

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

NIMESH PATEL, et al.,
Plaintiffs,
v.
FACEBOOK INC.,
Defendant.

Case No. [3:15-cv-03747-JD](#)

**ORDER RE RENEWED MOTION TO
DISMISS FOR LACK OF SUBJECT
MATTER JURISDICTION**

Re: Dkt. No. 227

In this putative class action case under the Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1 *et seq.* (“BIPA”), named plaintiffs allege that defendant Facebook, Inc. (“Facebook”) unlawfully collected and stored their biometric data without prior notice or consent. Dkt. No. 40. Facebook asks to dismiss the case under Federal Rule of Civil Procedure 12(b)(1) and *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016) (*Spokeo I*) on the ground that plaintiffs have failed to allege a concrete injury in fact. Dkt. No. 227. The motion is denied.

BACKGROUND

This consolidated action originated as three separate cases originally filed in Illinois courts. Two of the cases were filed in federal court, while a third was filed in Illinois state court and removed to federal court by Facebook under the Class Action Fairness Act. Notice of Removal, *Licata v. Facebook, Inc.*, No. 1:15-cv-04022 (N.D. Ill. filed May 6, 2015) (No. 1). The parties stipulated to transfer the cases to this Court, where they were consolidated into a single action. *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155, 1159 (2016). The consolidated class action complaint, Dkt. No. 40, is the operative complaint.

The consolidated complaint alleges that Facebook “operates the largest social network in the world, with over one billion active users.” Dkt. No. 40 ¶ 1. The named plaintiffs, Nimesh

1 Patel, Adam Pezen and Carlo Licata, use Facebook “to, among other things, upload and share
2 photographs with friends and relatives.” *Id.* ¶¶ 2, 7-9.

3 Plaintiffs’ claims arise out of Facebook’s “Tag Suggestions” program launched in 2010.
4 *Id.* ¶ 3. A user “tags” other Facebook users and non-users by identifying them in photographs
5 uploaded to Facebook. *Id.* ¶ 2. “Tag Suggestions” is intended to encourage more tagging. *Id.* ¶ 3.
6 It scans uploaded photographs “and then identif[ies] faces appearing in those photographs.” *Id.* If
7 the program “recognizes and identifies one of the faces appearing in [a] photograph, Facebook
8 will suggest that individual’s name or automatically tag them.” *Id.* In effect, the program
9 associates names with faces in photos and prompts users to tag those people.

10 Tag Suggestions uses “state-of-the-art facial recognition technology” to extract biometric
11 identifiers from photographs that users upload. *Id.* ¶¶ 4, 22. Facebook creates and stores digital
12 representations (known as “templates”) of people’s faces based on the geometric relationship of
13 facial features unique to each individual, “like the distance between [a person’s] eyes, nose and
14 ears.” *Id.* ¶ 23.

15 Plaintiffs allege that Facebook collected users’ biometric data secretly and without consent.
16 Specifically, they allege that the Tag Suggestions program violated BIPA because Facebook did
17 not: “[1] properly inform plaintiffs or the class in writing that their biometric identifiers (face
18 geometry) were being generated, collected or stored; [2] properly inform plaintiffs or the class in
19 writing of the specific purpose and length of time for which their biometric identifiers were being
20 collected, stored, and used; [3] provide a publicly available retention schedule and guidelines for
21 permanently destroying the biometric identifiers of plaintiffs and the class (who do not opt-out of
22 ‘Tag Suggestions’); and [4] receive a written release from plaintiffs or the class to collect, capture,
23 or otherwise obtain their biometric identifiers.” *Id.* ¶ 5. Plaintiffs seek declaratory and injunctive
24 relief and statutory damages. *Id.* ¶ 6.

DISCUSSION**I. Legal Standards**

“A Rule 12(b)(1) jurisdictional attack may be facial or factual. In a facial attack, the challenger asserts that the allegations contained in a complaint are insufficient on their face to invoke federal jurisdiction. By contrast, in a factual attack, the challenger disputes the truth of the allegations that, by themselves, would otherwise invoke federal jurisdiction.” *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004) (citations omitted).

In a facial jurisdictional challenge, the Court takes all factual allegations in the complaint as true and draws all reasonable inferences in plaintiffs’ favor. *Pride v. Correa*, 719 F.3d 1130, 1133 (9th Cir. 2013). In a factual challenge, the Court “may review evidence beyond the complaint without converting the motion to dismiss into a motion for summary judgment” and “need not presume the truthfulness of the plaintiff’s allegations.” *Safe Air*, 373 F.3d at 1039 (citations omitted). This discretion should be used with caution so that it does not usurp a merits determination. A “jurisdictional finding of genuinely disputed facts is inappropriate when the jurisdictional issue and substantive issues are so intertwined that the question of jurisdiction is dependent on the resolution of factual issues going to the merits of an action.” *Id.* (internal quotations and citations omitted).

II. Article III Standing

Federal courts are courts of limited jurisdiction, and the “case or controversy” requirement of Article III of the U.S. Constitution “limits federal courts’ subject matter jurisdiction by requiring, inter alia, that plaintiffs have standing.” *Chandler v. State Farm Mut. Auto. Ins. Co.*, 598 F.3d 1115, 1121 (9th Cir. 2010). As the Supreme Court recently reiterated, a plaintiff must demonstrate standing to sue by alleging the “irreducible constitutional minimum” of (1) an “injury in fact” (2) that is “fairly traceable to the challenged conduct of the defendants” and (3) “likely to be redressed by a favorable judicial decision.” *Spokeo I*, 136 S. Ct. at 1547. These requirements may not be abrogated by Congress. *Id.* at 1548. The specific element of injury in fact is satisfied when the plaintiff has “suffered ‘an invasion of a legally protected interest’ that is ‘concrete and

1 particularized’ and ‘actual or imminent, not conjectural or hypothetical.’” *Id.* (quoting *Lujan v.*
2 *Defenders of Wildlife*, 504 U.S. 555, 560 (1992)).

3 *Spokeo I* did not announce new standing requirements, as the citation to *Lujan* indicates.
4 Rather, it sharpened the focus on when an intangible harm such as the violation of a statutory right
5 is sufficiently concrete to rise to the level of an injury in fact. To determine whether an injury in
6 fact has been demonstrated in this “somewhat murky area,” *Robins v. Spokeo, Inc.*, 867 F.3d 1108,
7 1112 (9th Cir. 2017) (*Spokeo II*), the Supreme Court has held that “both history and the judgment
8 of Congress play important roles.” *Spokeo I*, 136 S. Ct. at 1549. History is instructive because an
9 intangible harm is likely to be concrete for standing purposes when it bears “a close relationship to
10 a harm that has traditionally been regarded as providing a basis for a lawsuit.” *Id.* Congress’s
11 judgment is particularly important because it is “well positioned to identify intangible harms” that
12 are in fact concrete for Article III purposes. *Id.* Congress has the power to create statutory rights
13 and causes of action “that will give rise to a case or controversy where none existed before.” *Id.*
14 Consequently, an intangible harm such as “the violation of a procedural right granted by statute
15 can be sufficient in some circumstances to constitute injury in fact. In other words, a plaintiff in
16 such a case need not allege any additional harm beyond the one Congress has identified.” *Id.*

17 While *Spokeo I* refers to Congress, neither side disputes that state legislatures are equally
18 well-positioned to determine when an intangible harm is a concrete injury. Our circuit said as
19 much when it held that “state law can create interests that support standing in federal courts. If
20 that were not so, there would not be Article III standing in most diversity cases, including run-of-
21 the-mill contract and property disputes. State statutes constitute state law that can create such
22 interests.” *Cantrell v. City of Long Beach*, 241 F.3d 674, 684 (9th Cir. 2001). While this
23 conclusion pre-dates *Spokeo I*, nothing there undercuts it. To be sure, state law cannot create
24 Article III standing where none exists under our federal precedents. But there is no good reason
25 why the judgment of a state legislature should be treated as less important than that of Congress in
26 deciding when the violation of a statutory grant in itself amounts to a real and concrete injury.

27 Our circuit has adopted decisions from sister circuits to hold that “an alleged procedural
28 violation [of a statute] can by itself manifest concrete injury where Congress conferred the

1 procedural right to protect a plaintiff’s concrete interests and where the procedural violation
 2 presents ‘a real risk of harm’ to that concrete interest.” *Spokeo II*, 867 F.3d at 1113 (internal
 3 citations omitted) (brackets in original). The dispositive inquiries are whether: (1) the statutory
 4 provisions at issue were established to protect the plaintiff’s concrete interests; and (2) the
 5 specifically alleged procedural violations “actually harm or present a material risk of harm” to
 6 those interests. *Id.*

7 **III. Concrete Injury**

8 The plain language of BIPA drives the standing analysis in this case. BIPA expresses the
 9 judgments of the Illinois legislature about the rights of Illinois citizens with respect to the
 10 collection of personal biometric data by corporations and businesses. *In re Facebook*, 185
 11 F. Supp. 3d at 1169 (citing 740 Ill. Comp. Stat. 14/5(b)). Specifically, BIPA manifests the Illinois
 12 legislature’s conclusions that:

13 (1) Biometrics are uniquely sensitive identifiers. “Biometrics are unlike other unique
 14 identifiers . . . [and] are biologically unique to the individual; therefore, once compromised, the
 15 individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from
 16 biometric-facilitated transactions.” 740 Ill. Comp. Stat. 14/5(c).

17 (2) Biometric technology is a new frontier subject to unpredictable developments. “The
 18 full ramifications of biometric technology are not fully known.” *Id.* at 14/5(f).

19 (3) People are apprehensive of transactions involving their biometrics. The
 20 “overwhelming majority of members of the public are weary of the use of biometrics when such
 21 information is tied to finances and other personal information” and are “deterred from partaking in
 22 biometric identifier-facilitated transactions.” *Id.* at 14/5(d)-(e).

23 (4) Regulation of biometric collection, use, and storage serves the public interest. The
 24 “public welfare, security and safety will be served by regulating the collection, use, safeguarding,
 25 handling, storage, retention, and destruction of biometric identifiers and information.” *Id.* at
 26 14/5(g).

27 To address these concerns and protect the rights of its residents to control their biometric
 28 information, the Illinois legislature enacted several measures. Section 15(a) of BIPA requires

1 private entities possessing biometric data to publish written policies on data retention and
2 destruction. Section 15(b) provides that biometric data may not be obtained without (1) written
3 notice that biometric data is at issue, (2) written notice of why and for how long the data is being
4 collected and stored, and (3) written consent from the subject. Sections 15(c) and (d) limit the
5 sale, trade, and disclosure of biometric data, and Section 15(e) sets security standards for storing
6 data. Plaintiffs have sued under Sections 15(a) and (b) for lack of notice and consent.

7 These provisions, along with the plain text of BIPA as a whole, leave little question that
8 the Illinois legislature codified a right of privacy in personal biometric information. There is
9 equally little doubt about the legislature's judgment that a violation of BIPA's procedures would
10 cause actual and concrete harm. BIPA vested in Illinois residents the right to control their
11 biometric information by requiring notice before collection and giving residents the power to say
12 no by withholding consent. As the Illinois legislature found, these procedural protections are
13 particularly crucial in our digital world because technology now permits the wholesale collection
14 and storage of an individual's unique biometric identifiers -- identifiers that cannot be changed if
15 compromised or misused. When an online service simply disregards the Illinois procedures, as
16 Facebook is alleged to have done, the right of the individual to maintain her biometric privacy
17 vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized.

18 Consequently, the abrogation of the procedural rights mandated by BIPA necessarily
19 amounts to a concrete injury. This injury is worlds away from the trivial harm of a mishandled zip
20 code or credit card receipt. A violation of the BIPA notice and consent procedures infringes the
21 very privacy rights the Illinois legislature sought to protect by enacting BIPA. That is
22 quintessentially an intangible harm that constitutes a concrete injury in fact. *See Spokeo II*, 867
23 F.3d at 1113 (and cases cited therein).

24 The Illinois legislature's considered judgments in enacting BIPA are also well-grounded in
25 a long tradition of claims actionable in privacy law. The "common law and the literal
26 understanding of privacy encompass the individual's control of information concerning his or her
27 person." *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017) (quoting *U.S. Dep't of*
28 *Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989)). "Violations of

1 the right to privacy have long been actionable at common law.” *Id.* “Actions to remedy
2 defendants’ invasions of privacy, intrusion upon seclusion, and nuisance have long been heard by
3 American courts, and the right of privacy is recognized by most states.” *Van Patten v. Vertical*
4 *Fitness Grp., LLC*, 847 F.3d 1037, 1043 (9th Cir. 2017) (citing Restatement (Second) of Torts §
5 652(B) (Am. Law Inst. 1977)).

6 Facebook insists that the collection of biometric information without notice or consent can
7 never support Article III standing without “*real-world* harms” such as adverse employment
8 impacts or even just “anxiety.” *See, e.g.*, Dkt. No. 227 at 1, and 5-7 (emphasis in original). That
9 contention exceeds the law. The Supreme Court has expressly recognized that the violation of
10 statutory procedural rights in itself can be sufficient, without any additional harm alleged. *Spokeo*
11 *I*, 136 S.Ct. at 1549. Our circuit has also found that “privacy torts do not always require additional
12 consequences to be actionable.” *Eichenberger*, 876 F.3d at 983. Intrusion on privacy alone can be
13 a concrete injury. *Id.*; *see also Mount v. PulsePoint, Inc.*, 684 F. App’x 32, 34 (2d Cir. 2017), as
14 amended (May 3, 2017) (unauthorized access to and monitoring of web-browsing is concrete
15 injury); *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 843 (N.D. Cal. 2017)
16 (tracking users’ web-browsing history is concrete injury). Our circuit has specifically affirmed
17 findings of concrete injury, and standing to sue, when plaintiffs were deprived of procedures that
18 protected privacy interests without any attendant embarrassment, job loss, stress or other
19 additional injury. *See, e.g., Syed v. M-I, LLC*, 853 F.3d 492, 499 (9th Cir. 2017) (loss of statutory
20 right to authorize credit check by prospective employer); *Eichenberger*, 876 F.3d at 983-84 (loss
21 of control over personal information under Video Privacy Protection Act).

22 The cases Facebook relies upon to contest standing are readily distinguishable. In *Gubala*
23 *v. Time Warner Cable, Inc.*, 846 F.3d 909 (7th Cir. 2017), for example, the plaintiff sued Time
24 Warner for retaining his social security number and other personal information in violation of the
25 Cable Communications Policy Act. But that is of scant relevance here because BIPA expressly
26 recognizes that social security numbers do not implicate the kinds of privacy concerns that
27 biometric identifiers do. Biometric identifiers, as the Illinois legislature found, are “unlike other
28

1 unique identifiers” such as “social security numbers,” because those “when compromised, can be
2 changed.” 740 Ill. Comp. Stat. 14/5(c).

3 In *McCullough v. Smarte Carte, Inc.*, No. 16 C 03777, 2016 WL 4077108 (N.D. Ill. Aug.
4 1, 2016), a case brought under BIPA, locker rental customers in Illinois had to complete their
5 rentals by “plac[ing] their finger on a fingerprint scanner, which is then displayed on the screen;
6 finally, the screen displays the locker number and unlocks the locker.” *Id.* at *1. The court found
7 that “a customer would understand that Smarte Carte collects and retains their fingerprint data for
8 at least the duration of the rental. The system would not work otherwise.” *Id.* n.1.

9 So too for *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499, 513
10 (S.D.N.Y. 2017), another decision under BIPA that the Second Circuit affirmed in part, vacated in
11 part, and remanded in *Santana v. Take-Two Interactive Software, Inc.*, ___ Fed. Appx. ___, No.
12 17-303, 2017 WL 5592589 (2d Cir. Nov. 21, 2017). In that case, the plaintiffs bought a basketball
13 videogame that allowed players to create personalized “avatars” using their own faces. 2017 WL
14 5592589 at *1. To make an avatar, players had to scan their faces for approximately 15 minutes
15 by standing “within 6 to 12 inches of the camera” and slowly moving “their heads 30 degrees to
16 the left and to the right.” *Id.* Critically, before a player could create an avatar, she was required to
17 consent by pressing “continue” after reading a notice stating that the “face scan” might be
18 recorded. *Id.* In these circumstances, the district court found that the plaintiffs clearly knew that
19 “Take-Two had to collect data based upon their faces in order to create the personalized basketball
20 avatars, and that a derivative of the data would be stored in the resulting digital faces of those
21 avatars so long as those avatars existed.” *Vigil*, 235 F. Supp. 3d at 515. The Second Circuit had
22 little troubling concluding that Take-Two had satisfied BIPA’s notice and consent provisions, and
23 that the plaintiffs could not allege a material risk of harm to a concrete interest protected by the
24 statute. 2017 WL 5592589 at *3.

25 While *McCullough* and *Vigil* involved BIPA, they turned on circumstances that are a far
26 cry from the ones alleged here. In those cases, the plaintiffs indisputably knew that their biometric
27 data would be collected before they accepted the services offered by the businesses involved.
28 *Vigil* had the specific fact of prior written notice and click-through consent. In each case, the

1 plaintiffs had sufficient notice to make a meaningful decision about whether to permit the data
2 collection. That factual difference makes these cases of little value in addressing the allegations in
3 the consolidated complaint that Facebook afforded plaintiffs no notice and no opportunity to say
4 no.

5 Facebook's reliance on *Spokeo II* is also misplaced. It highlights a comment in a footnote
6 that a plaintiff might have a hard time showing standing under FCRA provisions "which do *not*
7 turn on any alleged reporting inaccuracy." *Spokeo II*, 867 F.3d at 1116 n.2 (emphasis in original).
8 This point appears to be a further elaboration on Facebook's "real harm" contention and is
9 unpersuasive for the same reasons. But even taken on its own, it is again of little relevance
10 because BIPA, unlike FCRA, targets the unauthorized collection of information in the first
11 instance. The two statutes are sufficiently distinct so that *Spokeo II*'s FCRA concerns simply do
12 not apply here. *See Eichenberger*, 876 F.3d at 983-84 (*Spokeo I* and *II* distinguishable because
13 Video Privacy Protection Act, unlike FCRA, identifies a substantive right to privacy). In addition,
14 as the footnote itself suggests, the comment is likely dicta because the plaintiff in *Spokeo II* did
15 not allege a claim independent of a reporting inaccuracy. *Spokeo II*, 867 F.3d at 1116 n.2.

16 In addition to its legal arguments, Facebook has submitted its user agreement and data
17 policy, deposition excerpts and other extrinsic evidence to contend that BIPA's notice and consent
18 requirements were actually satisfied. *See, e.g.*, Dkt. No. 227 at 10-11. While that may or may not
19 prove true in the end, the salient point for present purposes is that notice and consent are
20 inextricably intertwined with the merits of plaintiffs' claims. The parties contest the facts
21 surrounding those issues, in contrast to the largely undisputed material facts in *McCullough* and
22 *Vigil*. These dispositive disputes on the merits should be decided on summary judgment or at trial,
23 and not in the Rule 12(b)(1) jurisdictional context. *Safe Air*, 373 F.3d at 1039.

CONCLUSION

Facebook's motion to dismiss for lack of subject matter jurisdiction is **DENIED**.

IT IS SO ORDERED.

Dated: February 26, 2018



JAMES DONATO
United States District Judge

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28