VERMONT SUPERIOR COURT
FILED

SEP 10 2020

CHITTENDEN UNIT

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.