2022 IL App (1st) 220187
No. 1-22-0187
Opinion filed December 23 , 2022

SIXTH DIVISION

IN THE

APPELLATE COURT OF ILLINOIS

FIRST DISTRICT

DAVID BARNETT, ETHEL BURR, and MICHAEL HENDERSON,	)	Appeal from the Circuit Court of Cook County.
Plaintiffs-Appellants,	)	
v.	)	No. 21 CH 3119
APPLE INC.,	)	The Honorable Neil H. Cohen,
Defendant-Appellee.	)	Judge, presiding.

JUSTICE ODEN JOHNSON delivered the judgment of the court, with opinion. Justices Walker and Tailor concurred in the judgment and opinion.

OPINION

¶ 1 Plaintiffs, David Barnett, Ethel Burr, and Michael Henderson, appeal the dismissal of their putative class action suit. The trial court dismissed their complaint with prejudice, pursuant to section 2-615 of the Code of Civil Procedure (735 ILCS 5/2-615 (West 2020)), for failure to state a cause of action. The two-count complaint alleges that defendant Apple Inc. (Apple) violated the Biometric Information Privacy Act (Act) (740 ILCS 14/1 *et seq.* (West 2020)) by offering users of its phones and computers the option of utilizing face and fingerprint recognition features (1) without first instituting a written policy regarding the

retention and destruction of the users' biometric information and (2) without first obtaining the users' written consent. Plaintiffs claim that, under the Act, Apple was in "possession" of, and had "collected" and "captured," the users' biometric information where Apple designed and owns the software that plaintiffs opted to use and where Apple has the ability to, and does, remotely update the software.

¶ 2 On this appeal, plaintiffs do not dispute that the user's biometric information is stored on the user's own device; that Apple does not collect or store this information on a separate server or device; that these features are completely optional; that the user is the sole entity deciding whether or not to use these features; that, to enable the features, the user employs his or her own device to capture and collect his or her own biometric information on that device; and that the user has the power to delete this biometric information from the device at any time without negatively impacting the device.

¶ 3 For the following reasons, we do not find plaintiffs' claims persuasive and affirm the trial court's dismissal.

¶ 4 BACKGROUND

¶ 5 I. The Complaint's Allegations

¶ 6 Since, on a motion to dismiss, we accept as true all the well-pleaded allegations of the complaint, we provide below what the complaint does and does not allege. See *infra* ¶ 29.

¶ 7 A. The Parties

¶ 8 The three named plaintiffs are Barnett, Burr and Henderson. The complaint alleges that "[t]his Court has personal jurisdiction over [Apple] because the biometrics that give rise to this lawsuit were captured from Plaintiff Barnett while he was residing and physically present in Cook County." There is no such similar allegation made with respect to the remaining two

plaintiffs, Burr and Henderson. However, all three plaintiffs are, and have been "at all relevant times," residents and citizens of Illinois.

¶ 9 The defendant is Apple, a California corporation, with its principal place of business in California. Apple manufactures iPhones, iPads, and MacBooks with "Touch ID" and "Face ID" features, and it sells or distributes these products throughout Illinois.

¶ 10 B. "Touch ID" and "Face ID"

¶ 11 "Touch ID" is a "fingerprint recognition feature" that gives the user the option of allowing his or her device to "extract[ ]" his or her fingerprint. Similarly, "Face ID" is a "facial recognition feature" that gives the user the option of allowing his or her device to "extract[ ]" the user's "facial geometry." The user may then use Touch ID and Face ID to unlock the device and authorize purchases on Apple Pay, as well as purchases and downloads on the App Store. Both Apple Pay and the App Store are regulated and controlled by Apple. Users may also use Touch and Face ID "as direct log-in methods" for apps by other developers.

¶ 12 The Touch and Face ID features work by means of a mathematical representation. After the user has the device collect his or her fingerprint or facial image, the Touch or Face ID software on the device uses the image "to create a unique mathematical representation." "[T]his representation is stored on [the] user's device." If a user has "already enrolled" in the Touch or Face ID feature, then the device compares the representation "with the saved representation" already on the device.

¶ 13 After the user's initial activation of Touch or Face ID, Apple "use[s]" subsequent log-in attempts "to augment [its] fingerprint and facial recognition technology." While the complaint does not allege how Apple "use[s]" the log-in attempts, the complaint cites in a footnote a 2017 article on Apple's website that says that the Face ID software on the device

may gather more information about the user's face during subsequent log-in attempts in order " 'to augment 'future matching.' " "Apple also collects diagnostic data from users, like how many are using Touch ID and how often they unlock their device."

¶ 14 Apple is the sole owner of its software, while users are licensees. Users cannot "access their own biometrics" collected by and stored on their own devices without violating "Apple's Software License Agreement." Apple regularly updates the software on its users' devices.

¶ 15 The complaint provides the following quote from Apple's website describing Touch ID:

> "The [Touch ID] sensor uses advanced capacitive touch to take a high-resolution image from small sections from your fingerprint from the subepidermal layers of your skin. Touch ID then intelligently analyzes this information with a remarkable degree of detail and precision. It categorizes your fingerprint as one of three basic types—arch, loop, or whorl. It also maps out individual details in the ridges that are smaller than the human can see, and even inspects minor variations in ridge direction caused by pores and edge structures *** It then creates a mathematical representation of your fingerprint and compares this to your enrolled fingerprint data to identify a match and unlock your device."[1]

¶ 16 The complaint provides the following quote from Apple's website describing Face ID:

> "The [Face ID] TrueDepth camera captures accurate face data by projecting and analyzing over 30,000 invisible dots to create a depth map of your face and also captures an infrared image of your face. A portion of the neural engine of the *** Bionic chip—protected with the Secure Enclave—transforms the depth map and

[1]The brackets and ellipses are in the complaint.

> infrared image into a mathematical representation and compares that representation to the enrolled facial data."

The Secure Enclave is on the user's device. The complaint details all the steps, with photos, that a user must take in order to capture and collect his or her biometric information and store it in the Secure Enclave within the device.

¶ 17 C. Counts and Relief

¶ 18 As noted above, the two-count complaint alleges that Apple violated the Act (740 ILCS 14/1 *et seq.* (West 2020)) by offering users of its phones and computers the option of using face and fingerprint recognition features (1) without first instituting a written policy regarding the retention and destruction of the users' biometric information and (2) without first obtaining the users' written consent.

¶ 19 In relief, plaintiffs seek class certification, attorney fees and costs, and "statutory damages of $5,000.00 for each and every intentional and/or reckless violation of [the Act] pursuant to 740 ILCS 14/20(2), or alternatively statutory damages of $1,000.00 for each and every violation pursuant to 740 ILCS 14/20-1 if the Court finds that Defendant's violations were negligent."

¶ 20 II. Motion to Dismiss

¶ 21 Plaintiffs filed their complaint on June 25, 2021, and served Apple on July 12, 2021. After an agreed-upon extension of time, Apple moved on October 8, 2021, to dismiss the complaint pursuant to section 2-615 (735 ILCS 5/2-615 (West 2020)) for failure to state a cause of action. In its motion, Apple argued that plaintiffs elected to use the Touch and Face ID features and that plaintiffs' biometric information is stored on their own devices. On November 12, 2021, plaintiffs filed a response that relied heavily on the cases of *Hazlitt v. Apple Inc.*, 500

F. Supp. 3d 738 (S.D. Ill. 2020), and *Zaluda v. Apple Inc.*, No. 2019-CH-11771 (Cir. Ct. Cook County, Oct. 29, 2020). [2]

¶ 22 As exhibits to their response, plaintiffs attached (1) the *Zaluda* complaint, (2) Apple's section 2-619.1 motion to dismiss in the *Zaluda* case, and (3) the October 29, 2020, order by the *Zaluda* circuit court denying Apple's motion to dismiss "[f]or the reasons stated on the record." As an exhibit to its reply, Apple attached, what appears to be, an excerpt from a transcript in the *Zaluda* case. The excerpt is preceded by a cover page entitled "Remote Zoom Motions Ruling[,] Thursday, October 22, 2020." The excerpt appears to be pages 9 and 10 from a 20-page transcript, and the excerpt both starts and ends in the middle of sentences. The excerpt states in full:

> "different motion, but that motion is not before us.
>
> Apple maintains that the user profile is not a voiceprint. The plaintiffs assert otherwise, specifically in the complaint citing to Paragraphs 49 through and inclusive of 51 in a factual way, at least what I'm viewing as a factual assertion, which is consistent with what the Code requires, they—plaintiffs have properly pled the existence of a voiceprint or that the user profile is a voiceprint. I think that's a better way to put it.
>
> So, the next issue is whether or not there has been, in a factual way, properly asserted allegations that there has been a collection of the voiceprint—assuming that it is a voiceprint, a collection of the voiceprint by Apple.

[2] *Hazlitt* and *Zaluda* are other ongoing cases alleging Act violations against Apple.

Apple maintains that it did not collect that, that it stays on the user's own piece of equipment, on the phone, and that it was never collected by Apple. It stays on the device itself. That is Apple's position.

In the plaintiffs' complaint, at Paragraphs 9, 43 and 44, 58 through and inclusive of 68, there have been proper factual allegations to the contrary. I don't know if that's accurate or not, but certainly that is the properly pled allegations contained within the plaintiffs' complaint.

Consequently, I am rejecting Apple's argument to the contrary.

There is an additional subset of that argument that in addition to there not being a collection of the voiceprint, that there was a disclosure of this to a third party.

In Paragraphs 47, 48, 55, as well as Note 10, there is an assertion by the plaintiffs that there was in fact a sharing of the voiceprint, of the user profile if you will, to—with third parties.

Whether it happened or not is not for me to determine at this stage of the"

¶ 23 On January 3, 2022, the trial court in the instant case issued a six-page memorandum order granting Apple's motion to dismiss, and on January 4, 2022, the trial court issued an almost identical "corrected" memorandum order, also granting Apple's motion to dismiss. The trial court's order distinguished *Zaluda*, as follows:

"In *Zaluda*, the plaintiffs alleged that their Apple devices generated voiceprints so that Siri could recognize the voiceprints and that these voiceprints were then sent to Apple's servers and third parties in violation of [the Act]. The Complaint in this case does not allege that Plaintiffs' biometric information was sent to Apple's servers or any

third party server, but expressly alleges that the information is stored locally on Plaintiffs' own devices."

¶ 24 The trial court's order also distinguished *Hazlitt*, a case involving Apple's Photos app, which employs facial recognition technology to scan a user's photographs and add frequently detected faces to a user's "People" album. *Hazlitt v. Apple Inc.*, 543 F. Supp. 3d 643 (S.D. Ill. 2021).[3] The trial court found *Hazlitt* distinguishable because the plaintiffs in *Hazlitt* had alleged that Apple stored the " 'faceprints' " in Apple's own databases and that users had no power to delete the collected information or disable the feature on their devices. *Barnett v. Apple, Inc.*, No. 21-CH -119, slip op. at 4 (Cir. Ct. Cook County, Jan. 4, 2022) (quoting *Hazlitt*, 543 F. Supp. 3d at 653).

¶ 25 Rejecting plaintiffs' arguments, the trial court found:

"The Complaint here does not allege that Apple has stored any of Plaintiffs' biometric data in Apple databases. Rather, the Complaint clearly alleges that Plaintiffs' biometric data was voluntarily scanned and stored by Plaintiffs on their own devices. Nor do Plaintiffs allege that they have no control over the data collected and stored on their own devices or that they cannot delete that data. The Complaint is clear that Plaintiffs voluntarily chose to use Face ID and Touch ID and can delete their biometric information from their devices if they choose. Finally, the Complaint does not allege any facts showing that they cannot use their Apple devices unless they use Face ID or Touch ID ***."

[3]Before discussing the *Hazlitt* case, the trial court observed that the district court order cited by plaintiffs (500 F. Supp. 3d 738) had been vacated on appeal, and that a new district court order (543 F. Supp. 3d 643) was issued.

¶ 26 The January 4, 2022, order stated that Apple's motion to dismiss was granted with prejudice and that the order was final and appealable. On February 2, 2022, plaintiffs filed a timely notice of appeal, and this appeal followed.

¶ 27 ANALYSIS

¶ 28 I. Standard of Review

¶ 29 In the case at bar, the trial court dismissed the complaint pursuant to section 2-615 of the Code (735 ILCS 5/2-615 (West 2020)) for failure to state a cause of action. The rules governing our review of such a dismissal are well established. When ruling on a section 2-615 motion, a court must accept as true all well-pleaded facts in the complaint, as well as any reasonable inferences that may be drawn from those facts. *Tyrka v. Glenview Ridge Condominium Ass'n*, 2014 IL App (1st) 132762, ¶ 33 (citing *DeHart v. DeHart*, 2013 IL 114137, ¶ 18).

¶ 30 Our supreme court has also stated "time and again" that Illinois is a fact-pleading jurisdiction. *Weiss v. Waterhouse Securities, Inc.*, 208 Ill. 2d 439, 451 (2004); *City of Chicago v. Beretta U.S.A. Corp.*, 213 Ill. 2d 351, 367 (2004). In a notice-pleading jurisdiction, such as the federal courts, "a plaintiff is not required to plead operative facts with particularity." *City of Chicago*, 213 Ill. 2d at 367; see *Johnson v. Matrix Financial Services Corp.*, 354 Ill. App. 3d 684, 696 (2004) (federal courts operate under a notice-pleading standard, while Illinois state courts operate under a fact-pleading standard). "[I]f there is any set of facts consistent with the plaintiff's complaint that would allow recovery, the court in a notice-pleading jurisdiction may not grant a defendant's motion to dismiss." *City of Chicago*, 213 Ill. 2d at 368. By contrast, Illinois plaintiffs are required to "allege facts sufficient to bring a claim within a legally recognized cause of action." *City of Chicago*, 213 Ill. 2d at 368. As a result of this difference,

we find less persuasive some of the federal cases cited by plaintiffs, such as *Hazlitt*, 543 F. Supp. 3d 643, and *Ronquillo v. Doctor's Associates, LLC*, No. 21-C-4903, 2022 WL 1016600 (N.D. Ill. Apr. 4, 2022), which denied dismissal motions under the more liberal federal standard.

¶ 31 Although Illinois plaintiffs are not required to set forth evidence in their complaint, they also cannot simply set forth conclusions. *Tyrka*, 2014 IL App (1st) 132762, ¶ 34 (citing *Marshall v. Burger King Corp.*, 222 Ill. 2d 422, 430 (2006)). Mere conclusory allegations unsupported by specific facts do not suffice. *Tyrka*, 2014 IL App (1st) 132762, ¶ 34 (citing *Primax Recoveries, Inc. v. Atherton*, 365 Ill. App. 3d 1007, 1010 (2006)). In short, with a motion to dismiss, an Illinois court must decide whether the complaint alleges sufficient well-pleaded facts that, if proved, would entitle the plaintiff to relief. *Bogenberger v. Pi Kappa Alpha Corp., Inc.*, 2018 IL 120951, ¶ 23.

¶ 32 On appeal, our review of a trial court's section 2-615 dismissal is *de novo*. *Tyrka*, 2014 IL App (1st) 132762, ¶ 35 (citing *DeHart*, 2013 IL 114137, ¶ 18). *De novo* review means that we perform the same analysis that a trial judge would perform. *Guvenoz v. Target Corp.*, 2015 IL App (1st) 133940, ¶ 41.

¶ 33 II. Statutory Sections at Issue

¶ 34 Plaintiffs allege violations of both section 15(a) and section 15(b) of the Act. 740 ILCS 14/15 (West 2020). Section 15(a) provides, in full:

> "(a) 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 or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in *possession* of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines." (Emphases added.) 740 ILCS 14/15(a) (West 2020).

The above section, by its express terms, applies only to a "private entity in *possession* of biometric identifiers or biometric information." (Emphasis added.) 740 ILCS 14/15(a) (West 2020). Apple argues that it is not "in possession," while plaintiffs argue that it is. The statute does not define the term "possession." 740 ILCS 14/15(a) (West 2020).

¶ 35 Section 15(b) provides, in full:

> "(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
>
> (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative." 740 ILCS 14/15(b) (West 2020).

Plaintiffs argue that Apple captures and collects their biometric information, while Apple argues that it does not.

¶ 36 Section 20 provides a right of action, and states in full:

> "Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation:
>
> (1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;
>
> (2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;
>
> (3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and
>
> (4) other relief, including an injunction, as the State or federal court may deem appropriate." 740 ILCS 14/20 (West 2020).

Plaintiffs allege that section 20 applies because they were "aggrieved by a violation" of the Act, while Apple argues that there is no violation. 740 ILCS 14/20 (West 2020).

¶ 37 III. Statutory Interpretation

¶ 38 With statutory interpretation, our primary goal is to ascertain and give effect to the intent of the statute's drafters. *VC&M, Ltd. v. Andrews*, 2013 IL 114445, ¶ 30. The most reliable indicator of the drafters' intent is the language they chose to use in the statute itself. *VC&M, Ltd.*, 2013 IL 114445, ¶ 30. When reading the language of the statute, we give the words their plain and ordinary meaning, *VC&M, Ltd.*, 2013 IL 114445, ¶ 30.

¶ 39 " 'When a statute does not define its own terms, a reviewing court may use a dictionary to ascertain the plain and ordinary meaning of those terms.' " *Watson v. Legacy Healthcare Financial, LLC*, 2021 IL App (1st) 210279, ¶ 36 (quoting *Maschek v. City of Chicago*, 2015 IL App (1st) 150520, ¶ 56 (citing *People v. McChristian*, 2014 IL 115310, ¶ 15, and *People v. Bingham*, 2014 IL 115964))); see *People v. Chapman*, 2012 IL 111896, ¶ 24 ("When a statute contains a term that is not specifically defined, it is entirely appropriate to look to the dictionary to ascertain the plain and ordinary meaning of the term.").This court has previously relied on Merriam-Webster Online Dictionary when interpreting words in this Act, including specifically the words "capture" and "collect," which are at issue in this appeal. *Mosby v. Ingalls Memorial Hospital*, 2022 IL App (1st) 200822, ¶ 43; *Watson*, 2021 IL App (1st) 210279, ¶¶ 58-59.

¶ 40 IV. Possession

¶ 41 As noted, the word "possession" is not defined in the statute. *People v. Ward*, 215 Ill. 2d 317, 325 (2005) ("undefined terms in a statute shall be given their ordinary and popularly understood meanings"). The first definition of the word in the dictionary is "the act of having or taking into control." Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/possession (last visited Dec. 19, 2022) [https://perma.cc/UUL9-8JXA]. Plaintiffs cite the *Ward* case, in which our supreme court similarly found: " 'Possession' means 'the act or condition of having in or taking into one's control or holding at one's disposal.' " *Ward*, 215 Ill. 2d at 325 (quoting Webster's Third New International Dictionary 1770 (1986)).

¶ 42 Plaintiffs then set forth a variety of legal concepts relating to possession, arguing that it may be actual or constructive, sole or joint, or direct or indirect. In *Ward*, which plaintiffs

cite, our supreme court acknowledged "that legal conceptions of 'possession' are many and varied." *Ward*, 215 Ill. 2d at 325. However, the court stated that it could find "no indication" that "the legislature intended to depart from the ordinary and popular meaning of 'possession' when it included this term" in the statute. *Ward*, 215 Ill. 2d at 325-26. We reach the same conclusion here.[4] Thus, we apply the ordinary and popular meaning of the word "possession," as found by our supreme court and found in a dictionary, which is to have control.

¶ 43 Plaintiffs argue that Apple "possesses" their information because Apple software collects and analyzes their information. This argument equates the product with the company. In essence, plaintiffs are arguing that, since they chose to employ Apple's optional software to collect, analyze, and store their own information on their own devices, they handed control over their information to Apple.

¶ 44 Based on the facts alleged by plaintiffs, it seems as though Apple designed these features almost with the express purpose of handing control to the user. The features are completely elective. In fact, the user must undertake a series of steps in order to use them. As plaintiffs' complaint demonstrates with step-by-step photos, the user utilizes her[5] own device in order to capture her own fingerprint or facial image. The device and the software are the tools, but it is the user herself who utilizes these tools to capture her own biometric information. After the user uses her own device to capture and collect her own information, the information is then stored solely on her device. She may then use these features to unlock her phone or use Apple Pay or other apps. At any time, if she decides that she no longer wants to use these features, she may delete them. There is no allegation that Apple stores this information on a

[4]In addition, plaintiffs do not make any arguments that the Act's legislators intended to depart from the ordinary and popular meaning of the words they used.

[5]For simplicity's sake, we are using "her" in a universalist, generic way here simply to denote one human.

separate server or that Apple has ever once prevented a user from deleting her own information. While Apple has the ability to remotely update the device, there is no allegation about what, if any impact, updates have had on the features at issue. A complaint must plead facts not possibilities. Although we are at an early stage of the litigation, plaintiffs did not seek to amend their complaint after these points were made in the court below. Given the facts alleged by plaintiffs, we cannot find that Apple possesses plaintiffs' biometric information.

¶ 45 Like the trial court, we do not find *Zaluda* or *Hazlitt* persuasive. They are both trial court decisions in cases that are still pending and have not been reviewed by the appellate courts; thus, the ultimate resolution is yet unknown. Additionally, their facts are readily distinguishable from the facts at bar. First, as the trial court found,

> "[i]n *Zaluda*, the plaintiffs alleged that their Apple devices generated voiceprints so that Siri could recognize the voiceprints and that these voiceprints were then sent to Apple's servers and third parties in violation of [the Act]. The Complaint in this case does not allege that Plaintiffs' biometric information was sent to Apple's servers or any third party server, but expressly alleges that the information is stored locally on Plaintiffs' own devices."

Second, as the trial court found, *Hazlitt* is distinguishable because the plaintiffs in *Hazlitt* alleged that Apple stored the facial information in Apple's own databases and that users had no power to delete the collected information or disable the feature on their devices. See *Hazlitt*, 543 F. Supp. 3d at 653. In contrast, here, it is alleged that the information is stored, not on Apple's databases, but on the users' individual devices and that users may delete the information and disable the features. For these reasons, we agree with the trial court's decision finding these cases readily distinguishable and not persuasive.

¶ 46 V. Collect and Capture

¶ 47 Plaintiffs argue that Apple collects and captures their biometric information, where plaintiffs utilized Apple software to collect and capture their fingerprints or facial images. Like the word "possession," the words "collect" and "capture" are not defined in the statute itself, so we turn to the dictionary and to our recent caselaw for guidance.

¶ 48 This court recently discussed the meaning of the word "capture" in the Act and found:

> "The first couple of definitions of 'capture' in the dictionary, such as 'to take captive' or 'to emphasize,' do not apply here. Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/capture (last visited May 9, 2022). However, the secondary meaning of 'to record in a permanent file (as in a computer)' clearly applies here. See *id*. After this definition, the dictionary provides the following example of its use in a sentence: 'The system is used to *capture* data ***.' (Emphasis in original.) *Id*. Similarly, *** the information is captured, or recorded in a permanent file, from an individual ***." (Emphasis in original.) *Mosby*, 2022 IL App (1st) 200822, ¶ 58.

¶ 49 This court also discussed the meaning of the word "collect" as used in the Act and found:

> "The first definitions of 'collect' in the dictionary are 'to bring together into one body and place,' 'to gather or exact from a number of persons or sources,' and 'to gather an accumulation of.' Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/capture (last visited May 9, 2022). Thus, after the capture of information from an individual ***, that information may be gathered or accumulated from a number of persons into one place." *Mosby*, 2022 IL App (1st) 200822, ¶ 59.

¶ 50 Neither of these definitions from *Mosby* help plaintiffs. First, to the extent that the information was captured or recorded in a permanent file, that permanent file was on the user's own device, not on the defendant's device as was the case in *Mosby*. *Mosby,* 2022 IL App (1st) 200822, ¶ 58. Second, the information was not "gathered or accumulated from a number of persons into one place," as it was in *Mosby*. *Mosby*, 2022 IL App (1st) 200822, ¶ 59. Instead, the information here remained in a multitude of different and distinct places, namely, the millions of devices of Apple's numerous users.

¶ 51 In support, plaintiffs cite *Ronquillo,* 2022 WL 1016600. First, like *Zaluda* and *Hazlitt*, *Ronquillo* appears to be an ongoing case where the ultimate resolution is yet unknown. Second, as an unpublished federal district court case, it has no binding or precedential authority "in Illinois courts." *King's Health Spa, Inc. v. Village of Downers Grove*, 2014 IL App (2d) 130825, ¶ 63. Third, like *Zaluda* and *Hazlitt*, *Ronquillo* is readily distinguishable on its facts. In *Ronquillo*, the plaintiff was an employee in a Subway store, who was required to clock in and out using his biometric information. The biometric scanner was owned by defendant HP Inc. (HP). Defendant Doctor's Associates, LLC (DAL) was the American franchisor for Subway, and it required its franchisees to use defendant HP's machines. DAL had installed software on these machines to collect employee biometric information and to store "reference templates" with the employees' information in "a database." *Ronquillo*, 2022 WL 1016600, at *1.

¶ 52 *Ronquillo* is factually distinguishable for several reasons, including that the *Ronquillo* plaintiff was required to use the biometric scanner or lose her job, that the biometric information in *Ronquillo* was stored exclusively on a device that was not in his possession, and that the *Ronquillo* plaintiff had no ability to delete the information after a template was created.

By contrast, in the case at bar, the feature is wholly optional, the information is stored exclusively on plaintiffs' devices, and they may delete the information at will. For these reasons, *Ronquillo* is readily distinguishable on its facts and, hence, not persuasive.

¶ 53 In their brief to this court, plaintiffs assume that the *Ronquillo* employee's template was stored on only the franchisee store's device. However, the district court never made such a specific finding. Instead, it referred generically to defendants' "POS hardware" or "POS system." *Ronquillo*, 2022 WL 1016600, at *1. Defendants HP and DAL had argued that only the individual franchisee store could be sued because only the franchisee stored the employee's information. However, the district court specifically rejected this argument, finding that it "rewrite[s]" the allegations of the complaint and that the "actual allegations" permitted "reasonable inferences" of control by defendants HP and DAL. *Ronquillo*, 2022 WL 1016600, at *4. The *Ronquillo* complaint alleged that one defendant captured the fingerprints and created the reference templates, while the other defendant stored the templates "on its hardware." *Ronquillo*, 2022 WL 1016600, at *3.[6] The court left "for another day" the question of what role DAL and HP "actually" played in storing the information. *Ronquillo*, 2022 WL 1016600, at *3. By contrast, in the case at bar, plaintiffs have specifically alleged that the information is stored only on their devices.

¶ 54 The *Ronquillo* court could leave this question for another day because, unlike Illinois state courts that employ a fact-pleading standard, federal courts employ a notice-pleading standard. *Johnson*, 354 Ill. App. 3d at 696 (federal courts operate under a notice-pleading standard, while Illinois state courts operate under a fact-pleading standard). This is yet another

[6]The court noted that defendants "DAL and HP did not explain the Biometric System, how they use the data collected through the Biometric System, or how long they keep the collected data." *Ronquillo*, 2022 WL 1016600, at *1.

difference between the two cases that makes *Ronquillo* inapposite to our case.[7] A complaint, such as the one in *Ronquillo*, "that would survive a motion to dismiss in a notice-pleading jurisdiction might not do so in a fact-pleading [one]." *City of Chicago*, 213 Ill. 2d at 368; *Johnson*, 354 Ill. App. 3d at 696 (noting that the burden is heavier on a plaintiff under a fact-pleading standard).

¶ 55 Lastly, even if we found *Ronquillo* persuasive, it would not help plaintiffs. In *Ronquillo*, the court found that the capture and collection mentioned in section 15(b) required a step beyond "mere possession." *Ronquillo, LLC*, 2022 WL 1016600, at *2. Since we already found in the prior section that Apple did not possess plaintiffs' biometric data, *Ronquillo* does not support plaintiffs' argument that Apple captured and collected it.

¶ 56 CONCLUSION

¶ 57 For the foregoing reasons, we cannot find, based on the facts alleged by plaintiffs in this case, and assuming those facts to be true, that Apple possessed, captured, or collected plaintiffs' biometric information.

¶ 58 As we noted above, on this appeal, plaintiffs do not dispute that the user's biometric information is stored on the user's own device; that Apple does not collect or store this information on a separate server or device; that these features are completely optional; that the user is the sole entity deciding whether or not to use these features; that, to enable the features, the user employs his or her own device to capture and collect his or her own biometric information on that device; that, to utilize these features, the user must undertake a number of steps, which are all documented in photos in plaintiffs' complaint; and that the user has the

[7]The *Ronquillo* court specifically stated that it was applying a notice-pleading standard. It stated that all the plaintiff before it had to do was to "assert a facially plausible claim and provide fair notice to the defendant." *Ronquillo*, 2022 WL 1016600, at *2.

power to delete this biometric information from the device, at any time, without negatively impacting the device. Based on these facts, we affirm the thoughtful memorandum order of dismissal by the trial court.

¶ 59 Affirmed.

***Barnett v. Apple Inc.*, 2022 IL App (1st) 220187**

Decision Under Review:	Appeal from the Circuit Court of Cook County, No. 21-CH-3119; the Hon. Neil H. Cohen, Judge, presiding.
Attorneys for Appellant:	William H. Beaumont, of Beaumont Costales LLC, of Chicago, and Philip L. Fraietta, of Bursor & Fisher, P.A., of New York, New York, for appellants.
Attorneys for Appellee:	Raj N. Shah, Eric M. Roberts, and Yan Grinblat, of DLA Piper LLP (US), and Joshua G. Vincent and Kimberly A. Jansen, of Hinshaw & Culbertson LLP, both of Chicago, and Isabelle Ord (*pro hac vice*), of DLA Piper LLP (US), of San Francisco, California, for appellee.