

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS**

M.C. 1 and M.C. 2, by and through their legal guardian NICOLE REISBERG, and M.C. 3 and M.C. 4, by and through their legal guardian LILA BYOCK, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

CURRICULUM ASSOCIATES, LLC

Defendant.

Civ. No. 1:25-cv-13942-FDS

**PLAINTIFFS' OPPOSITION TO DEFENDANT CURRICULUM
ASSOCIATES, LLC'S MOTION TO DISMISS COMPLAINT**

TABLE OF CONTENTS

I. PRELIMINARY STATEMENT.....1

II. LEGAL STANDARD.....1

III. ARGUMENT.....1

 A. Privacy laws do not absolve CA of its duty to obtain parental consent.....1

 B. Plaintiffs state a claim under ECPA and CIPA section 631.....5

 C. Plaintiffs state a claim under CIPA section 632.....10

 D. Plaintiffs state a pen-register claim.....12

 E. Plaintiffs state a CDAFA claim.....14

 F. Plaintiffs’ Massachusetts Privacy Act Claim should be sustained.....16

 G. Plaintiffs adequately allege that CA violated Chapter 93A.19

 H. Plaintiffs properly state an unjust enrichment claim in the alternative.....22

 I. Plaintiffs’ negligence claim should be sustained.24

IV. CONCLUSION.....25

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Amyndas Pharmaceuticals, S.A. v. Zealand Pharma A/S</i> , 48 F.4th 18 (1st Cir. 2022).....	25
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	1
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	1
<i>Bevilacqua v. Rodriguez</i> , 460 Mass. 762 (2011).....	1
<i>Biden v. Ziegler</i> , 737 F. Supp. 3d 958 (C.D. Cal. 2024).....	15
<i>Bignami v. Serrano</i> , 2020 WL 2257312 (Mass. Land Ct. May 7, 2020).....	17
<i>Brown v. Google LLC</i> , 685 F. Supp. 3d 909 (N.D. Cal. 2023).....	15
<i>BRV, Inc. v. Superior Ct.</i> , 143 Cal. App. 4th 742 (2006).....	2
<i>Cabral v. I.N.S.</i> , 15 F.3d 193 (1st Cir. 1994).....	5
<i>Calhoun v. Google, LLC</i> , 113 F.4th 1141 (9th Cir. 2024).....	16
<i>Champa v. Weston Pub. Schs.</i> , 473 Mass. 86 (2015).....	18
<i>Cherkin v. PowerSchool Holdings, Inc.</i> , 2025 WL 844378 (N.D. Cal. Mar. 17, 2025).....	3, 9, 12, 15
<i>Costa v. Zurich Am. Ins. Co.</i> , 2024 WL 5057723 (D. Mass. Dec. 10, 2024).....	21
<i>D’Angelo v. FCA US, LLC</i> , 726 F. Supp. 3d 1179 (S.D. Cal. 2024).....	7, 8
<i>Deivaprakash v. Condé Nast Digital</i> , 798 F. Supp. 3d 1100 (N.D. Cal. 2025).....	13
<i>Doe v. Baystate Health Sys., Inc.</i> , 2026 WL 776861 (D. Mass. Mar. 19, 2026).....	18
<i>Doe v. Lawrence General Hospital</i> , 2025 WL 2808055 (D. Mass. Aug. 29, 2025).....	7
<i>Doe v. Tenet Healthcare Corp.</i> , 731 F. Supp. 3d 142 (D. Mass. 2024).....	24
<i>Doe v. Thorell</i> , 106 Mass. App. Ct. 532 (2026).....	18
<i>Egan v. X-Mode Soc., Inc.</i> , 2024 WL 2701967 (D. Mass. May 24, 2024).....	21

Frasco v. Flo Health, Inc.,
 2025 WL 2680068 (N.D. Cal. Sept. 17, 2025).....11

Frazier v. Fairhaven Sch. Comm.,
 276 F.3d 52 (1st Cir. 2002)..... 3

Gonzaga Univ. v. Doe,
 536 U.S. 273 (2002) 3

Graham v. Noom, Inc.,
 533 F. Supp. 3d 823 (N.D. Cal. 2021)..... 8

Great Am. Ins. Co. v. Riso, Inc.,
 479 F.3d 158 (1st Cir. 2007)..... 25

Grp., Inc. v. Hewitt,
 598 U.S. 39 (2023) 2

Heiting v. Taro Pharmaceuticals USA, Inc.,
 709 F. Supp. 3d 1007 (C.D. Cal. 2023)..... 16

Hernandez-Silva v. Instructure, Inc.,
 2025 WL 2233210 (C.D. Cal. Aug. 4, 2025) 9

Hershenow v. Enterprise Rent-A-Car Co. of Bos.,
 445 Mass. 790 (2006)..... 20

Hiles v. Episcopal Diocese of Mass.,
 437 Mass. 505 (2002)..... 1

I.C. v. Zynga, Inc.,
 600 F. Supp. 3d 1034 (N.D. Cal. 2022)..... 12

In re Apple Data Priv. Litig.,
 2026 WL 146025 (N.D. Cal. Jan. 20, 2026) 14

In re Facebook, Inc. Internet Tracking Litig.,
 956 F.3d 589 (9th Cir. 2020) 15

In re TikTok, Inc., Minor Privacy Litig.,
 2025 WL 3628598 (C.D. Cal. Nov. 5, 2025) 12

Jones v. Google LLC,
 73 F.4th 636 (9th Cir. 2023) 12

Karp v. Gap, Inc.,
 2014 WL 4924229 (D. Mass. Sep. 29, 2014)..... 23

Kattar v. Demoulas,
 739 N.E.2d 246 (Mass. 2000) 21

L.B. v. LinkedIn Corp.,
 2025 WL 2899514 (N.D. Cal. Oct. 10, 2025)11

Lass v. Bank of Am., N.A.,
 695 F.3d 129 (1st Cir. 2012)..... 22, 23

Lionetta v. InMarket Media, LLC,
 798 F. Supp. 3d 139 (D. Mass. 2025)..... 20, 22, 23, 24

Lopez v. Sony Electronics, Inc.,
 5 Cal. 5th 627 (2018)..... 14

Mahoney v. Wells Fargo Bank, N.A.,
 2021 WL 1178377 (D. Mass. Mar. 29, 2021)..... 21

Massachusetts Eye & Ear Infirmary v. QLT Phototherapeutics, Inc.,
 552 F.3d 47 (1st Cir.)..... 23

McDermott v. Marcus, Errico, Emmer & Brooks, P.C.,
 911 F. Supp. 2d 1 (D. Mass. 2012)..... 15

McManus v. Tufts Med. Ctr., Inc.,
 2025 WL 2778025 (D. Mass. Sep. 29, 2025)..... 7

Mekhail v. N. Mem’l Health Care,
 726 F. Supp. 3d 916 (D. Minn. 2024) 6

Mirmalek v. L.A. Times Comms. LLC,
 2024 WL 5102709 (N.D. Cal. Dec. 12, 2024) 13

Mitchener v. CuriosityStream, Inc.,
 2025 WL 2272413 (N.D. Cal. Aug. 6, 2025) 12

Monks v. Astoria Bank,
 2017 WL 2435278 (D. Mass. June 5, 2017)..... 6

Morrissey v. New England Deaconess Association—Abundant Life Communities, Inc.,
 57 N.E.3d 1066 (Mass. App. Ct. 2016)..... 22

Neang Chea Taing v. Napolitano,
 567 F.3d 19 (1st Cir. 2009)..... 5

Nightingale v. National Grid USA Serv. Co.,
 107 F.4th 1 (1st Cir. 2024)..... 20

Polay v. McMahan,
 468 Mass. 379 (2014)..... 16

Powers v. Receivables Performance Mgmt., LLC,
 801 F. Supp. 3d 17 (D. Mass. 2025)..... 20

Priddy v. ZOLL Medical Corp.,
 2025 WL 975234 (D. Mass. Mar. 31, 2025) 20, 21

Q.J. v. PowerSchool Holdings LLC,
 2025 WL 2410472 (N.D. Ill. Aug. 20, 2025) 9

Rafferty v. Merck & Co., Inc.,
 479 Mass. 141 (2018)..... 21

Ragusa v. Malverne Union Free Sch. Dist.,
 549 F. Supp. 2d 288 (E.D.N.Y. 2008) 2

Rodriguez v. Culligan Int’l Co.,
 2025 WL 3064113 (S.D. Cal. Nov. 3, 2025)..... 12

Rodriguez v. Ford Motor Co.,
 722 F. Supp. 3d 1104 (S.D. Cal. Mar. 21, 2024)..... 10, 15

Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc.,
 409 Mass. 514 (1991)..... 19

Shah v. Fandom, Inc.,
 754 F. Supp. 3d 924 (N.D. Cal. 2024)..... 13

Shedd v. Sturdy Mem’l Hosp., Inc.,
 2022 WL 1102524 (Mass. Super. Apr. 5, 2022) 16, 22, 25

Small Just, LLC v. Xcentric Ventures LLC,
 2014 WL 1214828 (D. Mass. Mar. 24, 2014) 21

Smith v. Rack Room Shoes, Inc.,
 2025 WL 2210002 (N.D. Cal. Aug. 4, 2025) 6, 15

Smith v. YETI Coolers, LLC,
 754 F. Supp. 3d 933 (N.D. Cal. 2024)..... 11

Squeri v. Mount Ida College,
 954 F.3d 56 (1st Cir. 2020)..... 16

Squeri v. Mount Ida College,
 2019 WL 2249722 (D. Mass. May 24, 2019)..... 19

Steinmetz v. Coyle & Caron, Inc.,
 862 F.3d 128 (1st Cir. 2017)..... 21

Tate v. VITAS Healthcare Corp.,
 762 F. Supp. 3d 949 (E.D. Cal. 2025) 8

Taylor v. ConverseNow Techs., Inc.,
 2025 WL 2308483 (N.D. Cal. Aug. 11, 2025)11

Transamerica Ins. Co. v. KMS Patriots, L.P.,
 52 Mass. App. Ct. 189 (2001) 25

Turner v. Google LLC,
 737 F. Supp. 3d 869 (N.D. Cal. 2024).....11

Valenzuela v. Kroger Co.,
 2024 WL 1336959 (C.D. Cal. Mar. 28, 2024)..... 10

Valenzuela v. Nationwide Mut. Ins. Co.,
 686 F. Supp. 3d 969 (C.D. Cal. 2023)..... 8

Vass v. Blue Diamond Growers,
 2015 WL 9901715 (D. Mass. Aug. 11, 2015) 22

Vernonia School Dist. 47J v. Acton,
 515 U.S. 646 (1995)11, 12

Walgreen Co. v. Haseotes,
 778 F. Supp. 3d 264 (D. Mass. 2025)..... 6, 7

Webb v. Injured Workers Pharmacy, LLC,
 72 F.4th 365 (1st Cir. 2023)..... 20, 24

Williams v. Steward Health Care Sys., LLC,
 480 Mass. 286 (2018)..... 24

Zielenski v. Citizens Bank, N.A.,
 552 F. Supp. 3d 60 (D. Mass. 2021)..... 20

Statutes

15 U.S.C. § 6501 4, 5

15 U.S.C. § 6502 4, 5

18 U.S.C. § 2511(2)(d)..... 6

20 U.S.C. § 1232g..... 2, 3

Cal. Bus. & Prof. Code § 22584(b)(4) 3

Cal. Civ. Code § 1798.100(c)..... 13

Cal. Educ. Code § 49076(a)(2) 2

Cal. Penal Code § 631 7, 8

Cal. Penal Code § 632.....10, 11

MASS. GEN. LAW ch. 93A 20

MASS. GEN. LAWS ch. 214 § 1B..... 16

Regulations

16 C.F.R. § 312 4, 5, 12
34 C.F.R. § 99 2, 3
64 Fed. Reg. 59888 (Nov. 3, 1999)..... 5
603 CMR 23 17

Other Authorities

144 Cong. Rec. S8483 4
Brief for Amicus Curiae Federal Trade Commission in Support of Appellees, Shanahan v. IXL Learning, Inc., No. 24-6985 (9th Cir. Aug. 13, 2025), available at https://www.ftc.gov/system/files/ftc_gov/pdf/ShanahanAmicusBriefFiled.pdf..... 4

I. PRELIMINARY STATEMENT

Defendant Curriculum Associates (“CA”) opens its motion by engaging in *ad hominem* attacks against Plaintiffs and their counsel to distract from the well-pleaded facts of Plaintiffs’ complaint (“Complaint”), which plausibly alleges that CA commercially exploits millions of K-12 students’ personal information without effective consent. Plaintiffs are K-12 students compelled by their schools to use CA’s i-Ready assessment and personalized-instruction products (“i-Ready”) on school-issued devices. They allege injuries including invasion of privacy, exposure of sensitive educational behavior and outcomes, violation of statutory information rights, economic loss through unjust enrichment, and risks from both first-party and third-party sharing and profiling.

II. LEGAL STANDARD

To survive a Rule 12(b)(6) challenge, a plaintiff must allege “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A court must accept all allegations as true, and a claim has “facial plausibility” if the plaintiff pleads facts that “allow[] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Courts resolve facial attacks under Rule 12(b)(1) as they would a motion under Rule 12(b)(6). *See Bevilacqua v. Rodriguez*, 460 Mass. 762, 764 (2011); *Hiles v. Episcopal Diocese of Mass.*, 437 Mass. 505, 516 n.13 (2002).

III. ARGUMENT

A. Privacy laws do not absolve CA of its duty to obtain parental consent.

CA attempts to minimize the issue of consent by advancing its arguments only in the introduction and background, Mot. at 1-2, but this case is primarily about consent. As stated in the Complaint, “there is one question at the heart of this case: Does [CA] obtain effective consent before taking, using, and sharing *any* personal information from students in the compulsory setting

of K–12 education, let alone vast troves of it, as [CA] admits to doing?” ¶ 10.¹ CA may not avoid the central issue by artful briefing or by mischaracterizing it as an irrelevant “policy” matter.

CA contends that a “longstanding regulatory framework” purportedly absolves companies from obtaining parental consent in the context of K-12 education, citing statutes enacted to *protect* children’s informational privacy and parents’ rights over their children’s information. Mot. at 1-2. CA argues that exceptions to these statutes’ parental-consent requirements actually *eliminate* all such requirements. In support, it advances a policy argument—that schools “need support” from service providers like CA. *Id.* at 2. But Plaintiffs allege that CA’s student-data practices far exceed that contemplated by the exceptions to broad, express parental-consent requirements. Construing the statutes as CA suggests would thus turn these privacy statutes on their heads. The Supreme Court has made clear that “even the most formidable policy arguments cannot overcome a clear textual directive.” *Helix Energy Sols. Grp., Inc. v. Hewitt*, 598 U.S. 39, 59 (2023) (cleaned up).

FERPA does not provide a private defense. CA first contends that the Family Educational Rights and Privacy Act (“FERPA”) and analogous California state law absolve it of its duty to obtain parental consent before harvesting student data. Mot. at 2 (citing 34 C.F.R. § 99.31(a)(1)(i)(A); Cal. Educ. Code § 49076(a)(2)).² It argues that these laws “authorize schools to share student data with service providers for legitimate educational purposes—as determined by the school—without express parental consent.” *Id.* But FERPA regulates schools, not private companies. 20 U.S.C. § 1232g(a). It is a funding statute that “seeks to deter schools from adopting policies of releasing student records.” *Ragusa v. Malverne Union Free Sch. Dist.*, 549 F. Supp. 2d 288, 291 (E.D.N.Y. 2008). Accordingly, the U.S. Supreme Court has held that FERPA creates no

¹ Throughout Plaintiffs’ Opposition, “¶” citations refer to the Complaint [Dkt. 1].

² For brevity, this response refers to FERPA, which does not materially differ from California’s law, and CA does not appear to argue otherwise. See *BRV, Inc. v. Superior Ct.*, 143 Cal. App. 4th 742, 751-52 (2006) (law adopted “to eliminate potential conflicts between FERPA and state law”).

private rights. *Gonzaga Univ. v. Doe*, 536 U.S. 273, 290 (2002).

Further, construing FERPA as CA advocates would produce the absurd result of creating rights for private companies but not for students and their parents—those for whom the statute was enacted to protect—leaving them *less* protected than if the statute had not been enacted. *Frazier v. Fairhaven Sch. Comm.*, 276 F.3d 52, 67-68 (1st Cir. 2002) (FERPA enacted to assure student privacy by requiring parental consent). It would insulate companies against liability without providing a mechanism for holding them accountable. An interpretation so fundamentally at odds with the statute’s express purpose is impermissible. *Cherkin v. PowerSchool Holdings, Inc.*, 2025 WL 844378, *2 (N.D. Cal. Mar. 17, 2025) (rejecting similar arguments).

Even if FERPA could be construed as creating a private defense, analysis of whether a service provider like CA handles student information in compliance with the so-called “school official” exception is fact intensive. *See* 20 U.S.C. § 1232g(b)(1)(A); 34 C.F.R. § 99.33(a). Plaintiffs have plausibly alleged that CA does not. ¶¶ 118-21 (data taken by CA exceeds “education records”); ¶ 282 (schools do not control CA’s data practices); ¶ 294 (CA uses student data in excess of “legitimate educational purposes” and it impermissibly rediscloses it without parental consent).

SOPIPA does not obviate parental-consent requirements. CA cites another student-privacy law it contends obviates all parental-consent requirements, California’s Student Online Personal Information Protection Act (“SOPIPA”). Mot. at 2 (citing Cal. Bus. & Prof. Code § 22584(b)(4)). Plaintiffs allege that CA’s data practices do not comport with that narrow exception. They allege CA takes, uses, and shares student information, not only to allow or improve operability and functionality, but also to create invasive, persistent digital student profiles, ¶¶ 139, 144, 150-65, 203-05, 233; for advertising, ¶¶ 170, 184, 191-207, 239-42; to conduct marketing research, ¶¶ 140, 167; to test and build new products, including AI technologies, ¶¶ 143,

145, 147; and to secure commercially valuable third-party data-sharing agreements, ¶¶ 174-82.

Nothing in these student-privacy laws imbues schools or their vendors with virtually unlimited authority to exploit student information for nebulously defined “education purposes” or “product operability.” CA’s interpretation of these statutes would wholly subvert their legislative intent, transforming limited exceptions to parental consent into gaping pathways for the undisclosed, nonconsensual, mass transfer of student information to the private sector. Basic canons of statutory construction preclude CA’s ends-driven interpretation of these privacy laws.

COPPA does not permit schools to provide consent in lieu of parents. CA further argues that the FTC has absolved companies of their duty to obtain parental consent in the context of K–12 education. Mot. at 2 n.2. It misleadingly states that, “[f]or more than two decades, the Federal Trade Commission (“FTC”) has published guidance confirming that schools can consent on behalf of parents to the collection of personal information for educational purposes.” *Id.* In support, it cites FTC guidance to the Children’s Online Privacy Protection Act (“COPPA”). However, as the FTC recently clarified, its guidance does not “remotely support” the position that schools can stand in the shoes of parents for purposes of consenting to a private vendor’s terms of service.³

COPPA is a federal statute enacted to afford children under 13 greater data-privacy protections by expanding parents’ rights over what information internet companies may collect about their children and how that information may be used. *See* 15 U.S.C. § 6501 *et seq*; 144 Cong. Rec. S8483 (July 17, 1998). COPPA creates a detailed regulatory regime governing a company’s collection and use of children’s data. Among its terms are heightened parental notice-and-consent requirements and parental rights to access and control their child’s data. 15 U.S.C. § 6502; 16

³ *See* Brief for Amicus Curiae Federal Trade Commission in Support of Appellees at 18-19, *Shanahan v. IXL Learning, Inc.*, No. 24-6985 (9th Cir. Aug. 13, 2025), available at https://www.ftc.gov/system/files/ftc_gov/pdf/ShanahanAmicusBriefFiled.pdf.

C.F.R. §§ 312.3-.10. The enabling statute and implementing rule expressly require that a company obtain verifiable *parental* consent before it may collect and use children’s personal information. *See* 15 U.S.C. § 6501 *et seq.*, 16 C.F.R. § 312.1 *et seq.* They do not authorize schools to provide consent in lieu of parents. In fact, they do not even mention schools.

Instead of citing the COPPA statute or rule, CA cites the Statement of Basis and Purpose (“SBP”) that accompanied the Rule when first promulgated for the proposition that “online operators can rely on school authorization.” Mot. at 2 n.2 (citing 64 Fed. Reg. 59888, 59903 (Nov. 3, 1999)). First, CA materially misrepresents the language of those comments, which state only that, under certain circumstances, companies “can presume” that schools have obtained parental consent—not that companies may rely on school authorization in lieu of parental consent. 64 Fed. Reg. at 59903. Second, CA cites no authority that would allow this Court to even consider those extratextual comments in the absence of statutory ambiguity. *See Neang Chea Taing v. Napolitano*, 567 F.3d 19, 23 (1st Cir. 2009) (“If the statutory text is plain and unambiguous, the court ‘must apply the statute according to its terms.’”) (cleaned up); *see also Cabral v. I.N.S.*, 15 F.3d 193, 194 (1st Cir. 1994). And the COPPA statute expressly and unambiguously identifies the exceptions to parental consent, none of which includes school technology. 15 U.S.C. § 6502(b)(2).

The absence of valid consent is the throughline of every claim in this case: it defeats CA’s invocation of the wiretap party exception; renders its data practices unauthorized, unjust, and unfair under state law; and confirms the highly offensive nature of CA’s intrusion into Plaintiffs’ privacy. Because Plaintiffs plausibly allege that CA did not obtain effective consent before taking, using, and sharing Plaintiffs’ personal information, dismissal is unsupported.

B. Plaintiffs state a claim under ECPA and CIPA section 631.

The party exception does not apply. CA erroneously argues that the party exception to the

ECPA and CIPA requires dismissal of Plaintiffs' claims. Mot. at 4-5. It does not.

First, the party exception to the ECPA applies only if a defendant, when intercepting communications, did not intend to commit a crime or tort. *See Mekhail v. N. Mem'l Health Care*, 726 F. Supp. 3d 916, 927 (D. Minn. 2024) (exception inapplicable if party intercepts communication ““for the purpose of committing any criminal or tortious act in violation of”” state or federal law) (quoting 18 U.S.C. § 2511(2)(d)). Here, the crime-tort exception precludes the party exception because the Complaint alleges that CA tortiously obtained student data without parental consent in violation of federal and state law, including by using third parties' tracking technologies. ¶¶ 9, 11-16, 20, 34-37, 121-23, 171, 182, 254-85, 288-90, 292-95. These allegations support the inference that CA intercepted and disclosed those communications for the purpose of committing tortious acts, including invasion of privacy, ¶ 367, and unfair and deceptive practices under Chapter 93A, such as obtaining and exploiting Plaintiffs' data through false and misleading statements, ¶¶ 287, 484, 491. *See Smith v. Rack Room Shoes, Inc.*, 2025 WL 2210002, at *5 (N.D. Cal. Aug. 4, 2025) (retaining ECPA claim where invasion of privacy alleged); *Monks v. Astoria Bank*, 2017 WL 2435278, at *4 (D. Mass. June 5, 2017) (where “a claim for a violation of Chapter 93A is based on a false representation . . . the claim sounds in tort.”) (citation omitted).

The Complaint further alleges that CA's interception and disclosure of Plaintiffs' data constituted conversion. ¶¶ 486-87. Courts in this District have recognized that the unauthorized taking and use of valuable, non-public data for a defendant's own benefit can constitute conversion. *Walgreen Co. v. Haseotes*, 778 F. Supp. 3d 264, 296 (D. Mass. 2025) (“intangible property rights may be the subject of conversion if they customarily merge in or identify with certain kinds of documents.”) Here, Plaintiffs have alleged that their data is property capable of being converted because CA generates reports using student data. ¶¶ 50-51, 57, 59, 66-67, 73, 79-

80, 84-87, 96-97, 102, 108, 140, 153-54. As in *Walgreen*, Plaintiffs allege that CA appropriated non-public information and exercised dominion over it by using and disclosing it for its own commercial purposes and for the benefit of third parties. ¶¶ 34-36, 45-48, 147-150, 166-174, 183-253. Although student data differs from business operational data, Plaintiffs plausibly allege that their data carries independent economic and functional value, making it susceptible to wrongful control. ¶¶ 34-39, 147-253.

This case is thus fundamentally different from *Doe v. Lawrence General Hospital*, where the court found no independent tort or criminal purpose beyond the interception itself. 2025 WL 2808055, at *13 (D. Mass. Aug. 29, 2025) (“*LGH*”). Here, Plaintiffs plausibly allege that CA intercepted and disclosed their data for the independent purpose of exploiting it for commercial gain—including through Chapter 93A violations and conversion—conduct that goes beyond the interception. *McManus v. Tufts Med. Ctr., Inc.* is likewise inapposite because Plaintiffs do not rely on a generalized “financial motive” alone, 2025 WL 2778025, at *3 (D. Mass. Sep. 29, 2025), but allege interception for the purpose of committing those separate torts. Further, *LGH* confirms that ordinary financial motives do not defeat the crime–tort exception where the interception facilitates a distinct tortious use of the data. 2025 WL 2808055, at *20.

Second, the party exception does not apply to CIPA claims when the party “aids, agrees with, employs, or conspires with” another to eavesdrop on communications in real time for that party’s own purpose. *D’Angelo v. FCA US, LLC*, 726 F. Supp. 3d 1179, 1202 (S.D. Cal. 2024) (quoting Cal. Penal Code § 631(a)). Plaintiffs allege that CA maintains a network of third parties that provide services or payment to CA in return for CA installing those parties’ tracking tools to intercept data from its products in real time for their own benefit, ¶¶ 169-70, 172-74, 178-81, 183-253, and unknown to the students whose information is intercepted, ¶¶ 20, 125-34, 137, 168, 170,

173, 202, 258-65, 349-50, 364. See *D'Angelo*, 726 F. Supp. 3d at 1202 (“[P]ermitting an entity to engage in the unauthorized duplication and forwarding of unknowing users’ information would render permissible the most common methods of intrusion, allowing the exception to swallow the rule.”) (cleaned up); *Valenzuela v. Nationwide Mut. Ins. Co.*, 686 F. Supp. 3d 969, 981 (C.D. Cal. 2023) (rejecting *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823 (N.D. Cal. 2021)).

Third-party interception. CA contends that it cannot be liable for aiding third-party violations of CIPA under the fourth clause of section 631(a) because “CIPA does not impose liability for a party’s disclosure of data to service providers that merely store or analyze that data for its own use.” Mot. at 6 (citing *Graham*, 533 F. Supp. 3d at 832).

Graham is inapplicable. First, Plaintiffs allege that third-party recipients of the data use the data for their own benefit. ¶¶ 6-7, 36, 170, 174, 181, 195, 203-04, 231-53. Second, courts have broadly rejected *Graham*’s third-party “use” requirement in favor of a requirement that plaintiffs allege facts showing that a third party *is capable* of using intercepted data for the third party’s own benefit. See *Tate v. VITAS Healthcare Corp.*, 762 F. Supp. 3d 949, 954-57 (E.D. Cal. 2025); *D'Angelo*, 726 F. Supp. 3d at 1200-02. And the Complaint extensively alleges that numerous third parties can use data they intercepted from Plaintiffs in real time due to CA’s help, including advertising, marketing, and identity-resolution companies and at least one data broker. ¶¶ 6-7, 36, 169-70, 173-74, 179-81, 183-253; see also *Tate*, 762 F. Supp. 3d at 956 (allegations sufficient that third party’s terms of service stated that it *may* use data obtained from calls to defendant for its own purposes); *D'Angelo*, 726 F. Supp. 3d at 1201 (allegations sufficient that third party “harvest[ed]” and “exploit[ed]” data collected from chat conversations for financial gain and “analyze[d]” conversations for its own “business purposes”); *Valenzuela*, 686 F. Supp. 3d at 979-81 (allegations sufficient that third-party’s business model was harvesting data from

communications made on defendant's website).

In-transit interception. CA argues that the Complaint lacks any allegations as to M.C. 1, M.C. 2, and M.C. 4 that the contents of their communications were intercepted by third parties while in transit because part of Plaintiffs' forensic analysis focused on the interception of data from M.C. 3 and students who use Chromebooks. Mot. at 7. But the Complaint extensively alleges in transit interception for all four Plaintiffs, including alleging that categories of intercepted data vary by CA product, not by student, school, or school district, ¶¶ 185-86; forensic testing was conducted on M.C. 3's Chromebook and M.C. 4's iPad, ¶ 187; any student interaction with the i-Ready platform for a diagnostic assessment or personalized lesson causes information about the student and their activity to be recorded and instantaneously transmitted to third parties outside of CA, ¶ 189; all four named plaintiffs have school-required Google profiles that, along with Google's tracking tools installed on CA's products, allow Google to identify each student, ¶¶ 216-30; and Google's marketing and tracking tools automatically send students' data to Google in real-time every time any student loads the i-Ready homepage or any i-Ready page, ¶¶ 231-32. *See generally* ¶¶ 183-253. These allegations support a reasonable inference of contemporaneous interception.

Further, CA relies on *Hernandez-Silva v. Instructure, Inc.*, 2025 WL 2233210, *5 (C.D. Cal. Aug. 4, 2025), but the allegations in *Instructure* did not contain forensic analysis. Here, the Complaint extensively alleges how CA intercepted Plaintiffs' communications—and aided third parties' interception of Plaintiffs' communications—in real time through application programming interface technology and installing tracking tools in its products, allegations supported by forensic evidence. ¶¶ 183-253. Other courts have upheld wiretapping claims in similar cases. *See, e.g., Cherkin*, 2025 WL 844378, at *5; *Q.J. v. PowerSchool Holdings LLC*, 2025 WL 2410472, at *1, 8 (N.D. Ill. Aug. 20, 2025).

CA aided third-party interception. CA contends that, as to M.C. 3, Plaintiffs do not allege that CA aided Google’s misconduct because they do not allege that CA knew about Google’s misconduct. Mot. at 7-8. But Plaintiffs allege that CA was aware of Google’s mass surveillance of Americans through tracking technologies and purposefully installed those trackers onto CA’s platforms where reams of children’s data would be sent to Google without notice or consent. ¶¶ 197, 207. The Complaint also alleges that CA knowingly assists Google’s interception of student data. For example, it alleges that CA installs Google’s surveillance software, including tracking pixels, on its products in exchange for Google’s proprietary suites of marketing, advertising, and customer-analytics software, including Google Analytics, Google AdSense, and Google Tag Manager. ¶¶ 191-230. It further alleges that when any student loads any i-Ready page, such as the homepage, dashboard, or a lesson, the action triggers certain Google marketing and tracking tools, which then automatically record and transmit the student’s interactions to Google in real time. ¶¶ 231-32.⁴ The cases CA cites are distinguishable. *Valenzuela v. Kroger Co.*, 2024 WL 1336959, at *4 (C.D. Cal. Mar. 28, 2024) (allegation insufficient where plaintiff alleged that defendant knew that third party “captured” communications via code that defendant “allowed” third party to embed); *Rodriguez v. Ford Motor Co.*, 722 F. Supp. 3d 1104, 1124 (S.D. Cal. Mar. 21, 2024) (allegation insufficient where plaintiff alleged defendant knew third party “captured” data). Here, Plaintiffs allege that CA itself installed Google’s tracking tools in its products in exchange for services from Google. ¶¶ 183-253.

C. Plaintiffs state a claim under CIPA section 632.

CA initially argues that Plaintiffs’ section 632 claim fails for two reasons raised in Section

⁴ CA cites an allegation (¶ 233) it contends implies “that M.C. 3’s Chromebook and/or Google Classroom facilitate the collection and disclosure of M.C. 3’s data.” Mot. at 7-8. But that allegation explicitly states that “i-Ready causes” the student data to be sent to Google, and other allegations describe how i-Ready does so. ¶¶ 191-253.

B, *supra*—that Plaintiffs do not allege that (1) as to M.C. 3, CA knew about Google’s misconduct; and (2) as to M.C. 1, M.C. 2, and M.C. 4, any third parties eavesdropped on their communications. Mot. at 8. But again, the Complaint thoroughly alleges that CA has knowledge about and actively assists Google’s recording of student communications. ¶¶ 183-253. Plaintiffs plead that CA aided Google and other third parties to record Plaintiffs’ communications. ¶¶ 183-253.

CA next argues that “internet communications” are not “confidential communications” under section 632 because Plaintiffs have no reasonable expectation of privacy in them. Mot. at 8. But courts routinely hold that internet communications can have sufficient confidential character to support a section 632 claim. *See, e.g., L.B. v. LinkedIn Corp.*, 2025 WL 2899514, *18 (N.D. Cal. Oct. 10, 2025) (health information); *Taylor v. ConverseNow Techs., Inc.*, 2025 WL 2308483, *7-8 (N.D. Cal. Aug. 11, 2025) (financial information); *Frasco v. Flo Health, Inc.*, 2025 WL 2680068, *7, 10 (N.D. Cal. Sept. 17, 2025) (health information). CA fails to demonstrate, beyond factual dispute, that allegations that children whose communications were intercepted while doing schoolwork cannot meet that standard. ¶¶ 423, 425-27, 431; *Turner v. Google LLC*, 737 F. Supp. 3d 869, 884 (N.D. Cal. 2024) (minors alleged reasonable expectation of privacy in personal data disclosed on apps); *Smith v. YETI Coolers, LLC*, 754 F. Supp. 3d 933, 943 (N.D. Cal. 2024) (this “fact-intensive inquiry” is “often too difficult to resolve at the pleadings stage”) (cleaned up).

CA contends student communications are not “confidential communications” because “students within the school environment have a lesser expectation of privacy than members of the population generally.” Mot. at 9. CA cites *Vernonia School Dist. 47J v. Acton*, which involved a school district’s student-athlete drug policy and noted that “with regard to medical examinations and procedures,” and even more so with student athletes, students “have a lesser expectation of privacy” than the general population. 515 U.S. 646, 656-57 (1995). But that court addressed only

students' expectation of privacy as to the district's actions, not private companies, and did not address student communications. *Id.* Here, Plaintiffs' privacy interest in their personal information—which includes statutorily protected education records—“is expressly recognized in federal and California state law,” *Cherkin*, 2025 WL 844378, at *2. That interest does not vanish simply because student information is collected through software instead of paper.

D. Plaintiffs state a pen-register claim.

CA first contends that Plaintiffs lack standing to bring a pen-register claim because “they have suffered no injury in fact involving personal information over which they have a cognizable privacy interest,” arguing that Plaintiffs have no reasonable expectation of privacy in their IP addresses and routing metadata. Mot. at 9-10. But COPPA bars the collection of persistent identifiers, including IP addresses, from children under 13 without parental consent, which is relevant in setting children's reasonable expectations of privacy as to how their data would be collected and used. 16 C.F.R. §§ 312.2, 312.5; *Jones v. Google LLC*, 73 F.4th 636, 640 (9th Cir. 2023); *In re TikTok, Inc., Minor Privacy Litig.*, 2025 WL 3628598, at *14 (C.D. Cal. Nov. 5, 2025).

CA's cases are distinguishable. Mot. at 10 n.9 (citing *Mitchener v. CuriosityStream, Inc.*, 2025 WL 2272413, at *5 (N.D. Cal. Aug. 6, 2025) (dismissing pen-register claim on other grounds, noting but not deciding that plaintiff TikTok user would not have reasonable expectation of privacy in metadata); *Rodriguez v. Culligan Int'l Co.*, 2025 WL 3064113, at *5 (S.D. Cal. Nov. 3, 2025) (dismissing claim because business-website user had no expectation of privacy in IP address and other data collected by business); *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1049 (N.D. Cal. 2022) (collection or disclosure of contact information stolen in data breach of online game deemed not highly offensive)). Those cases involve people voluntarily using apps or websites. Here, by contrast, Plaintiffs allege that they, as students engaged in compulsory schoolwork, have a

reasonable expectation of privacy in their IP addresses and other personal information. ¶¶ 14, 21, 52, 68, 81, 99, 259-63, 269, 274-75, 305, 423, 425-27, 431.

CA further contends that Plaintiffs have not alleged how the capture of their IP addresses and related metadata “constitute[s] a harm with a close historical or common-law analogue sufficient to confer . . . standing.” Mot. at 10. But Plaintiffs have adequately alleged that they suffered injury. ¶¶ 19-21, 423-36. CA’s argument also ignores the defining feature of this case: Plaintiffs did not voluntarily disclose this information in a consumer setting—they were compelled to do so as part of their education. ¶¶ 14, 21, 52, 68, 81, 99, 261, 269, 305, 423, 426-27, 430-31. None of CA’s authorities involve such critical allegations.

CA next contends that the pen-register statute does not apply to IP addresses, arguing that the statute “never mentions the phrase ‘IP address’ or the word ‘metadata,’” and that “all indications point to the California legislature intending the . . . statute to regulate telephonic communications only.” Mot. at 11. But courts have broadly interpreted CIPA as protecting privacy interests and applied it to new technologies. *See Deivaprakash v. Condé Nast Digital*, 798 F. Supp. 3d 1100, 1107 (N.D. Cal. 2025) (pen-register claim based on recording of unique user ID, IP address, and device metadata by website owner’s installation of trackers on his internet browser); *Shah v. Fandom, Inc.*, 754 F. Supp. 3d 924, 932 (N.D. Cal. 2024) (pen-register claim based on recording and sharing of their IP addresses by third-party software trackers on website); *Mirmalek v. L.A. Times Comms. LLC*, 2024 WL 5102709, *3-4 (N.D. Cal. Dec. 12, 2024) (pen-register claim based on collection of IP address by third-party trackers on website).

CA also contends that CIPA is in tension with the California Consumer Privacy Act (“CCPA”) because the CCPA allows the collection of personal information that is “reasonably necessary” to achieve the purpose of the collection. Cal. Civ. Code § 1798.100(c). But CA’s

authority, *Lopez v. Sony Electronics, Inc.*, involved a claim that fell “within the ambit of” two irreconcilable limitations provisions. 5 Cal.5th 627, 634 (2018). Plaintiffs here do not bring a CCPA claim. Further, the CCPA addresses the collection, use, disclosure, and sale of the personal information of general consumers, not kids doing schoolwork.

Finally, CA argues its products are not pen registers, contending that a pen register must be separate from the source of the communications and that Plaintiffs allege that CA’s products are both pen registers and the sources of the communications. Mot. at 13 (citing *In re Apple Data Priv. Litig.*, 2026 WL 146025, *3 (N.D. Cal. Jan. 20, 2026) (finding allegation insufficient because it pointed to same device as pen register and source of communication)). Unlike *Apple*, Plaintiffs do not allege that the pen register and source of the communications are the same. Rather, they allege CA’s products are pen registers, and Plaintiffs’ browsers, computers, and tablets are the sources of the communications. ¶¶ 401-03. The paragraph CA cites as purportedly alleging CA’s products are the sources of the communications pertains to CA’s generation and collection of data when students interact with i-Ready, not the recording of non-content signaling data. Mot. at 13 (citing ¶ 8).

E. Plaintiffs state a CDAFA claim.

CA contends that Plaintiffs lack standing under CDAFA because they do not sufficiently allege a damage or loss. Mot. at 13. CA argues that allegations that it unjustly profited from its exploitation of Plaintiffs’ personal information do not suffice. Mot. at 13. CA’s arguments fail.

CA’s contention that the unjust-profit allegations are conclusory is incorrect. *Id.* Plaintiffs extensively allege that CA unjustly profits from its collection, use, and disclosure of their personal information without effective consent, including allegations that CA uses the data to develop and market its products, and that it obtains the use of Google’s proprietary suites of marketing, advertising, and customer-analytics software in exchange for installing Google’s tracking tools on

its products. ¶¶ 5-6, 36, 136-49, 166-82, 193-97, 200-01, 305, 332.

CA's argument that the unjust-profit allegations do not support a CDAFA claim also fails. Courts recognize allegations of unjust profit as sufficient to allege damage or loss under CDAFA. *Rodriguez*, 772 F. Supp. 3d at 1109-10; *Smith v. Rack Room Shoes, Inc.*, 2025 WL 2210002, *3 (N.D. Cal. Aug. 4, 2025); *Brown v. Google LLC*, 685 F. Supp. 3d 909, 925-26 (N.D. Cal. 2023).

Plaintiffs also allege damage and loss due to privacy violations, which is sufficient under CDAFA. ¶¶ 302-07; *see also Cherkin*, 2025 WL 844378, at *6 (retaining similar CDAFA claim on basis of statutory language and purpose). Plaintiffs further allege economic loss because there is a market for their data and they were not compensated, and because CA's use of their data diminished its value. ¶¶ 35-36, 38-41, 47-48, 149, 191-92, 203-04, 330, 379, 434, 477, 494; *see also Rodriguez*, 772 F. Supp. 3d at 1110; *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 600 (9th Cir. 2020) (stake in unjustly earned profits exists no matter individual's intent to sell or diminution of data's value); *Brown*, 685 F. Supp. 3d at 940 (evidence of market for plaintiffs' data precludes ruling as a matter of law that plaintiffs suffered no damages under CDAFA); *Biden v. Ziegler*, 737 F. Supp. 3d 958, 976 (C.D. Cal. 2024) (CDAFA claim viable where plaintiff, as owner of data, alleges he suffered damages caused by defendant in amount to be proven at trial).

CA argues that Plaintiffs cannot show that CA accessed their data knowing it lacked permission because it purportedly relied on schools' consent. Mot. at 14-15. But CA's erroneous reliance on school consent in lieu of parental consent would not shield it from liability, as a mistake of law is generally not a defense. *McDermott v. Marcus, Errico, Emmer & Brooks, P.C.*, 911 F. Supp. 2d 1, 82 (D. Mass. 2012), *amended in part*, 969 F. Supp. 2d 74 (D. Mass. 2013), *aff'd in part, rev'd in part and remanded*, 775 F.3d 109 (1st Cir. 2014). Even if it was, what CA knew or believed about any purported school-consent exception—and whether schools provided effective

consent—is a fact question. *Calhoun v. Google, LLC*, 113 F.4th 1141, 1151 (9th Cir. 2024).

CA last argues that Plaintiffs cannot show CA “access[ed]” their data because they do not allege that CA “collected data from or accessed parts of [the] children’s computers *outside* of [CA’s] products.” Mot. at 15. But CA’s case, *Heiting v. Taro Pharmaceuticals USA, Inc.*, is inapposite. 709 F. Supp. 3d 1007 (C.D. Cal. 2023). The *Heiting* court found allegations of access inadequate where the defendant allegedly collected data without consent when the plaintiff engaged in a chat with the defendant on its website. *Id.* at 1020. Unlike an adult voluntarily visiting a website, Plaintiffs are children who allege that school personnel created their i-Ready accounts, and their data was taken by CA without effective consent. ¶¶ 14, 21, 52, 68, 81, 99, 261, 269, 305.

F. Plaintiffs’ Massachusetts Privacy Act Claim should be sustained.

CA seeks dismissal of Plaintiffs’ Massachusetts Right to Privacy Act, MASS. GEN. LAWS ch. 214 § 1B (“MPA”), claim, arguing that Plaintiffs fail to allege (1) the data at issue is highly personal or intimate, and (2) CA had no legitimate, countervailing interest to justify the disclosure. Mot. at 16-18. Plaintiffs have alleged both.

Under the MPA, a “plaintiff must show that there was a gathering and dissemination of information which she contends was private.” *Shedd v. Sturdy Mem’l Hosp., Inc.*, 2022 WL 1102524, at *11 (Mass. Super. Apr. 5, 2022) (cleaned up). The invasion must be unreasonable and substantial or serious, which are generally questions of fact. *Squeri v. Mount Ida College*, 954 F.3d 56, 69 (1st Cir. 2020). Whether there is a legitimate business interest for the intrusion is not an independent element but factors into the reasonableness of the intrusion. *Polay v. McMahon*, 468 Mass. 379, 383 (2014). Dismissal is unsupported where, as here, a substantial and unreasonable privacy invasion is plausibly alleged.

Highly personal, intimate data. Plaintiffs allege that CA collected and disclosed vast

troves of highly personal, intimate information about them and other minor students, including their special education status and learning difficulties or weaknesses. *See, e.g.*, ¶¶ 57, 61-63, 73-76, 84, 87, 90-91, 102, 108, 111-12, 118, 152-65, 424. CA attempts to sidestep these allegations by mischaracterizing the data as mere directory information, such as names, home addresses, and emails, Mot. at 16-17, but the Complaint makes clear that the data at issue goes beyond directory information and includes deeply sensitive educational and behavioral details.

Additionally, the sensitivity of Plaintiffs' data is underscored by federal statutes protecting the confidentiality of student records, including COPPA and FERPA, discussed *supra*. "Massachusetts also has similar laws recognizing and protecting children's privacy and a parent's right to raise them without intrusion by others." *Bignami v. Serrano*, 2020 WL 2257312, at *15 (Mass. Land Ct. May 7, 2020). Consistent with these protections, the Massachusetts Department of Elementary and Secondary Education ("DESE") enacted regulations to (1) ensure parents' and students' rights of confidentiality and destruction of student records, 603 CMR 23.01, and (2) prohibit third parties from accessing most student records without the informed, written consent of a parent or a student over 13 years old, 603 CMR 23.07(4). There are no analogous protections for directory information. In fact, the DESE regulations explicitly distinguish directory information, which may be shared without consent, 603 CMR 23.07(4)(a), from other student records, which may be shared without consent only in limited circumstances, such as to comply with a court order or law enforcement. 603 CMR 23.07(4)(b)-(h).⁵

Moreover, the Supreme Judicial Court of Massachusetts has determined that "information about [a] child's [learning] disability, progress, and needs. . . is highly personal, and disclosure

⁵ Even in these limited circumstances, DESE regulations require that personally identifiable information other than directory information "only be released to a third party on the condition that he/she will not permit any other third party to have access to such information without the written consent of the eligible student or parent." 603 CMR 23.07(4).

may result in embarrassment and potentially lead to stigma[.]” *Champa v. Weston Pub. Schs.*, 473 Mass. 86, 97 (2015). The *Champa* court considered whether settlement agreements between a public school and the parents of a student who required special education services are “public records” or exempt from disclosure. *Id.* at 87. The court noted that “agreements [identifying students placed in out-of-district private special education programs] may contain information that amounts to an unwarranted invasion of the student’s personal privacy.” *Id.* at 97. Similarly, information related to a minor’s individualized education plan is confidential. *See Doe v. Thorell*, 106 Mass. App. Ct. 532, 544 n.12 (2026) (citing *Champa*, 473 Mass. at 90-95).

Accordingly, Plaintiffs sufficiently allege that CA collected and disclosed highly personal, intimate information, including, *inter alia*, assessment scores, behavioral and interaction data, special education status, learning difficulties or weaknesses, predictions about their academic growth potential, online searches they perform, and online content they consume. ¶¶ 19, 57, 61-63, 73-76, 84, 87, 90-91, 102, 108, 111-12, 118, 152-65, 424.

No Legitimate, Countervailing Interest. Even if CA had a legitimate reason for disclosing some data to perform its essential functions, its disclosure exceeded that purpose. CA’s argument also fails because “under Massachusetts law, whether marketing and business analytics are legitimate purposes that outweigh intrusions on [] privacy interests is ‘a question of fact not suitable for resolution on a motion to dismiss.’” *Doe v. Baystate Health Sys., Inc.*, 2026 WL 776861, at *3 (D. Mass. Mar. 19, 2026) (citations omitted).

CA’s detailed, pervasive catalog of online activities and student identifiers⁶ disclosed to third parties, including data brokers and digital advertisers, ¶¶ 166-70, 172-73, 191-98, 207, 229-53, bears no relation to its purported interest. That CA harvested data from minors surreptitiously

⁶ These unique identifiers include their names, device identifiers, browser fingerprints, and other information collected by trackers such as cookies and pixels. ¶¶ 118, 195, 221-30, 253.

in the context of compulsory education, failed to disclose tracking technologies, produced and sold the equivalent of credit reports on children, and misrepresented how it used the data—all without parental consent in violation of federal and state law—further demonstrates the unreasonableness of its intrusion. ¶¶ 170-73, 202, 254-85, 321-22, 427-31.

The cases cited by CA regarding legitimate, countervailing interests are factually distinguishable. CA primarily relies upon *Squeri v. Mount Ida College*, 2019 WL 2249722 (D. Mass. May 24, 2019), *aff'd*, 954 F.3d 56 (1st Cir. 2020). In *Squeri*, a college had been acquired and shared student enrollment information with another educational institution for the purpose of future enrollment. *Id.* at 61-64. The First Circuit affirmed dismissal of the complaint, noting that the college was justified in disclosing records because the transfer of records was authorized by state law and required by state regulations. *Id.* at 69.⁷

This case bears no resemblance to *Squeri*. CA did not share Plaintiffs' sensitive data pursuant to state law or regulation or in connection with a business acquisition, and both CA and the third-party recipients of private data are for-profit corporations rather than non-profit educational institutions. Instead, CA shared highly sensitive information with for-profit third parties for purposes unrelated to education, to advance advertising and data monetization efforts. ¶¶ 136, 166, 170, 172, 174, 181, 184, 197, 207-08, 231-53, 331-32, 424, 426, 429. Unlike in *Squeri*, the disclosures here did not serve students' interests or further the educational mission; they exploited students' data for commercial gain.

G. Plaintiffs adequately allege that CA violated Chapter 93A.

Plaintiffs allege that CA's data practices constitute unfair and deceptive business practices

⁷ CA also cites *Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, an action against a securities seller to enjoin it from making sales calls to the plaintiff at his law office. 409 Mass. 514 (1991). *Schlesinger*, which ruled that "scattered telephone calls to the plaintiff's place of business over a period of years did not constitute an actionable invasion of the plaintiff's privacy," is factually distinguishable and was decided on summary judgment. *Id.* at 515.

in violation of MASS. GEN. LAW ch. 93A, § 2(a) (“Chapter 93A”). ¶¶ 479-98. CA seeks dismissal of the Chapter 93A claim, arguing: (1) Plaintiffs failed to plead a cognizable injury; and (2) it was not engaged in trade or commerce. Mot. at 18-19. Both arguments fail.

Cognizable Injuries. Chapter 93A provides a claim for any consumer injured by an unfair or deceptive act or practice. MASS. GEN. LAW ch. 93A, § 9(1). Cognizable injuries may be economic or non-economic, and Chapter 93A’s provision of nominal damages “eliminates the need to quantify an amount of actual damages if the plaintiff can establish a cognizable loss caused by a deceptive act.” *Hershenow v. Enterprise Rent-A-Car Co. of Bos.*, 445 Mass. 790, 799 n.18 (2006).

Courts in this Circuit recognize privacy-related harms as cognizable injuries under Chapter 93A. *See, e.g., Nightingale v. National Grid USA Serv. Co.*, 107 F.4th 1, 8-9 (1st Cir. 2024) (reversing summary judgment for defendant on Chapter 93A claim where debtor demonstrated privacy-related injuries based on excessive collection calls); *Powers v. Receivables Performance Mgmt., LLC*, 801 F. Supp. 3d 17, 29-31 (D. Mass. 2025) (denying summary judgment on Chapter 93A claim); *Zielenski v. Citizens Bank, N.A.*, 552 F. Supp. 3d 60, 72 (D. Mass. 2021) (injuries include “an invasion of the consumer’s personal privacy causing injury or harm worth more than one penny”). In a Chapter 93A action based on surreptitious data collection, this District recognized injury where geolocation data was collected and sold without consent. *Lionetta v. InMarket Media, LLC*, 798 F. Supp. 3d 139, 154 (D. Mass. 2025); *see also Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 372-73 (1st Cir. 2023) (privacy injury in data breach).⁸

CA relies on *Priddy v. ZOLL Medical Corp.*, 2025 WL 975234 (D. Mass. Mar. 31, 2025), for the proposition that a decrease in the inherent value of personal information is not a cognizable

⁸ CA also argues that a privacy harm is insufficient to sustain an injury-in-fact because it is not a separate identifiable harm *arising from* the unfair or deceptive act. Mot. at 18 n.16. This argument fails because the privacy harm stems in part from the disclosure and sale of personal data, which is separate from the unfair and deceptive data collection. *Lionetta*, 798 F. Supp. 3d at 154-55.

injury. Mot. at 19. But *Priddy* did not concern Chapter 93A, and in fact, supports Plaintiffs' case. The *Priddy* plaintiffs had standing based on actual misuse and future risk of misuse of their private information. 2025 WL 975234 at *4-7. Here, in addition to alleging privacy intrusions and the diminution in value of their data, Plaintiffs allege actual misuse and future risk of misuse of their private information and loss of money and/or property based on the unauthorized disclosure and taking of their personal information. ¶¶ 302-22, 494.⁹ Thus, Plaintiffs allege cognizable injuries.¹⁰

Trade or Commerce. CA next contends it was not “engaged in trade or commerce” because its contracts were with schools rather than with Plaintiffs. Mot. at 19-20. But privity is not a required element of a Chapter 93A claim. See *Mahoney v. Wells Fargo Bank, N.A.*, 2021 WL 1178377, at *11 (D. Mass. Mar. 29, 2021) (citing *Kattar v. Demoulas*, 739 N.E.2d 246, 258 (Mass. 2000)). While some commercial relationship is required, *Steinmetz v. Coyle & Caron, Inc.*, 862 F.3d 128, 141 (1st Cir. 2017), it is sufficient that the plaintiff used the defendant’s product, “even if it was sold to another,” *Rafferty v. Merck & Co., Inc.*, 479 Mass. 141, 161 (2018). A person whose rights have been affected by another’s Chapter 93A violation is entitled to bring an action so long as the relationship between the parties is not minor or insignificant. *Costa v. Zurich Am. Ins. Co.*, 2024 WL 5057723, at *4 (D. Mass. Dec. 10, 2024); *Small Just, LLC v. Xcentric Ventures LLC*, 2014 WL 1214828, at *9 (D. Mass. Mar. 24, 2014).

Plaintiffs were among the intended and foreseeable third-party beneficiaries of contracts between their schools and CA, and their rights were violated as a result of that commercial activity. ¶¶ 21, 45-46, 149, 268-69, 305, 426, 459-60. CA’s commercial success, in turn, depended on its

⁹ Notably, 93A damages may be calculated based on the unjustly earned profits. *Egan v. X-Mode Soc., Inc.*, No. 23-CV-11651-DJC, 2024 WL 2701967, at *3 (D. Mass. May 24, 2024).

¹⁰ CA also claims Plaintiffs did not allege any attempts to sell their data or that their ability to do so was hampered by CA, but Plaintiffs allege that they were deprived of the ability to choose how they would monetize their data. Compare Mot. at 19, with ¶¶ 321-22, 332.

ability to collect and monetize Plaintiffs' data. ¶¶ 21, 45-48, 61, 72, 89, 110, 149, 305-06. These allegations establish a direct and substantial relationship between Plaintiffs and CA that falls squarely within Chapter 93A's scope.

CA's reliance on *Morrissey v. New England Deaconess Association—Abundant Life Communities, Inc.*, 57 N.E.3d 1066 (Mass. App. Ct. 2016), is unavailing. There, the plaintiff's injuries arose from incidental property damage caused by a construction project, and the plaintiff had no meaningful connection to the defendant's commercial activity. *Id.* By contrast, Plaintiffs here were the central subjects of CA's data practices and the intended users of its products. Further, *Morrissey* does not support dismissal at this juncture because the *Morrissey* Chapter 93A claim was decided at summary judgment, not the pleading stage. *Id.*

H. Plaintiffs properly state an unjust enrichment claim in the alternative.

CA seeks dismissal of Plaintiffs' unjust enrichment claim, arguing Plaintiffs have an adequate remedy in law and failed to plead measurable benefit to CA and unjust detriment to Plaintiffs. Mot. at 20-23. CA is wrong on the law and misstates Plaintiffs' allegations.

Plaintiffs May Plead in the Alternative. CA overlooks the fact that Plaintiffs assert unjust enrichment in the alternative. ¶¶ 439, 455. Courts in this District have sustained both unjust enrichment claims and legal claims at the pleading stage. *See, e.g., Shedd*, 2022 WL 1102524, at *11 (“it would be inappropriate to dismiss the unjust enrichment claim simply because Plaintiffs have asserted as well claims of breach of implied contract, and or statutory and tort-based claims for relief.”); *Lionetta*, 798 F. Supp. 3d at 153-55 (unjust enrichment and Chapter 93A claims); *Lass v. Bank of Am., N.A.*, 695 F.3d 129, 140 (1st Cir. 2012) (“it is accepted practice to pursue both [contract and unjust enrichment] theories at the pleading stage”); *Vass v. Blue Diamond Growers*, 2015 WL 9901715, at *11 (D. Mass. Aug. 11, 2015), *report and recommendation adopted*, 2016

WL 1275030 (D. Mass. Mar. 31, 2016) (recognizing split of authority, following *Lass*, and sustaining Chapter 93A and unjust enrichment claims because a plaintiff may plead in the alternative); *see also Massachusetts Eye & Ear Infirmary v. QLT Phototherapeutics, Inc.*, 552 F.3d 47, 57 (1st Cir.) (trial on unjust enrichment and Chapter 93A claims), *decision clarified on denial of reh'g*, 559 F.3d 1 (1st Cir. 2009). Thus, Plaintiffs may pursue both theories in the alternative.

Realized Economic Value. “Massachusetts courts have recognized that misuse of confidential information may lead to unjust enrichment.” *Id.* Nevertheless, CA contends that the unjust enrichment claim should be dismissed, relying on *Karp v. Gap, Inc.*, 2014 WL 4924229 (D. Mass. Sep. 29, 2014), to argue that Plaintiffs’ allegations regarding how CA used their data for commercial purposes are too vague. Mot. at 21-22. But unlike *Karp*, in which the plaintiff failed to separately allege how the defendant realized any economic value, 2014 WL 4924229, at *2, Plaintiffs specifically allege numerous ways in which CA monetized their data, including: to derive behavioral analytics and “user insights;” to digitally profile students; to develop, enhance, market, sell, deliver, support and improve products, including CA’s artificial-intelligence technologies; and to sell back to schools and third parties. *See, e.g.*, ¶¶ 21, 35, 61, 63, 74, 76, 85-87, 90, 108, 111, 136-89, 317, 321, 429.¹¹ Thus, this case is more akin to *Lionetta*, in which the plaintiffs plausibly alleged that they conferred a measurable benefit upon the defendant through its collection and sale of their location data. 798 F. Supp. 3d at 152-53.

Inequitable Benefit. CA’s final challenge to Plaintiffs’ unjust enrichment claim is that the alleged way CA uses Plaintiffs’ data “does not defy the reasonable expectations of the parties and thus is not inequitable.” Mot. at 22. But Plaintiffs’ Complaint is clear that it was unreasonable for CA to surreptitiously harvest and disclose children’s private data during mandated school activities

¹¹ These allegations are bolstered by CA’s admissions about how it uses student data. ¶ 140.

without the informed consent of their parents in violation of federal and state law, specifically alleging they maintained a reasonable expectation of privacy in their devices, activity, and data, and that CA unreasonably and unjustly invaded their privacy by collecting, using, disclosing, and monetizing their sensitive data without compensating them for their property and labor. *See, e.g.*, ¶¶ 14, 21, 52, 68, 81, 99, 259-63, 269, 274-75, 305, 330-332, 423-27, 431, 441-53. These allegations are sufficient to support an unjust enrichment claim. *Lionetta*, 798 F. Supp. 3d at 152.

I. Plaintiffs' negligence claim should be sustained.

A negligence claim requires allegations that the defendant owed a duty of reasonable care, breached that duty, the plaintiff was damaged, and the breach proximately caused the damage. *Williams v. Steward Health Care Sys., LLC*, 480 Mass. 286, 290 (2018). CA challenges Plaintiffs' allegations of causation and damages, Mot. at 23-25, but Plaintiffs have alleged both.

Actual Damages. Plaintiffs allege damages arising from CA's commercial exploitation and privacy violations. ¶¶ 475, 477. Specifically, Plaintiffs allege that CA took and transmitted their private data to third parties without consent, causing both present and future harm. ¶¶ 37, 52, 64, 68, 77, 81, 92, 99, 114, 120, 141, 171-73, 182, 188-89, 256, 302-30, 461, 463.¹² CA contends Plaintiffs' damages are too speculative, Mot. at 23, but speculative damages may support a negligence claim, and a material risk of future harm is concrete harm, *Webb*, 72 F.4th at 376. Allegations of privacy invasions as damages are sufficient at the pleading stage. *See, e.g., Doe v. Tenet Healthcare Corp.*, 731 F. Supp. 3d 142, 149 (D. Mass. 2024) (alleged damages resulted from collection and transmission of personal information via pixels without consent).

Economic Loss Doctrine. CA invokes the economic loss doctrine, Mot. 24-25, which

¹² Allegations regarding time and effort spent mitigating risks from online data collection are sufficient to satisfy the damages element, *Webb*, 72 F.4th at 376, and Plaintiffs detail the efforts made to determine how their data was collected, identify what data was collected, and prevent future collection, ¶¶ 65, 78, 93-94, 114-15, 128, 131-32. Notably, CA cites precedent recognizing mitigation efforts as damages. Mot. at 24.

generally bars recovery of purely economic losses in tort absent personal injury or property damage. But there are exceptions, and a Massachusetts court declined to apply the doctrine in a comparable data breach case. *Shedd*, 2022 WL 1102524, at *7-8. The *Shedd* court held that a “special relationship” may exist where “patients are required to provide highly sensitive PII to a hospital to obtain medical care, are powerless to protect that information but rely on the hospital to do so consistent with state and federal law, and the hospital should reasonably have foreseen and guarded against the risk of disclosure.” *Id.* at *8. Here, the doctrine should not apply because Plaintiffs were required to provide sensitive data to CA at school, Plaintiffs are powerless to protect that data and rely on CA to do so consistent with state and federal law, and the harm from CA’s disclosure was foreseeable. *See* ¶¶ 459-76 (alleging special relationship).¹³

Causation. Plaintiffs allege CA’s collection and disclosure of their private data caused their damages. ¶¶ 150-82, 475, 477. CA does not dispute that its conduct was the actual or proximate cause of injury. Mot. at 25. Instead, it repeats the incorrect assertion that Plaintiffs did not suffer cognizable harm and claims the alleged injury is not separate from the negligent conduct. Mot. at 25. But Plaintiffs’ allegations plead causation: they allege injuries from the disclosure of their data, current misuse and risk of future misuse of that data, and mitigation efforts distinct from CA’s data collection practices. ¶¶ 302-22, 494. These allegations are sufficient.

IV. CONCLUSION

CA’s motion to dismiss should be denied in its entirety. In the alternative, should the Court grant any portion of CA’s motion, Plaintiffs respectfully request leave to amend their Complaint.

Amyndas Pharmaceuticals, S.A. v. Zealand Pharma A/S, 48 F.4th 18, 37 (1st Cir. 2022).

¹³ Moreover, injuries arising from privacy violations are often covered by personal injury insurance policies and explicitly set out therein. *See, e.g., Great Am. Ins. Co. v. Riso, Inc.*, 479 F.3d 158, 160 (1st Cir. 2007); *Transamerica Ins. Co. v. KMS Patriots, L.P.*, 52 Mass. App. Ct. 189, 190-91 (2001).

Dated: April 3, 2026

/s/ Karen Dahlberg O'Connell
Karen Dahlberg O'Connell
Mass. BBO No. 659969
ALMEIDA LAW GROUP LLC
157 Columbus Avenue, 4th Floor
New York, NY 10023
Phone: (347) 395-5666
Karen@almeidawgroup.com

Julie U. Liddell*
W. Andrew Lidell*
EdTech Law Center PLLC
904 Rio Grande, Suite 100
Austin, TX 78701
Phone: (512) 200-8028
julie.liddell@edtech.law
andrew.liddell@edtech.law

Andrew R. Tate*
PEIFFER WOLF CARR
KANE CONWAY & WISE LLP
235 Peachtree St. NE, Suite 400
Atlanta, GA 30303
Phone: (314) 669-3600
atate@peifferwolf.com

Lori G. Feldman*
Hecht Partners LLP
125 Park Avenue, 25th Floor
New York, NY 10017
Main Phone: (212) 851-6821
LFeldman@hechtpartners.com
e-servicecapg@hechtpartners.com

Attorneys for Plaintiffs

**Pro Hac Vice Applications Granted*

CERTIFICATE OF SERVICE

I, Karen Dahlberg O'Connell, hereby certify that on this 3rd day of April 2026, the foregoing document, filed through the ECF system, will be sent electronically to the registered participants on the Notice of Electronic Filing, and paper copies will be sent to any non-registered participants.

/s/ Karen Dahlberg O'Connell
Karen Dahlberg O'Connell