

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION**

TREVOR SLOAN, JOSEPH BLEIBERG, )  
ARYEH LOUIS ROTHBERGER, )  
PATRICK COMMERFORD, KEVIN )  
FARR, ELMER ORPILLA, KEITH )  
LAPATING, and SAGAR DESAI, on behalf )  
of themselves and all others similarly situated, )

Plaintiffs, )

v. )

ANKER INNOVATIONS LIMITED, )  
FANTASIA TRADING LLC, and POWER )  
MOBILE LIFE LLC, )

Defendants. )

No. 22 C 7174

Judge Sara L. Ellis

**OPINION AND ORDER**

Plaintiffs Trevor Sloan, Joseph Bleiberg, Aryeh Louis Rothberger, Patrick Commerford, Kevin Farr, Sagar Desai, Elmer Orpilla, and Keith Lapating allege Defendants Anker Innovations Limited, Fantasia Trading LLC, and Power Mobile Life LLC violated various privacy laws relating to their practices in storing data connected to their “eufy” branded security products.<sup>1</sup> Specifically, Plaintiffs seek redress under the Federal Wiretap Act, 8 U.S.C. § 2510; the Biometric Information Privacy Act (“BIPA”), 740 Ill. Comp. Stat. 14/1 *et seq.*; several consumer fraud statutes—the Illinois Consumer Fraud and Deceptive Trade Practices Act (“ICFA”), 815 Ill. Comp. Stat. 505/1 *et seq.*; the New York Deceptive Acts and Practices Law, NY Gen. Bus. §§ 349 and 350; the Massachusetts Consumer Fraud Law, Chapter 93A (“Mass. Ch. 93A”); and the Florida Deceptive and Unfair Trade Practices (“FDUPTA”), Fla. Stat. §

---

<sup>1</sup> On May 8, 2023, the Court consolidated this case with *Bleiberg v. Anker Innovations Ltd.*, No. 22 C 7218 (N.D. Ill.), and *Desai v. Anker Technology Corp.*, No. 23 C 1607 (N.D. Ill), for all purposes.

501.201; and for unjust enrichment. Defendants filed a motion to dismiss Plaintiffs' claims pursuant to Federal Rule of Civil Procedure 12(b)(6).

The Court grants in part and denies in part Defendants' motion to dismiss. The Wiretap Act does not apply to the facts of this case because Defendants are a party to the communication—specifically the transmission of data from the eufy products to Plaintiffs' receipt of that data on the eufy Security app—and so the Court dismisses the Wiretap Act claim. Similarly, the Court dismisses Plaintiffs' BIPA and ICFA claims as to the non-Illinois resident plaintiffs and the nationwide class because neither statute applies extraterritorially. Finally, the Court dismisses Plaintiffs' ICFA, NY Gen. Bus. § 349, Mass. Ch. 93A, and FDUPTA claims to the extent they rely on Defendants' statements relating to security because those statements are puffery. Plaintiffs may proceed on their remaining claims as discussed below.

## **BACKGROUND<sup>2</sup>**

Plaintiffs' claims arise from their purchase and use of Defendants' "eufy" branded security products, specifically eufy home security cameras and video doorbells (the "eufy products"). The eufy products can access Wi-Fi, record and stream video, and detect motion. The eufy products apply a facial recognition program called the BionicMind System, which differentiates between known individuals and strangers by recognizing biometric identifiers and comparing the face template against those stored in a database. The eufy products sync to a consumer's phone through the eufy Security app, which automatically notifies the consumer of

---

<sup>2</sup> The Court takes the facts in the background section from Plaintiffs' consolidated complaint and presumes them to be true for the purpose of resolving Defendants' motion to dismiss. *See Phillips v. Prudential Ins. Co. of Am.*, 714 F.3d 1017, 1019–20 (7th Cir. 2013). Although the Court normally cannot consider extrinsic evidence without converting a motion to dismiss into one for summary judgment, *Jackson v. Curry*, 888 F.3d 259, 263 (7th Cir. 2018), the Court may consider "documents that are central to the complaint and are referred to in it" in ruling on a motion to dismiss, *Williamson v. Curran*, 714 F.3d 432, 436 (7th Cir. 2013).

motion around the camera either by showing a thumbnail image taken from the camera or sending a text message indicating the motion.

As advertised, the cameras store the video recordings and data to conduct facial recognition locally, “meaning on equipment located with and controlled by the consumer.” Doc. 31 ¶ 2. Additionally, Defendants advertised that information from the eufy products remained encrypted, so only the user could access the data. The eufy products’ packaging included the following statements: “your privacy is something we value as much as you do”; “to start, we’re taking every step imaginable to ensure that your data remains private, with you”; “whether it’s your newborn crying for mom, or your victory dance after a game, your recorded footage will be kept private”; “stored locally with military grade encryption”; “transmitted to you, and only you”; and “that’s just the start of our commitment to protect you, your family, and your privacy.” *Id.* ¶ 32. Defendants also warranted that “there is no online link available to any video.” *Id.* ¶ 33. Defendants’ privacy policy stated that the eufy products operate with “no clouds.” *Id.* ¶ 37.

Plaintiffs all purchased at least one eufy product between June 2020 and November 2022 and installed them in their respective residences—Sloan and Orpilla in Illinois, Bleiberg and Rothberger in New York, Desai in Florida, Commerford in Texas, Farr in Massachusetts, and Lapating in California. Plaintiffs all allege they relied on representations that the products would store data locally and encrypt their data when purchasing the eufy products. Similarly, Plaintiffs all allege they would have paid less or not purchased the eufy products at all if they knew the data would not be encrypted, could be accessed by third parties, or would be uploaded to Defendants’ servers.

In November 2022, Paul Moore, a security researcher, posted several tweets and videos revealing holes in the security network for the eufy products. Specifically, Moore identified that the eufy products uploaded the thumbnail images used to notify users of movement through the app to Defendants' cloud storage without encryption. Moore determined that he could stream content from his videos through unencrypted websites and posted a video showing that his camera feed could be accessed through an incognito web browser. SEC Consult, a security firm, and *The Verge*, an online technology media outlet, confirmed Moore's results.

Defendants initially denied that the eufy products streamed video without encryption. However, on November 29, 2022, Defendants released a statement asserting that “[a]lthough our eufy Security app allows users to choose between text-based or thumbnail-based push notifications, it was not made clear that choosing thumbnail-based notifications would require preview images to be briefly hosted on the cloud. The lack of communication was an oversight on our part and we sincerely apologize for the error.” *Id.* ¶ 57. Several months later, in January 2023, Anker's global head of communication provided a statement to *The Verge* acknowledging prior denials from the company regarding the production of unencrypted videos were wrong and that the unencrypted video streams were “a known issue, easily replicated and had been reported by the media.” *Id.* ¶ 65.

### **LEGAL STANDARD**

A motion to dismiss under Rule 12(b)(6) challenges the sufficiency of the complaint, not its merits. Fed. R. Civ. P. 12(b)(6); *Gibson v. City of Chi.*, 910 F.2d 1510, 1520 (7th Cir. 1990). In considering a Rule 12(b)(6) motion, the Court accepts as true all well-pleaded facts in the plaintiff's complaint and draws all reasonable inferences from those facts in the plaintiff's favor. *Kubiak v. City of Chi.*, 810 F.3d 476, 480–81 (7th Cir. 2016). To survive a Rule 12(b)(6)

motion, the complaint must assert a facially plausible claim and provide fair notice to the defendant of the claim's basis. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007); *Adams v. City of Indianapolis*, 742 F.3d 720, 728–29 (7th Cir. 2014). A claim is facially plausible “when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Iqbal*, 556 U.S. at 678.

Rule 9(b) requires a party alleging fraud to “state with particularity the circumstances constituting fraud.” Fed. R. Civ. P. 9(b). This “ordinarily requires describing the ‘who, what, when, where, and how’ of the fraud, although the exact level of particularity that is required will necessarily differ based on the facts of the case.” *AnchorBank, FSB v. Hofer*, 649 F.3d 610, 615 (7th Cir. 2011) (citation omitted). Rule 9(b) applies to “all averments of fraud, not claims of fraud.” *Borsellino v. Goldman Sachs Grp., Inc.*, 477 F.3d 502, 507 (7th Cir. 2007). “A claim that ‘sounds in fraud’—in other words, one that is premised upon a course of fraudulent conduct—can implicate Rule 9(b)'s heightened pleading requirements.” *Id.*

## ANALYSIS

### I. Group Pleading

Defendants move to dismiss Plaintiffs' entire complaint for improper use of group pleading. Under Rule 8, Plaintiffs need only provide a “short and plain statement of the claim showing that [they are] entitled to relief.” Fed. R. Civ. P. 8(a). There “is no ‘group pleading’ doctrine, *per se*, that either permits or forbids allegations against defendants collectively.” *Robles v. City of Chi.*, 354 F. Supp. 3d 873, 875 (N.D. Ill. 2019). Group pleading does not violate Rule 8 “so long as the complaint provides sufficient detail to put the defendants on notice of the claims.” *Horton v. City of Rockford*, No. 18 C 6829, 2019 WL 3573566, at \*3 (N.D. Ill.

Aug. 6, 2019) (citations omitted). A complaint that directs every allegation at all the defendants can provide sufficient detail to put the defendants on notice because the defendants “do not have to speculate about which claims or allegations pertain to them; they must defend against them all.” *Gorgas v. Amazon.com, Inc.*, No. 22 CV 5159, 2023 WL 4209489, at \*3 (N.D. Ill. June 23, 2023). Here, Defendants “do not have to speculate about which claims or allegations pertain to them” because Plaintiffs have asserted all claims against all three defendants, so the allegations do not violate Rule 8. *Id.*

However, group pleading can run headfirst into Rule 9(b)’s requirement for particularity for averments sounding in fraud or “premised upon a course of fraudulent conduct.” *Borsellino v. Goldman Sachs Grp., Inc.*, 477 F.3d 502, 507 (7th Cir. 2007). This is because in fraud cases involving multiple defendants, “the complaint should inform each defendant of the nature of his alleged participation in the fraud.” *Vicom, Inc. v. Harbridge Merch. Servs., Inc.*, 20 F.3d 771, 778 (7th Cir. 1994).

Plaintiffs’ use of group pleading does not violate Rule 9(b). Plaintiffs’ Wiretap Act and BIPA claims do not sound in fraud so neither must meet the heightened pleading requirement of Rule 9(b). *See Doe v. Smith*, 429 F.3d 706, 708 (7th Cir. 2005) (not applying Rule 9(b) to pleadings regarding “interceptions” under the Wiretap Act); *Kuklinski v. Binance Cap. Mgmt. Co.*, No. 21-CV-001425-SPM, 2023 WL 2788654, at \*10 (S.D. Ill. Apr. 4, 2023) (finding BIPA does not require heightened pleading). However, Plaintiffs’ consumer fraud statute claims do sound in fraud because they assert Defendants deceived Plaintiffs through misleading statements that induced Plaintiffs’ purchase of the eufy products. *See, e.g., Joseph v. TGI Friday’s, Inc.*, No. 21-CV-1340, 2022 WL 17251277, at \*3 (N.D. Ill. Nov. 28, 2022) (“Claims alleging fraud, including those asserted under the ICFA, are subject to the heightened pleading standard of

Federal Rule of Civil Procedure 9(b)[.]”); *Gross v. LoanCare LLC*, No. 1:21-CV-5589 (ALC), 2022 WL 4585418, at \*5 (S.D.N.Y. Sept. 29, 2022) (applying Rule 9(b) to a claim under N.Y. GBL § 349); *Toca v. Tutco, LLC*, 430 F. Supp. 3d 1313, 1328 (S.D. Fla. 2020) (applying Rule 9(b) to claim arising under FDUPTA); *Rick v. Profit Mgmt. Assocs., Inc.*, 241 F. Supp. 3d 215, 225 (D. Mass. 2017) (“A 93A claim sounding in fraud must satisfy the heightened pleading requirement of Fed. R. Civ. P. 9(b).”). Yet the use of group pleading does not run afoul of Rule 9(b) here. Even under heightened pleading standards, the Court must evaluate whether the complaint “adequately puts Defendants on notice of the unlawful acts that she alleges both committed.” *Joseph*, 2022 WL 17251277, at \*4 (rejecting Defendants’ arguments that a defendant should be dismissed on group pleading grounds, even under a heightened 9(b) pleading standard, and choosing to do so on other grounds instead). Here, Plaintiffs allege that each of the Defendants “acted jointly to perpetrate the acts” underlying the complaint. Doc. 31 ¶ 22. The facts alleged throughout the complaint, including the specific statements made by Defendants in their marketing and in response to media inquiries about their products, provide sufficient detail to put Defendants on notice of the unlawful acts Plaintiffs allege. *Joseph*, 2022 WL 17251277, at \*4 (“As Defendants do not suffer any apparent confusion over Plaintiff’s allegations, the Court declines to dismiss Plaintiff’s allegations against Defendants for improper lumping together.”); *see also In re Chevrolet Bolt EV Battery Litig.*, 633 F. Supp. 3d 921, 962 (E.D. Mich. 2022) (not dismissing claim for group pleading issue because plaintiffs sufficiently alleged the roles of both defendants in the events at issue in the case). As such, Plaintiffs do not contravene pleading standards by using group pleading, and so the Court proceeds to evaluate Defendants’ claim-specific arguments.

## II. The Wiretap Act

The Wiretap Act empowers a private citizen to bring a civil claim against someone who “intentionally intercepts [or] endeavors to intercept . . . any wire, oral, or electronic communication.” 18 U.S.C. § 2511(1)(a); *id.* § 2520 (civil remedies). Defendants contend Plaintiffs failed to state a claim under the Wiretap Act for two reasons. First, Defendants argue that the Wiretap Act does not apply as a matter of law because Plaintiffs used the eufy Security app to access the video, making Defendants a party to the communication. Second, Defendants assert that Plaintiffs have not adequately alleged that Defendants intercepted their communications in violation of the Wiretap Act. Because the Court finds that Defendants were parties to the communication, the Court dismisses Plaintiffs’ Wiretap Act claim.

The Wiretap Act exempts a person who intercepted an electronic communication “where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.” 18 U.S.C. § 2511(2)(d). Here, the communication at issue is the transmission of data from the eufy products to Plaintiffs’ device, which Plaintiffs allege is “contemporaneously intercepted and sent to Anker’s server.” Doc. 31 ¶ 113. Plaintiffs allege that the interception of data occurs when their home cameras “upload images and facial recognition data to Defendants’ cloud storage, which is hosted by a third party (Amazon Web Services (‘AWS’), a subsidiary of Amazon.com, Inc.), even where the user did not sign up for cloud storage or services.” *Id.* ¶ 6. However, Plaintiffs also allege that to access the data from their eufy products, they had to use the eufy Security app. *Id.* ¶ 15. The communication, therefore, is not between the eufy product and Plaintiffs, but rather between the eufy product and



the eufy Security app, which Defendants own and operate. As such, the communication necessarily requires Defendants' participation, even if Plaintiffs did not intend to share their information with Defendants. *See Zak v. Bose Corp.*, No. 17-CV-02928, 2019 WL 1437909, at \*3 (N.D. Ill. Mar. 31, 2019) (finding a defendant may be a participant to the communication under the Wiretap Act "even if the defendant was not an intended participant, and even if the defendant became a participant through a fraud in the inducement"); *cf. Vasil v. Kiip, Inc.*, No. 16-CV-09937, 2018 WL 1156328, at \*6 n. 5 (N.D. Ill. Mar. 5, 2018) (finding Kiip, an advertising company that delivered ads in the Runkeeper app, was not a participant when it surreptitiously received data the user shared directly with the Runkeeper app because "Kiip was not a substitute for Runkeeper"). That Defendants, parties to the communication, then upload some of that data to a third-party cloud server does not transform Defendants' action into an interception under the Wiretap Act. *See Kurowski v. Rush Sys. for Health*, No. 22 C 5380, 2023 WL 2349606, at \*4 (N.D. Ill. Mar. 3, 2023) (concluding that plaintiffs could not hold the defendant liable under the Wiretap Act because, despite sharing information with third parties Facebook, Google, and Bidtellect, defendant was "the intended recipient of the communication" and therefore defendant was "a party to those communications and cannot be liable under the Wiretap Act for its alleged interception of them, if such an interception even occurred"). Because Defendants, as a party to the communication, cannot be liable under the Wiretap Act, the Court dismisses this claim.<sup>3</sup>

---

<sup>3</sup> Because the Court finds that Defendants were, as a matter of law, a party to the communication and therefore not liable under the Wiretap Act, it does not consider whether the interception was contemporaneous.

### **III. BIPA**

#### **A. Sufficiency of the Pleading**

Defendants challenge the sufficiency of Plaintiffs' BIPA claim only as to whether the information that Plaintiffs allege Defendants illegally collected and stored qualifies for protection under BIPA. BIPA makes it unlawful to “collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifiers and/or biometric information” without a written release. 740 Ill. Comp. Stat. 14/15(b). BIPA further requires that “[a] private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied.” 740 Ill. Comp. Stat. 14/15(a). BIPA defines biometric identifiers as “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.” 740 Ill. Comp. Stat. 14/10. The biometric identifier definition excludes photographs. *Id.* BIPA defines biometric information as “any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.” *Id.* The biometric information definition excludes “information derived from items or procedures excluded under the definition of biometric identifiers.” *Id.*

Defendants argue the data Plaintiffs allege has been illegally collected and stored—namely, thumbnails photographs—do not qualify as biometric data. While photographs alone do not support a BIPA action, photographs used by a system that can take a geometric scan of a person do qualify as biometric data. *Sosa v. Onfido, Inc.*, 600 F. Supp. 3d 859, 871 (N.D. Ill. 2022) (determining that faceprints—scans of identification cards and photographs—qualify as

biometric identifiers because they “plausibly constitute scans of face geometry”). This is because “a ‘biometric identifier’ is not the underlying medium itself, or a way of taking measurements, but instead is a set of measurements of a specified physical component (eye, finger, voice, hand, face) used to identify a person.” *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1096 (N.D. Ill. 2017); *see also Sosa*, 600 F. Supp. 3d at 871 (“But nothing in section 10 expressly excludes information derived from photographs from the definition of biometric identifiers.”).

Here, Plaintiffs allege that Defendants do more than simply upload thumbnail information to their cloud storage. They instead assert that Defendants “upload images and facial recognition data to Defendants’ cloud storage.” Doc. 31 ¶ 6. Plaintiffs do not specify what facial recognition data Defendants store. However, they do describe the BionicMind program, which Plaintiffs allege “enables eufy cameras to differentiate between known individuals and strangers by recognizing biometric identifiers (i.e. details about the face’s geometry as determined by facial points and contours) and comparing the resulting ‘face template’ (or ‘faceprint’) against the face templates stored in a database.” *Id.* ¶ 28; *see also id.* ¶ 43 (“[T]he Camera Products paired consumers’ facial scans with other personally identifiable information from the consumer, which made Defendants capable of determining consumers’ identities.”). Considering the allegations that the eufy products used the BionicMind programs to construct faceprints and Defendants stored facial recognition data on the cloud together, Plaintiffs have described a scheme that “plausibly constitutes scans of face geometry.” *Sosa*, 600 F. Supp. 3d at 871, 873. Therefore, Plaintiffs have sufficiently stated their BIPA claim and the Court will not dismiss it.

## **B. Non-Illinois Resident Plaintiffs**

Defendants also argue that the Court should dismiss Bleiberg, Rothberger, Desai, Commerford, Farr, Lapating, and the Nationwide Class' BIPA claims because those Plaintiffs failed to allege sufficient facts to tie their harm to Illinois. The Court agrees.

Under Illinois law, “a statute is without extraterritorial effect unless a clear intent in this respect appears from the express provisions of the statute.” *Avery v. State Farm Mut. Auto. Ins. Co.*, 216 Ill. 2d 100, 184–85 (2005) (citation omitted).<sup>4</sup> Because “none of BIPA’s express provisions indicates that the statute was intended to have extraterritorial effect . . . BIPA does not apply extraterritorially.” *Monroy*, 2017 WL 4099846, at \*5. To avoid the extraterritoriality doctrine, “the circumstances that relate to the disputed transaction [must have] occur[red] primarily and substantially in Illinois,” with “each case . . . decided on its own facts.” *Avery*, 216 Ill. 2d at 187.

The non-Illinois resident Plaintiffs have not alleged any facts suggesting that the “bulk of the circumstances that make up a fraudulent transaction occur[ed] within Illinois.” *Rivera*, 238 F. Supp. 3d at 1102 (quoting *Avery*, 216 Ill. 2d at 186). None of the non-Illinois plaintiffs claim they purchased their eufy products in Illinois. And Plaintiffs’ allegations that Anker Innovations exports and sells its products “throughout the world, including throughout the United States in New York and Illinois,” do not establish that the non-Illinois resident Plaintiffs acquired their eufy products in Illinois. Doc. 31 ¶ 19. Instead, Plaintiffs’ pleadings illustrate that the circumstances making up each transaction occurred primarily and substantially in the state of residency for each Plaintiff. Plaintiffs all experienced their alleged harm—access to their data

---

<sup>4</sup> While Plaintiffs attempt to distinguish cases that rely on *Avery* based on the fact that *Avery* interpreted ICFA and not BIPA, courts have applied *Avery* to other Illinois statutes, including BIPA. See *Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846, at \*6 n.4 (N.D. Ill. Sept. 15, 2017) (discussing *Avery*’s application to other Illinois laws, including BIPA).

without their consent—at their residence, where they had installed the cameras. *Neals v. PAR Tech. Corp.*, 419 F. Supp. 3d 1088, 1091 (N.D. Ill. 2019) (dismissing BIPA claim where plaintiff failed to allege where her biometric information was collected). As alleged, the eufy products provide home security; therefore, the bulk of the circumstances at issue for each individual Plaintiff would occur in his own home. For those who reside out of Illinois, those circumstances would occur outside of Illinois. Accordingly, as alleged, BIPA does not apply to the non-Illinois residents.

Plaintiffs, however, argue that because they are governed by Illinois law, as detailed in the choice of law provision in the End User License Agreement for Camera Products and the eufy Security App, the non-Illinois putative class members and named Plaintiffs may benefit from BIPA. This argument is incorrect. *Shaw v. Hyatt Int'l Corp.*, No. 05 C 5022, 2005 WL 3088438, at \*3 (N.D. Ill. Nov. 15, 2005) (“As discussed above, the extraterritorial application of the ICFA is limited to deceptive trade practices occurring primarily and substantially within Illinois. The fact that Illinois law was selected to govern disputes arising out of Hyatt's website does nothing to further the contention that the allegedly deceptive practices occurred in Illinois.”), *aff'd*, 461 F.3d 899 (7th Cir. 2006). Therefore, the Court dismisses the BIPA claims as to Plaintiffs Bleiberg, Rothberger, Desai, Commerford, Farr, and Lapating. Plaintiffs Sloan, and Orpilla may proceed on their BIPA claim.

#### **IV. Consumer Protection Laws**

Plaintiffs bring claims on behalf of both individual Plaintiffs and statewide classes under four state consumer protection laws: ICFA, NY Gen. Bus. §§ 349 and 350, Mass. Ch. 93A, and FDUPTA. While the consolidated complaint states that the statements were unfair and deceptive, the parties only discuss whether the statements support a deceptive practice claim

under each of the consumer fraud statutes. The Court therefore similarly only considers whether Plaintiffs have alleged a deceptive practices theory within the meaning of each consumer fraud statute. *See Rudy v. Fam. Dollar Stores, Inc.*, 583 F. Supp. 3d 1149, 1158 (N.D. Ill. 2022) (only applying the standard for deceptive practice to a ICFA claim where the plaintiff's claim "challenges a 'deceptive,' as opposed to an 'unfair,' practice").

To state a claim for deceptive practices under any of the alleged state consumer fraud statutes, Plaintiffs must allege a deceptive statement or act that caused their harm. *Camasta v. Jos. A. Bank Clothiers, Inc.*, 761 F.3d 732, 739 (7th Cir. 2014) (listing the elements of an ICFA claim: "(1) a deceptive or unfair act or promise by the defendant; (2) the defendant's intent that the plaintiff rely on the deceptive or unfair practice; and (3) that the unfair or deceptive practice occurred during a course of conduct involving trade or commerce"); *Tomasella v. Nestle USA, Inc.*, 962 F.3d 60, 71 (1st Cir. 2020) (stating a claim under Mass. Ch. 93A requires the plaintiff to allege "(1) a deceptive act or practice on the part of the seller; (2) an injury or loss suffered by the consumer; and (3) a causal connection between the seller's deceptive act or practice and the consumer's injury"); *Carriuolo v. Gen. Motors Co.*, 823 F.3d 977, 983 (11th Cir. 2016) (under FDUPTA, a plaintiff must allege "(1) a deceptive act or unfair practice; (2) causation; and (3) actual damages"); *Mirza v. Ignite USA, LLC*, 439 F. Supp. 3d 1058, 1072 (N.D. Ill. 2020) (listing the elements of a N.Y. Gen. Bus. § 349 claim: "defendant has engaged in (1) consumer-oriented conduct that is (2) materially misleading and that (3) [the] plaintiff suffered injury as a result of the allegedly deceptive act or practice").

Defendants raise identical arguments for the dismissal of each of the consumer protection law claims.<sup>5</sup> First, Defendants argue that the consumer fraud claims fail because Plaintiffs do

---

<sup>5</sup> Because the parties analyze the consumer fraud statutes together in their briefs and have not identified any meaningful differences between the various state laws, the Court generally cites to Illinois caselaw,

not allege cognizable deceptive statements, either because the statements constitute puffery, are not false, or are omissions that Plaintiffs have not alleged with sufficient particularity. Second, Defendants argue that Plaintiffs fail to allege that the statements caused their harm with the particularity required by Rule 9(b).

#### **A. Deceptive Acts**

“[A] statement is deceptive if it creates a likelihood of deception or has the capacity to deceive.” *Bober v. Glaxo Wellcome PLC*, 246 F.3d 934, 938 (7th Cir. 2001). “[T]he allegedly deceptive act must be looked upon in light of the totality of the information made available to the plaintiff.” *Davis v. G.N. Mortg. Corp.*, 396 F.3d 869, 884 (7th Cir. 2005). “Courts apply a ‘reasonable consumer’ standard to analyze the likelihood of deception.” *Benson v. Fannie May Confections Brands, Inc.*, 944 F.3d 639, 646 (7th Cir. 2019); *see also Mirza*, 439 F. Supp. 3d at 1072 (“Under New York law, ‘materially misleading’ conduct means an act that is likely to mislead a reasonable consumer acting reasonably under similar circumstances.”); *Tomasella*, 962 F.3d 60 at 71 (applying the reasonable consumer standard to Mass. Ch. 93A); *Carruiolo*, 823 F.3d at 983 (finding plaintiff must show that “the alleged practice was likely to deceive a consumer acting reasonably in the same circumstances”). “[T]he question of whether a representation is materially misleading ‘is generally a question of fact not suited for resolution at the motion to dismiss stage.’” *Colpitts v. Blue Diamond Growers*, 527 F. Supp. 3d 562, 581 (S.D.N.Y. 2021) (citation omitted); *see also Cooper v. Anheuser-Busch, LLC*, 553 F. Supp. 3d 83, 95 (S.D.N.Y. 2021) (“At this stage of the case, however, such a determination is appropriate only if Plaintiffs’ claims are patently implausible or unrealistic.”). Defendants argue that the

---

providing additional citations to cases applying the other state consumer fraud laws as necessary. *See DeMaso v. Walmart Inc.*, 655 F. Supp. 3d 696, 704 (N.D. Ill. 2023) (treating various state consumer fraud laws as “substantially the same as the ICFA” when “determining whether a reasonable consumer would be deceived by the product’s label”).

alleged statements constitute either puffery or substantially true statements, neither of which can constitute a deceptive statement under any of the alleged consumer fraud acts.

### 1. Puffery

“Puffery is a statement of subjective description or opinion, and is not actionable as a fraudulent misrepresentation.” *Castaneda v. Amazon.com, Inc.*, No. 22-CV-3187, 2023 WL 4181275, at \*6 (N.D. Ill. June 26, 2023) (citations omitted). “Puffing ‘denotes the exaggerations reasonably to be expected of a seller as to the degree of quality of his or her product, the truth or falsity of which cannot be precisely determined.’” *Schwebe v. AGC Flat Glass N. Am., Inc.*, 2013 WL 2151551, at \*4 (N.D. Ill. 2013) (quoting *Avery*, 216 Ill. 2d at 173); *see also* *Lugones v. Pete & Gerry’s Organic, LLC*, 440 F. Supp. 3d 226, 241 (S.D.N.Y. 2020) (defining puffery as “generalized or exaggerated statements which a reasonable consumer would not interpret as a factual claim upon which he could rely . . . [or] an exaggeration or overstatement expressed in broad, vague, and commendatory language, as distinguished from misdescriptions or false representations of specific characteristics of a product”); *Martin*, 2010 WL 3928707, at \*3 (same for Mass. Ch. 93A). “Examples of puffery include ‘high-quality,’ ‘expert workmanship,’ ‘custom quality,’ ‘perfect,’ ‘magnificent,’ ‘comfortable,’ and ‘picture perfect.’” *Lateef v. Pharmavite LLC*, No. 12 C 5611, 2013 WL 1499029, at \*3 (N.D. Ill. Apr. 10, 2013); *see also* *Isaac v. Ashley Furniture Indus., Inc.*, No. CV 17-11827-RGS, 2017 WL 4684027, at \*1 (D. Mass. Oct. 18, 2017) (listing “slogans, catch phrases, and focus-grouped puffing by manufacturers and distributors [who are] striving to make themselves heard in the din of a consumption-driven marketplace” as nonactionable puffery).

Defendants identify five statements, which they have categorized in their briefing as “statements relating to privacy,” as puffery: (1) “your privacy is something that we value as



much as you do”; (2) “that’s just the start of our commitment to protect you, your family and your privacy”; (3) “privacy and protection are our top priorities”; (4) “your privacy is our priority”; and (5) “to start, we’ve taken every step imaginable to ensure that your data remains private, with you.” *See* Doc. 45-1 at 24. The first four statements emphasize the value Defendants place on a consumer’s privacy generally; they do not speak to a promise of heightened privacy provided by their products as distinguished from their competitors. *Cf. Evolve Biosystems, Inc. v. Abbott Lab’ys*, No. 19 C 5859, 2022 WL 846900, at \*6 (N.D. Ill. Mar. 22, 2022) (finding that customers will rely on “commercial language as ‘poten[t],’ ‘stabl[e],’ and ‘high-quality’ to denote the products’ function and efficacy” where customers are aware that “infant probiotic products can be tested for function and efficacy”). These statements relate to general values and priorities of a company and qualify as puffery because they are subjective, not objective facts that one can prove true or false. *See Williams v. Aztar Ind. Gaming Corp.*, 351 F.3d 294, 299 & n.5 (7th Cir. 2003) (determining that the statement that “[a]s always, our top priority is simply this: to ensure your complete, 100% satisfaction” amounts to sales puffery); *Brown v. Coty, Inc.*, No. 22 CIV. 2696 (AT), 2023 WL 2691581, at \*4 (S.D.N.Y. Mar. 29, 2023) (finding press statements that did not describe the product at issue but instead conveyed company mission statements constituted puffery).

Plaintiffs argue that the fifth statement, that Defendants took every step imaginable to ensure that consumers’ data remained private, differs from the other four statements because it can be tested and proven whether Defendants did so. While it may be possible to count how many steps Defendants took, no reasonable consumer would expect a company to take every step she could literally imagine to protect her data. Further, it is unclear how someone, other than an expert in data security, could identify “every step imaginable” in protecting someone’s data. A

reasonable consumer would thus interpret “every step imaginable” as Defendants’ exaggeration to convey their general commitment to their consumers’ privacy, not as a statement of fact. *See, e.g., Castaneda*, 2023 WL 4181275, at \*7 (determining that a claim that a game console worked at “lightning speed” was puffery even though a consumer can measure speed of a game console because “no reasonable consumer would expect literal ‘lightning speed.’”). Therefore, the Court dismisses the ICFA, N.Y. Gen. Bus. § 349, Mass. Ch. 93A, and FDUPTA claims to the extent they rely on the statements discussed in this section—(1) “your privacy is something that we value as much as you do”; (2) “that’s just the start of our commitment to protect you, your family and your privacy”; (3) “privacy and protection are our top priorities”; (4) “your privacy is our priority”; and (5) “to start, we’ve taken every step imaginable to ensure that your data remains private, with you”—because those statements constitute puffery.

## 2. Accurate Statements

Defendants claim each of the remaining statements are not misleading because they are not false. Defendants categorized these statements into the following three groups—statements relating to storage and streaming,<sup>6</sup> statements relating to facial recognition,<sup>7</sup> and statements relating to encryption.<sup>8</sup> At this stage, however, Plaintiffs have sufficiently pleaded that

---

<sup>6</sup> These statements include “all your footage is securely stored locally[,] [e]nsuring the videos you record are for you and only you”; “storage[:] You are in control of your recordings. We have designed controls to ensure all videos are stored securely, in your home, on your local storage, with cloud storage available as an additional option”; “no data [is] shared with third parties”; and “whether it’s your newborn crying for mom, or your victory dance after a game, your recorded footage will be kept private. Stored locally. With military-grade encryption. And transmitted to you, and only you.” *See* Doc. 45-1 at 24–25.

<sup>7</sup> Only one statement falls within this category: “On-Device AI[:] Our AI is built in to your security devices. It analyzes recorded video locally without the need to send it to the cloud for analysis.” *See* Doc. 45-1 at 25.

<sup>8</sup> These statements include “the camera products use ‘Military Grade AES-256 data encryption’”; and “End-to-end encryption[:] All recorded videos are encrypted from device to phone—only you have the key to decrypt and access your videos via the eufy Security app.” *See* Doc. 45-1 at 25.

statements in each of these categories are false or misleading. Plaintiffs allege that Defendants stored data acquired from their eufy products on a third-party cloud server, *see* Doc. 31 ¶¶ 44, 55, directly challenging the validity of Defendants’ statements regarding storage and streaming. Similarly, Plaintiffs allege Defendants stored data for facial recognition on their third-party cloud website, *see id.* ¶¶ 43, 53, challenging the representation that Defendants’ AI conducts facial recognition on a local server. Finally, Plaintiffs allege video streams could be accessed online without using secure encryption codes, *see id.* ¶¶ 42, 45, 64–65, challenging the statements that Defendants secure the captured video using military grade encryption. Defendants may ultimately prove that the statements at issue are true, but at this stage in the case, Plaintiffs have sufficiently alleged that the storage, encryption, and facial recognition statements may have misled a reasonable consumer and so they may proceed on those statements. *See, e.g., Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 776 (W.D.N.Y. 2017) (finding plaintiffs alleged materially misleading statements where Defendants stated on their website that they “would maintain adequate data privacy and security practices and procedures to safeguard . . . PII and PHI from unauthorized disclosure, release, data breaches, and cyber attack”), *on reconsideration on other grounds*, 304 F. Supp. 3d 333 (W.D.N.Y. 2018), *order clarified on unrelated grounds*, 502 F. Supp. 3d 724 (W.D.N.Y. 2020).

### **3. Omissions**

Defendants also argue that omissions cannot support claims under ICFA, Mass. Ch. 93A, or FDUPTA because omissions would not materially mislead a reasonable consumer.

Defendants identify four pleaded omissions: (1) thumbnails and biometric information would be stored on their cloud servers, (2) that such information would be sent without encryption, (3) that

such information would be subject to facial recognition off of their devices, and (4) that there would be unencrypted access to Plaintiffs' cameras.

When bringing a consumer fraud claim based on an omission, the omission must be “employed as a device to mislead.” *Spector v. Mondelez Int’l, Inc.*, 178 F. Supp. 3d 657, 672 (N.D. Ill. 2016); *see also Mack v. Cultural Care Inc.*, No. 1:19-CV-11530-ADB, 2020 WL 4673522, at \*8 (D. Mass. Aug. 12, 2020) (a statement is actionable under Mass. Ch. 93A “when it fails to disclose to a buyer or prospective buyer any fact, the disclosure of which may have influenced the buyer or prospective buyer not to enter into the transaction.”). An omission misleads a reasonable consumer when it creates an “affirmatively false impression” not just an incomplete thought. *Spector*, 178 F. Supp. 3d at 672. Plaintiffs must allege “direct statements that contain material omissions,” not just “opportunities or locations where [Defendants] could have disclosed the alleged defect.” *Guajardo v. Skechers USA, Inc.*, 503 F. Supp. 3d 746, 754 (C.D. Ill. 2020).

Defendants only challenge Plaintiffs' reliance on omissions to the extent that the omissions cannot be misleading because they do not track how the eufy products functioned. However, Plaintiffs have alleged that Defendants stored data for facial recognition on their third-party cloud website, *see* Doc. 31 ¶¶ 43, 53, and that video streams could be accessed online without using secure encryption codes, *see id.* ¶¶ 42, 45, 64-65. While discovery may ultimately prove that each of the stated omissions does not accurately describe how the eufy products function, at this stage, Plaintiffs have alleged enough to pursue their consumer fraud claims based on a theory of omissions for their ICFA and Mass. Ch. 93A claims.

However, Plaintiffs may not rely on omissions to further their FDUPTA claim. To proceed based on an omission, FDUPTA requires Plaintiffs to also allege a duty to disclose

based on a confidential, contractual, or fiduciary relationship. *See DJ Lincoln Enters., Inc. v. Google LLC*, No. 21-12894, 2022 WL 203365, at \*3 (11th Cir. Jan. 24, 2022). Plaintiffs have not included any allegations suggesting a confidential, contractual, or fiduciary relationship between Plaintiffs and Defendants, and Plaintiffs fail to address this argument in their response. Accordingly, the Court dismisses the FDUPTA claim to the extent that Plaintiffs rely on omissions to support it.

### **B. Causation**

Defendants also argue that Plaintiffs have not alleged causation with the particularity required by Rule 9(b). To establish causation for the consumer fraud claims, “a plaintiff must allege that he was, in some manner, deceived.” *Oliveira v. Amoco Oil Co.*, 201 Ill. 2d 134, 155 (2002); *Walsh v. TelTech Sys., Inc.*, 821 F.3d 155, 160 (1st Cir. 2016) (“To establish causation [for a claim under Mass. Ch. 93A], a plaintiff must prove that the defendant’s unfair or deceptive act caused an adverse consequence or loss.”). To do so, a “plaintiff must state in his complaint that he has seen the misleading statements of which he complains before he came into possession of the products he purchased.” *Goldemberg v. Johnson & Johnson Consumer Cos.*, 8 F. Supp. 3d 467, 480 (S.D.N.Y. 2014) (sufficient to establish causation where the plaintiff alleges the misleading advertising and states the misleading statements have already deceived plaintiff). Further, a plaintiff must allege that she was damaged by that deception. *See Oshana v. Coca-Cola Co.*, 472 F.3d 506, 513–14 (7th Cir. 2006). Notably, however, “the required allegation of proximate cause is minimal since that determination is best left to the trier of fact.” *Connick v. Suzuki Motor Co.*, 174 Ill. 2d 482, 504 (1996).

Here, Plaintiffs all allege that they personally saw some misrepresentations by Defendants, relied on those misrepresentations when purchasing their products, and consequently

experienced financial harm in overpaying for or purchasing that product. *See Muir v. Playtex Prods., LLC*, 983 F. Supp. 2d 980, 991 (N.D. Ill. 2013) (“By claiming that ‘he personally saw the misrepresentations [on the Diaper Genie II Elite package], was deceived by them, and was financially damaged as a result,’ Muir has adequately pleaded proximate cause.”). Sloan, Bleiberg, and Rothberger all plead the precise statements that they relied on when purchasing their products. *See* Doc. 31 ¶ 11 (“Prior to purchase, Sloan read and relied on Anker’s representations concerning the security and privacy of the Video Doorbell, including . . . whether it’s your newborn crying for mom, or your victory dance after a game, your recorded footage will be kept private. Stored locally. With military grade encryption. And transmitted to you and only you . . . [a]ll of your footage is securely stored locally . . . Had Sloan known that . . . his pictures and video were not encrypted . . . he would not have purchased the Camera Products or would have paid less.”); *id.* ¶ 12 (“Bleiberg chose to purchase a eufy camera, rather than competing products, because he read and relied on Defendants’ representations concerning the security and privacy features of eufy cameras, including their claims that eufy cameras operated with ‘no cloud,’ that only the user had access to images captured by the camera, and that eufy cameras used strong encryption.”); *id.* ¶ 13 (“Rothberger read and relied on Anker’s representations . . . including the representations that . . . [Y]our recorded footage will be kept private. Stored locally. With military-grade encryption. And transmitted to you and only you” and “[a]ll your footage is stored locally[,] [e]nsuring the videos you record are for you and only you”). In pleading the specific dates when they purchased the products and noting that they relied on the stated representations when making those purchases, Sloan, Bleiberg, and Rothberger all satisfy Rule 9(b).

While Farr, Desai, and Orpilla did not explicitly quote the representations on which they relied in the paragraph of the complaint describing their purchases, *see id.* ¶¶ 14, 16, 17, reading the complaint in its entirety reveals that Farr, Desai, and Orpilla do identify the statements on which they relied. Both Farr and Desai state they relied on the “privacy commitments as advertised on [ ] Anker’s eufy website.” *See id.* ¶ 14, 16. The complaint details the privacy commitment on Defendants’ website “during all relevant times,” which included statements that “all recorded videos are encrypted from device to phone—only you have the key to decrypt and access your videos via the eufy Security app” and “our AI is built in to your security devices. It analyzes recorded video locally without the need to send it to the cloud for analysis.” *Id.* ¶ 33. Similarly, Orpilla stated he “reviewed the accompanying labels and disclosures” on the eufy products he purchased. *Id.* ¶ 17. As Plaintiffs allege, “each of the camera products, on the product’s label, advertises and warrants” statements including that the videos were “stored locally [,] [w]ith military-grade encryption” and “transmitted to you, and only you.” *Id.* ¶ 32. Reviewing the allegations together and in the light most favorable to Plaintiffs Farr, Desai, and Orpilla, they have met the particularity requirement of Rule 9(b) in alleging causation.

### **C. Extraterritoriality under the ICFA**

Finally, Defendants move to dismiss any non-Illinois resident Plaintiffs and classes from the ICFA count on extraterritoriality grounds. Like their BIPA claims, only Plaintiffs residing in Illinois, Sloan and Orpilla, have alleged sufficient facts to establish that the misrepresentation substantially occurred in Illinois. *See Crichton v. Golden Rule Ins. Co.*, 576 F.3d 392, 396 (7th Cir. 2009) (“[F]or a nonresident plaintiff to have standing under the [Illinois Consumer Fraud] Act, the court required that ‘the circumstances that relate to the disputed transaction occur

primarily and substantially in Illinois.” (citing *Avery*, 216 Ill. 2d at 187). Accordingly, the Court dismisses the ICFA claim as to any non-Illinois resident Plaintiffs or classes.

## **V. Unjust Enrichment**

Defendants’ sole argument to dismiss Plaintiffs’ unjust enrichment claim is the failure of Plaintiffs’ consumer fraud claims. Unjust enrichment claims “stand or fall with the related claim” when “an unjust enrichment claim rests on the same improper conduct alleged in another claim.” *Cleary v. Philip Morris Inc.*, 656 F.3d 511, 517 (7th Cir. 2011). As detailed above, the Court dismisses Plaintiffs’ consumer fraud claims to the extent they rely on statements related to privacy because those statements are puffery and the FDUPTA claim based on any omissions. Plaintiffs’ unjust enrichment claims cannot rely on those statements. However, as Defendants do not argue any other basis to dismiss Plaintiffs’ unjust enrichment claims, the Court otherwise allows the claim to proceed.

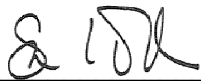
## **CONCLUSION**

For the foregoing reasons, the Court grants in part and denies in part Defendants’ motion to dismiss [45]. The Court dismisses Plaintiffs’ Wiretap Act claim (Count III) in its entirety without prejudice. The Court dismisses Plaintiffs’ BIPA claim (Count IV) as to all non-Illinois resident Plaintiffs without prejudice; Sloan, Orpilla, and the Illinois class may proceed on the BIPA claim. The Court dismisses without prejudice Plaintiffs’ consumer fraud claims (Counts I, II, V, VI) and their unjust enrichment claim (Count VII) to the extent they rely on the statements related to privacy identified above, Plaintiffs’ ICFA claim (Count I) for non-Illinois residents, and Plaintiffs’ FDUPTA claim (Count VI) to the extent it relies on omissions. Finally, because



Commerford and Lapating no longer have any viable claims, the Court also dismisses them as named Plaintiffs.

Dated: January 9, 2024

  
\_\_\_\_\_  
SARA L. ELLIS  
United States District Judge