IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

MATTHEW STRAUBMULLER, individually and on behalf of all others similarly situated,	:	
v.	:	Civil Action No. DKC 23-384
JETBLUE AIRWAYS CORP.	:	

MEMORANDUM OPINION

Presently pending and ready for resolution is the motion to dismiss filed by Defendant Jetblue Airways Corporation. (ECF No. 11). The issues have been briefed, and the court now rules, no hearing being deemed necessary. Local Rule 105.6. For the following reasons, the motion to dismiss will be granted.

I. Background

The following facts are alleged in the Complaint. (ECF No. 1). Defendant is an airline offering domestic and international flights. (ECF No. 1 ¶ 38). Defendant operates the website www.jetblue.com. (ECF No. 1 ¶ 38). Defendant procures and embeds various Session Replay Codes from third-party Session Replay Providers on Defendant's website to track and analyze user interactions with the website. (ECF No. 1 ¶¶ 39-40).

Session Replay Code enables website operators to record, save, and replay website visitors' interactions with a given

website, including "mouse movements, keystrokes (such as text being entered into an information field or text box), URLs or web pages visited, and/or other electronic communications in real-time." (ECF No. 1 ¶¶ 1, 22). Website operators can then view a visual reenactment of the user's visit through the Session Replay Provider, typically in the form of a video. (ECF No. 1 ¶ 27).

Plaintiff Matthew Straubmuller visited Defendant's website, at which time his interactions with the website were captured by Session Replay Code and sent to various Session Replay Providers. (ECF No. 1 ¶¶ 44-47).

On February 10, 2023, Plaintiff filed a complaint, on behalf of himself and others similarly situated, against Defendant. In Count I, the Complaint alleges that Defendant violated the Maryland Wiretapping and Electronic Surveillance Act ("MWESA"), Md. Code Ann., Cts. & Jud. Proc. § 10-401, by intercepting Plaintiff's electronic communications with Defendant's website without consent. (ECF No. 1 ¶ 78). In Count II, the Complaint alleges that Defendant's conduct also constitutes an invasion of privacy and intrusion upon seclusion. (ECF No. 1 ¶ 3). On April 17, 2023, Defendant moved to dismiss the Complaint for lack of subject matter jurisdiction, Fed.R.Civ.P. 12(b)(1), lack of personal jurisdiction, Fed.R.Civ.P. 12(b)(2), and failure to state a claim, Fed.R.Civ.P. 12(b)(6). (ECF No. 11). On May 1, 2023, Plaintiff

responded in opposition (ECF No. 14), and on May 15, 2023, Defendant replied (ECF No. 19).

II. Standard of Review

The issue of standing may be challenged on a motion to dismiss for lack of subject matter jurisdiction under Fed.R.Civ.P. 12(b)(1) because it challenges a court's authority to hear the matter. The plaintiff bears the burden of proving that subject matter jurisdiction exists. *Demetres v. East West Constr., Inc.*, 776 F.3d 271, 272 (4th Cir. 2015). When a defendant challenges subject matter jurisdiction facially, as here, the plaintiff "is afforded the same procedural protection" as under Fed.R.Civ.P. 12(b)(6). *Wikimedia Found. v. NSA*, 857 F.3d 193, 208 (4th Cir. 2017) (quotation omitted). "[T]he motion must be denied if the complaint alleges sufficient facts to invoke subject matter jurisdiction." *Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009). The court must accept all well-pleaded allegations in the complaint as true and draw all reasonable inferences in the light most favorable to the plaintiff. *Mays v. Sprinkle*, 992 F.3d 295, 299 (4th Cir. 2021).

III. Analysis

Defendant contends that Plaintiff lacks standing to bring this suit because Plaintiff has not alleged a concrete harm

necessary to establish an injury in fact.[1] Plaintiff argues that he sufficiently alleges an injury in fact.

Article III of the Constitution limits the jurisdiction of federal courts to "Cases" and "Controversies." U.S. Const. art. III, § 2. To establish standing, a plaintiff bears the burden of establishing: (1) an injury in fact that is concrete, particularized, and actual or imminent; (2) a sufficient causal connection between the injury and the conduct complained of; and (3) a likelihood that the injury will be redressed by a favorable decision. *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 157-58 (2014). A concrete injury is "'real,' and not 'abstract.'" *Spokeo, Inc. v. Robins*, 136 S.Ct 1540, 1548 (2016). While tangible harms such as physical and monetary harms constitute sufficiently concrete injuries in fact, intangible harms can also be concrete. *TransUnion LLC v. Ramirez*, 141 S.Ct. 2190, 2204 (2021).

A. Intangible harm

Defendant argues that Plaintiff has alleged a bare procedural violation of MWESA without asserting a concrete harm. (ECF No. 11

[1] In its Notice of Supplemental Authority, Defendant brought the recently decided case *Lightoller v.Jetblue Airways Corp.* to the court's attention, which involved the same defendant as here and a nearly identical complaint. *See* ECF No. 20; Complaint, *Lightoller v. Jetblue Airways Corp.*, No. 23-CV-00361-H-KSC, 2023 WL 3963823 (S.D. Cal. June 12, 2023). In *Lightoller*, the court held that the plaintiff lacked standing because she did not allege disclosure of personal information sufficient to establish a concrete harm to her substantive privacy rights. *Id.* *4.

at 11). Plaintiff argues that a MWESA violation is itself a concrete harm, and he need not allege any additional harm because MWESA resembles traditional common law privacy torts whose violation automatically results in an injury in fact. (ECF No. 14 at 14-15).

A plaintiff proceeding under a statutory cause of action whose injury has "a close historical or common-law analogue" for which courts have traditionally provided a remedy has standing even if the injury alone does not satisfy Article III standing requirements. *Garey v. James S. Farrin, P.C.*, 35 F.4th 917, 921 (4th Cir. 2022) (quoting *TransUnion*, 141 S.Ct. at 2204). Concrete intangible harms with a close relationship to harms traditionally recognized as bases for lawsuits include reputational harms, disclosure of private information, and intrusion upon seclusion. *TransUnion*, 141 S.Ct. at 2204 (citing *Meese v. Keene*, 481 U.S. 465, 473 (1987) (reputational harms); *Davis v. Federal Election Comm'n*, 554 U.S. 724, 733 (2008) (disclosure of private information); *Gadelhak v. AT&T Services, Inc.*, 950 F.3d 458, 462 (7th Cir. 2020) (intrusion upon seclusion)). While a legislature may elevate previously existing harms to actionable status, it may not enact an injury into existence. *See id.* at 2204-05 (citing *Spokeo*, 578 U.S. at 341). Courts must independently decide whether a plaintiff has suffered a concrete harm because a plaintiff cannot automatically satisfy the injury in fact requirement whenever

there is a statutory violation. *TransUnion*, 141 S.Ct. at 2205 ("[U]nder Article III, an injury in law is not an injury in fact.").

Plaintiff argues that MWESA simply "elevated" previously existing privacy rights, as evidenced by the "clear consensus amongst federal courts" establishing that violations of privacy protective statutes such as MWESA sufficiently establish concrete, intangible injuries in fact. (ECF No. 14 at 14-17). Plaintiff is incorrect. As Judge Xinis's opinion in *Sprye v. Ace Motor Acceptance Corp.*, No. 16-cv-03064-PX, 2017 WL 1684619 (D.Md. May 3, 2017), illustrates, there is no consensus that MWESA violations alone give rise to an injury in fact. In *Sprye*, Judge Xinis held that the plaintiff's allegation that the defendant surreptitiously recorded its phone calls to the plaintiff "constitute[s] numerous and multiple violations of [MWESA]" did not assert an injury sufficient to establish standing. *Id.* at *6. Like in *Sprye*, allegations that Defendant has violated MWESA, without additional concrete harm, cannot satisfy Article III standing requirements.

Plaintiff's reliance on cases involving non-MWESA statutes, such as the Telephone Consumer Protection Act, Fair Credit Reporting Act, Driver's Privacy Protection Act ("DPPA"), California Invasion of Privacy Act ("CIPA"), and Title III of the Omnibus Crime Control and Safe Streets Act ("Federal Wiretap Act") fares no better. (ECF No. 14 at 15-16). Even in the context of

CIPA, which, like MWESA, is a state-law analogue to the Federal Wiretap Act,[2] there is far from a consensus regarding whether statutory violations automatically give rise to concrete harm. *Compare, e.g.*, *Licea v. Am. Eagle Outfitters, Inc.*, No. 22-cv-1702-MWF, 2023 WL 2469630, at *3 (C.D.Cal. Mar. 7, 2023) (holding that a bare violation of CIPA is a cognizable violation of privacy rights sufficient to establish standing), *Licea v. Cinmar, LLC*, No. 22-cv-6454-MWF, 2023 WL 2415592, at *3 (C.D.Cal. Mar. 7, 2023) (same), *Garcia v. Build.com, Inc.*, No. 22-CV-01985-DMS-KSC, 2023 WL 4535531, at *4 (S.D.Cal. July 13, 2023) (same), *with Byars v. Sterling Jewelers, Inc.*, No. 22-cv-1456-SB, 2023 WL 2996686, at *4 (C.D.Cal. Apr. 5, 2023) (holding that CIPA violations do not constitute an injury in fact without an additional showing of harm); *Lightoller*, 2023 WL 3963823, at *5 (S.D.Cal. June 12, 2023) (same), *and Massie v. Gen. Motors LLC*, No. CV 21-787-RGA, 2022 WL 534468, at *2, 5 (D.Del. Feb. 17, 2022) (same). Neither is there a consensus that violations of the Federal Wiretap Act alone give rise to an injury in fact. *Compare In re Vizio, Inc. Consumer Privacy Litig.*, 238 F.Supp.3d 1204, 1215-16 (C.D.Cal 2017) (finding concrete harm from Federal Wiretap Act violations due to "the close similarity between the conduct proscribed under the

[2] *See Sprye*, 2017 WL 1684619 at *5 (explaining the relationship between MWESA and the Federal Wiretap Act); *Campbell v. Facebook Inc.*, 77 F.Supp.3d 836, 848 (N.D.Cal. 2014) (explaining the relationship between CIPA and the Federal Wiretap Act).

[Federal] Wiretap Act and the tort of intrusion upon seclusion"), *with Lopez v. Apple, Inc.*, 519 F.Supp.3d 672, 681 (N.D.Cal 2021) (finding that plaintiffs asserting Federal Wiretap Act violations lacked standing because they did not allege non-speculative, concrete injury beyond a statutory privacy harm).

Plaintiff further argues that under *TransUnion*, MWESA violations constitute a concrete harm closely related to the traditional tort of invasion of privacy. (ECF No. 14 at 14, 16-17). Plaintiff analogizes this case to *Garey*, 35 F.4th 917. (ECF No. 14 at 16). In *Garey*, the United States Court of Appeals for the Fourth Circuit determined that DPPA violations automatically confer standing because "the DPPA is aimed squarely at 'the right of the plaintiff . . . 'to be let alone.'" 35 F.4th at 922 (quoting William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960). Plaintiff contends that likewise, MWESA violations also automatically confer standing because MWESA is "squarely aimed at protecting an individual's right to privacy." (ECF No. 14 at 16). MWESA's purpose is two-fold: "1) to be a useful tool in crime detection and 2) to assure that interception of private communications is limited." *Agnew v. State*, 461 Md. 672, 681 (2018) (quoting *State v. Maddox*, 69 Md.App. 296, 300 (1986)). Assisting crime detection and limiting the interception of private communications – which suggest that interception in certain circumstances may be acceptable – is distinguishable from the

DPPA's right "to be let alone" entirely from attorney advertisers using personal information from car accident reports to send unsolicited mail, *see Garey*, 35 F.4th at 920, 922.

While the substantive right to privacy indeed "encompass[es] the individual's control of information concerning his or her person," *U.S. Dept. of Just. v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 763-64 (1989), the Complaint does not allege that Plaintiff disclosed any personal information while interacting with Defendant's website.[3] The Complaint merely states, "Plaintiff visited www.jetblue.com on his computer while in Maryland." (ECF No. 1 ¶ 44). Plaintiff states that during his visit to Defendant's website, his "electronic communications," such as mouse movements, clicks, and keystrokes, were captured and sent to various Session Replay Providers. (ECF No. 1 ¶ 1). Plaintiff further describes various types of "highly sensitive" personal information that could be captured by Session Replay Code, including personally identifying information and credit card details. (ECF No. 1 ¶¶ 28, 31). Here, it is dispositive that Plaintiff only alleges that Session Replay Code *could* capture personal information, not that it actually captured Plaintiff's

[3] In the Complaint, Plaintiff includes screenshots of information sent to a Session Replay Provider depicting a flight from Pittsburg, PA to Las Vegas, NV, with a connecting flight through Boston, MA. (ECF No. 1 ¶ 48). The Complaint fails to explain how this specific flight information captures Plaintiff's personal information.

personal information. Because the Complaint says nothing about the kinds of interactions Plaintiff had with Defendant's website, much less the specific kinds of captured personal information implicating a substantive privacy interest, Plaintiff has not alleged that his personal information was intercepted and recorded by Defendant.[4]

B. Tangible harm

Plaintiff also argues that Defendant's disclosure of his electronic communications to Session Replay Providers gives rise to a plausible risk of enhanced privacy threats, such as identity

[4] Other courts have found that violations tantamount to a substantive privacy injury require disclosure of specific personal information. *See Byars*, 2023 WL 2996686, at *3 ("Plaintiff does not allege that she disclosed any sensitive information to Defendant, much less identify any specific personal information she disclosed that implicates a protectable privacy interest. She therefore has not identified any harm to her privacy."); *Mikulsky v. Noom, Inc.*, No. 3:23-CV-00285-H-MSB, 2023 WL 4567096, at *5 (S.D.Cal. July 17, 2023) (holding that the plaintiff's claims that she had suffered concrete harm arising from inputting her personal information in text fields fails to establish standing because she did not identify the specific personal information disclosed); *Massie*, 2022 WL 534468, at *4 (D.Del. Feb. 17, 2022) ("Plaintiffs have not alleged any disclosure of any of their private information. Insofar as Plaintiffs have alleged GM disclosed their non-private information to Decibel, they have not alleged that Decibel used that information in any way, let alone in a way that harmed or would likely harm Plaintiffs."); *Lightoller*, 2023 WL 3963823, at *4 (finding allegations that the defendant intercepted the plaintiff's communications with the defendant's website, without alleging disclosure of any specific personal information, fail to assert a concrete privacy harm).

theft, constituting a concrete tangible harm.[5] (ECF No. 14 at 18). Defendant argues that Plaintiff fails to establish a personal and non-conjectural risk of enhanced privacy threats. (ECF No. 11 at 11-12).

A threatened injury constitutes an injury in fact when it is certainly impending. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013). Sufficiently imminent injuries in fact cannot be premised on a "highly attenuated chain of possibilities." *Id.* at 410. The Fourth Circuit has interpreted *Clapper* to require targeting or misuse before a future risk of identity theft qualifies as an injury in fact. *See Beck v. McDonald*, 848 F.3d 262, 274 (4th Cir. 2017) (holding that without evidence of misuse or deliberate targeting by data thieves, an enhanced risk of identity theft as a result of a data breach is too speculative to constitute an injury in fact); *Hutton v. Nat'l Bd. of Examiner in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018) (holding that data breach victims who had already experienced identity theft and

[5] In his Response in Opposition to Defendant's Motion to Dismiss, (ECF No. 14), Plaintiff does not respond to Defendant's additional contention that Plaintiff's allegations of mental anguish and lost economic value are too conclusory to establish an injury in fact. (ECF No. 11 at 12-13). By failing to respond, Plaintiff has conceded this point. *See Ferdinand-Davenport v. Children's Guild*, 742 F.Supp.2d 772, 777 (D.Md. 2010) (holding that in failing to respond to the defendant's arguments for why her claim should be dismissed, a plaintiff abandoned her claim); *Stenlund v. Marriott Int'l, Inc.*, 172 F.Supp.3d 874, 887 (D.Md. 2016) ("In failing to respond to [defendant's] argument, Plaintiff concedes the point.").

credit card fraud sufficiently alleged an injury in fact); *O'Leary v. TrustedID*, 60 F.4th 240 (4th Cir. 2023) (holding that a plaintiff who cannot connect the alleged statutory violation to an increased risk of identity theft without a "Rube Goldberg-type chain reaction" lacks standing).

Here, Plaintiff has not alleged facts establishing targeting or misuse of his personal information. In fact, as Defendant states, "[Plaintiff] does not allege that he provided any information to JetBlue that could be used to commit the 'identity theft, online scams, and other privacy threats' he allegedly fears." (ECF No. 19 at 12). While Plaintiff argues that being a visitor to Defendant's website subject to Session Replay Code results in non-conjectural privacy risks, (ECF No. 14 at 17-18), for identity theft to materialize, Defendant's Session Replay providers must suffer a data breach, the breach must compromise Plaintiff's sensitive personal information, and an identity thief must misuse that information to harm Plaintiff – the very kind of chain reaction *Clapper* has deemed too speculative.

Because Plaintiff has failed to establish an injury in fact necessary for Article III standing, his claims will be dismissed. Thus, it is unnecessary to address whether this court has personal jurisdiction over Defendant and whether Plaintiff has failed to state a claim.

IV. Conclusion

For the foregoing reasons, Defendant's motion to dismiss will be granted. A separate Order will follow.

/s/
DEBORAH K. CHASANOW
United States District Judge