitted). "Nonetheless, where the plaintiff does not allege a legally cognizable claim, dismissal is appropriate." Montague v. Hundred Acre Homestead, LLC, 2019 VT 16, ¶ 11, 209 Vt. 514. Because the State has not sufficiently alleged that the data was acquired by "fraudulent means," dismissal of Count III is appropriate.

VI. Standing

Finally, Clearview contends that the State lacks standing to bring this action. Typically, the standing doctrine requires that a plaintiff "must have suffered a particular injury that is attributable to the defendant and that can be redressed by a court of law." Paige v. State, 2018 VT 136, ¶ 8, 209 Vt. 379 (quotation omitted). However, the standing analysis is different when the plaintiff is a sovereign state rather than a private individual. Massachusetts v. E.P.A., 549 U.S. 497, 518 (2007). The U.S. Supreme Court has recognized that where the state has a procedural right to bring that action and a "stake in protecting its quasi-sovereign interests, the [state] is entitled to special solicitude in our standing analysis." Id. at 520–21 & n.17 (Massachusetts has quasi-sovereign standing to challenge EPA's refusal to regulate greenhouse gas emissions).

The State asserts that it has such standing under the "*parens patriae*" doctrine. "[T]o have such standing the State must assert an injury to . . . a 'quasi-sovereign' interest," an admittedly vague judicial construct with no "simple or exact definition. Its nature is perhaps best understood by comparing it to other kinds of interests that a State may pursue and then by examining those interests that have historically been found to fall within this category." Alfred L. Snapp & Son, Inc. v. Puerto Rico, ex rel., Barez, 458 U.S. 592, 601 (1982). Quasi-sovereign interests generally "consist of a set of interests that the State has in the well-being of its populace." Id. at 602. The Court has summarized the doctrine as follows:

> In order to maintain such an action, the State must articulate an interest apart from the interests of particular private parties, *i.e.*, the State must be more than a nominal party. The State must express a quasi-sovereign interest. Although the articulation of such interests is a matter for case-by-case development—neither an exhaustive formal definition nor a definitive list of qualifying interests can be presented in the abstract—certain characteristics of such interests are so far evident. These characteristics fall into two general categories. First, a State has a quasi-sovereign interest in the health and well-being—both physical and economic—of its residents in general. Second, a State has a quasi-sovereign interest in not being discriminatorily denied its rightful status within the federal system.

Id. at 607. Additionally, the State must "allege[] injury to a sufficiently substantial segment of its population." Id.

The State has a clear procedural right to bring this action. The Consumer Protection Act prohibits "unfair or deceptive acts or practices in commerce." 9 V.S.A. § 2453(a). "Whenever the Attorney General . . . has reason to believe that any person is using or is about to use any method, act, or practice declared by section 2453 . . . to be unlawful, . . . and that proceedings would be in the public interest," he may "bring an

action in the name of the State against such person to restrain by temporary or permanent injunction the use of such method, act, or practice . . . ." 9 V.S.A. § 2458(a).

The State also has quasi-sovereign interests in protecting a fair and honest marketplace from deceptive advertising statements, and in avoiding societal harm from mass surveillance. Mass surveillance could reasonably chill citizens' freedoms of assembly and political expression. *See* Compl. ¶ 78. These interests go beyond those of any individual party, and courts have recognized these interests as sufficient to confer standing. *See* People ex rel. Cuomo v. Liberty Mut. Ins. Co., 861 N.Y.S.2d 294, 296 (N.Y. App. Div. 2008) ("the Attorney General sued to redress injury to its quasi-sovereign interest in securing an honest marketplace for all consumers") (quotation omitted); State ex rel. Hatch v. Cross Country Bank, Inc., 703 N.W.2d 562, 569 (Minn. Ct. App. 2005) ("The state . . . is pursuing its claim[] not with the purpose of obtaining relief for particular victims, but to vindicate a 'quasi-sovereign' interest: protecting the privacy of its citizens."); State of N. Y. by Abrams v. Gen. Motors Corp., 547 F. Supp. 703, 705 (S.D.N.Y. 1982) ("The State's goal of securing an honest marketplace in which to transact business is a quasi-sovereign interest."); Kelley v. Carr, 442 F. Supp. 346, 356–57 (W.D. Mich. 1977), aff'd in part, rev'd in part, 691 F.2d 800 (6th Cir. 1980) ("Surely some of the most basic of a state's quasi-sovereign interests include . . . protection of its citizens from fraudulent and deceptive practices [and] support for the general welfare of its residents and its economy . . . .").

Moreover, the State estimates that millions of photographs of Vermonters may be part of Clearview's database, State's Opp'n at 75, a reasonable implication from the complaint. *See* Compl. ¶¶ 24–25, 44, 47–49. This surely constitutes a substantial segment of Vermont's population. "This is not a case in which the state is gratuitously attempting

to prosecute purely personal claims of its citizens, but rather is one in which the state is seeking to protect the public interest." Kelley, 442 F. Supp. at 357. Given the lower bar for standing at the pleading stage, the complaint adequately alleges sufficient facts to confer standing on the State as *parens patriae* in this action. *See* Connecticut v. Am. Elec. Power Co., 582 F.3d 309, 333 (2d Cir. 2009), rev'd on other grounds, 564 U.S. 410 (2011); *see also* 13B Wright & Miller, Fed. Prac. & Proc. Juris. § 3531.11.1 (3d ed.) ("There can be no doubt whatever that in its own courts and under its own law, a state has standing to enforce broad concepts of the public interest against individual defendants, whether through criminal or civil proceedings.").

Order

Clearview's motion to dismiss is granted as to one of the deceptive statements alleged in Count I—specifically paragraph 81(b) of the complaint—and as to Count III. The motion is denied in all other respects. The parties shall proceed with scheduling according to the court's May 6, 2020 order.

Dated at Burlington this 4th day of September, 2020.

Helen M. Toor
Superior Court Judge