

DEC 10 2025

David W. Slayton, Executive Officer/Clerk of Court
By: L. Gomez, Deputy

Superior Court of California

County of Los Angeles

Department 50

EMILY RODRIGUEZ,

Plaintiff,

vs.

INK AMERICA INTERNATIONAL GROUP
LLC, a California entity d/b/a
WWW.GODSSMUSIC.COM,

Defendant.

Case No.: 25STCV15350

Hearing Date: December 10, 2025

Hearing Time: 2:00 p.m.

[PENTATIVE] ORDER RE:

MOTION FOR JUDGMENT ON THE
PLEADINGS BY DEFENDANT INK
AMERICA

Background

Plaintiff Emily Rodriguez (Plaintiff) filed this action on May 27, 2025, against Defendant Ink America International Group LLC (Ink America). Plaintiff filed a First Amended Complaint (FAC) on August 08, 2025. The Complaint asserts a sole cause of action for violation of California Invasion of Privacy Act under Penal Code section 638.51 (CIPA).

The following facts are taken from the allegations of the FAC, which the Court accepts as true for purposes of the motion.

Ink America owns and operates the website godpsmusic.com (the Website). When a user accesses the website, the website collects the website visitors IP address and causes the users computer to install a beacon software that allows third parties to collect information and “fingerprint” users. (FAC ¶¶ 1, 37, 46, 58.) In particular, Plaintiff alleges that the analytical tools employed collect and link together a wide range of identifiers, including users IP addresses, operating system and browser data, screen resolution, geolocation data, email addresses, mobile advertising IDs, embedded social medial identities, customer or loyalty IDs, cookies, and device

1 signatures. (FAC ¶ 89.) Plaintiff alleges that the analytical tools employed (log files and/or
2 beacons) are each a pen register or a trap and trace device as defined in Cal. Penal Code section
3 638.50. (FAC ¶ 108-109.)

4 Ink America now moves for an order granting judgment on the pleadings to the first
5 amended complaint for CIPA under Penal Code section 638.51. Plaintiff in opposition contends
6 the statutory based claim is properly pled. Ink America has filed a reply.

7 8 ***Request for Judicial Notice***

9 The Court grants the parties' requests for judicial notice and takes notice of the submitted
10 legislative material and court records as public records.

11 12 ***Discussion***

13 **A. Legal Standard**

14 A motion for judgment on the pleadings has the same function as a general demurrer but
15 is made after the time for demurrer has expired. Except as provided by Code of Civil Procedure
16 section 438, the rules governing demurrers apply. (*Cloud v. Northrop Grumman Corp.* (1998) 67
17 Cal.App.4th 995, 999.) A motion by a defendant can be made on the ground that the complaint
18 (or any cause of action therein) "does not state facts sufficient to constitute a cause of action
19 against that defendant." (Code Civ. Proc., § 438, subd. (c)(1)(B)(ii).) Pursuant to Code of Civil
20 Procedure section 438, subdivision (d), "[t]he grounds for motion provided for in this section
21 shall appear on the face of the challenged pleading or from any matter of which the court is
22 required to take judicial notice."

23 "To survive a demurrer, the complaint need only allege facts sufficient to state a cause of
24 action; each evidentiary fact that might eventually form part of the plaintiff's proof need not be
25 alleged." (*C.A. v. William S. Hart Union High School Dist.* (2012) 53 Cal.4th 861, 872.) For the
26 purpose of testing the sufficiency of the cause of action, the demurrer admits the truth of all
27 material facts properly pleaded. (*Aubry v. Tri-City Hospital Dist.* (1992) 2 Cal.4th 962, 966-967.)
28

1 A demurrer “does not admit contentions, deductions or conclusions of fact or law.” (*Daar v.*
2 *Yellow Cab Co.* (1967) 67 Cal.2d 695, 713.)

3
4 B. Violation of California Invasion of Privacy Act Section 638.51

5 For purposes of the motion, Ink America contends the operative complaint fails to allege
6 sufficient facts establishing the actual use of a “pen register” or “trap and trace device” within
7 the meaning of the California Invasion of Privacy Act (CIPA) notwithstanding the admitted
8 allegations in the first amended complaint regarding the use of said technology. (Motion p. 8-
9 11.) Plaintiff argues that the software constitutes a “pen register” or “trap and trace device”
10 because the software identifies or captures information about a user when a user contacts the
11 website.

12 There is currently no published appellate California authority about whether such causes
13 of action are viable or whether such software can fall under the definition of a “pen register” or
14 “trap and trace device” within the meaning of CIPA. As a result, courts have reached divergent
15 conclusions about the scope of Cal. Penal Code section 638.51. *See Deivaprakash v. Condé Nast*
16 *Digital*, - F. Supp. 3d -, 2025 WL 2541952 (N.D. Cal. Sept. 4, 2025) (holding that user
17 sufficiently alleged that operator’s trackers were a prohibited pen register under CIPA); *In re*
18 *Meta Pixel Tax Filing Cases*, - F. Supp. 3d -, 2025 WL 2243615 (N.D. Cal. Aug. 6, 2025)
19 (holding that complaint clearly alleged that company used tracking device, a pen register, in
20 violation of CIPA); *Casillas v. Transitions Optical*, Case No. 23STCV30742 (Cal. Super. Apr.
21 23, 2024) (sustaining a demurrer to a complaint for violation of CIPA, Penal Code section
22 638.51).

23 CIPA Penal Code section 638.51(a) proscribes any “person” from “install[ing] or us[ing]
24 a pen register or a trap and trace device without first obtaining a court order.” Subdivision (b)
25 permits the use of such a device if, among other things, the consent of the user has been
26 obtained. (Cal. Penal Code § 638.51(b).)

1 CIPA defines a “pen register” as “a device or process that records or decodes dialing,
2 routing, addressing, or signaling information transmitted by an instrument or facility from which
3 a wire or electronic communication is transmitted, but not the contents of a communication.”
4 (Cal. Penal Code § 638.50(b).) A “[t]rap and trace device means any device or process that
5 captures the incoming electronic or other impulses that identify the originating number or other
6 dialing, routing, addressing, or signaling information reasonably likely to identify the source of a
7 wire or electronic communication, but not the contents of a communication.” (Cal. Penal Code §
8 638.50(c).) As characterized by Plaintiff in her first amended complaint, “a ‘pen register’ is a
9 ‘device or process’ that records outgoing information, whereas a ‘trap and trace device’ is a
10 ‘device or process’ that records incoming information.” (FAC ¶ 16.)

11 Ink America contends that CIPA’s trap and trace or pen register definition does not apply
12 to websites. Ink America argues that CIPA has been interpreted and applied to prevent the
13 collection of private call log information from telephones, not the collection of data by website
14 software. However, Plaintiff argues that as defined under Cal. Penal Code § 638.50(c) a pen
15 register or trap and trace device is a “device or process” and need only capture the information of
16 an “electronic communication,” not necessarily a telephonic communication.

17 Plaintiff cites *Greenley v. Kochava, Inc.* (2023) 684 F.Supp.3d 1024, to stand for the
18 proposition that “pen registers take the form of software.” The *Greenley* court emphasized that
19 the statutory definition of Cal. Penal Code § 63850 is focused on the “type of data a pen register
20 collects – ‘dialing, routing, addressing, or signaling information...’ but is vague and inclusive as
21 to the form of the collection tool – ‘a device or process.’” (*Ibid.*) The *Greenley* court concluded
22 that “[t]his indicates courts should focus less on the form of the data collector and more on the
23 result.” (*Ibid.*) Accordingly, the *Greenley* court held that” [a] process can take many forms[,]
24 [a]mong them is software that identifies consumers, gathers data, and correlates that data through
25 unique ‘fingerprinting.’” (*Ibid.*) However, *Greenley*, unlike in this case, involved a claim against
26 the software developer that allegedly captured the data, not the consumer-facing website operator
27 that used the software.
28

1 Further, the language of Penal Code § 638.50 defining trap and trace devices follows the
2 language of 18 U.S.C § 3127(4), which was modified by the USA Patriot Act of 2001 to include
3 electronic communications beyond telephonic communications. (Pub. L. No. 107-56, § 216, 115
4 Stat. 272 (2001).) The legislative history indicates that the change “ensures that the pen register
5 and trap and trace provisions apply to facilities other than telephonic lines.” (147 Cong. Rec.
6 S10990-02, 147 Cong. Rec. S10990-02, S11006, 2001 WL 1297566.) However, it appears that
7 CIPA’s history and structure represents a telephonic limitation, referenced throughout the
8 statutory scheme.

9 In construing a statute, the Court must determine the Legislature’s intent to effectuate the
10 purpose of the statute, giving the statute’s words their usual and ordinary meaning. (*Day v. City*
11 *of Fontana* (2001) 25 Cal.4th 268, 272.) If “the statutory terms are ambiguous,” the Court may
12 examine “extrinsic sources” and “select the construction that comports most closely with the
13 apparent intent of the Legislature... and to avoid an interpretation that would lead to absurd
14 consequences.” (*Ibid.*) As discussed above, there is some ambiguity as to the application and
15 scope of the definition of pen register and trap and trace device as defined in Penal Code §
16 638.50. Thus, an examination of extrinsic sources to determine the interpretation that comports
17 most closely with the Legislative intent is proper.

18 The penal code requires that interpretation of its provisions include only those offenses
19 that come clearly within the import of the language and will not be given application beyond
20 their plain intent. (*DeMille v. American Federation of Radio Artists* (1947) 31 Cal.2d 139, 156.)
21 When the language of a penal statute is ambiguous or reasonably susceptible to multiple
22 interpretations, courts construe the statute as favorably to criminal defendants as reasonably
23 permitted by the statutory language and the circumstances. (*People v. Robles* (2000) 23 Cal.4th
24 1106, 1115.) Thus, with construction of a criminal statute, the defendant must be given the
25 benefit of every reasonable doubt as to whether the statute applies. (*In re Zerbe* (1964) 60 Cal.2d
26 666, 668.)

1 The legislative history indicates that CIPA's provisions do not concern the analytical
2 tools employed here. Rather, CIPA's structure and history indicate that its pen-register
3 provisions were aimed at telephonic-style surveillance, not at the routine operation of
4 commercial websites or analytical software. As such, the statute cannot reasonably be read as
5 broadly as Plaintiff attempts to read it.

6 If the California Legislature wanted to apply § 638.52 to the website tracking tools, it
7 could do so by amending such provision. The Legislature's drafting in related provisions
8 confirms that it knows how to regulate internet-based activity when it wishes to do so.
9 Specifically, the Legislature has expressly referenced "internet" or "online" communications and
10 services when extending protections beyond traditional telephonic technologies. For example,
11 the California Legislature added Cal. Penal Code § 632.01 in 2017. This provision punishes
12 anyone who violates § 632(a) and then intentionally discloses or distributes, in any manner, in
13 any forum, including, but not limited to, Internet Web sites and social media ... the contents of a
14 confidential communication with a health care provider" (See Cal. Penal Code § 632.01.)
15 "When the Legislature has carefully employed a term in one place and has excluded it in another,
16 it should not be implied where excluded." (internal quotations and citations omitted) (*Bradsbery*
17 *v. Vicar Operating, Inc.* (2025) 110 Cal.App.5th 899, 910.)

18 As indicated by Ink America, websites have used the software at issue here when the
19 Legislature enacted penal code § 638.52 in 2015 and when it was amended in 2016 and 2022.
20 The absence of any comparable reference to website communications in Penal Code § 638
21 indicates a deliberate choice not to sweep ordinary website analytics within CIPA's pen register
22 and trap and trace provisions. Additionally, pending Legislation, Senate Bill 690, shows a
23 Legislative intent that CIPA was not intended to apply to the website tracking tools at issue. In
24 describing SB 690's purpose, Senator Anna Caballero stated:

25
26 "I rise today to present SB 690, a Bill to protect California businesses from a
27 wave of abusive and predatory lawsuits that are threatening jobs, innovation, and
28

1 the very ability to do business in our state. [] California already has the strongest
2 privacy law in the nation, the California Consumer Protection Act, or CCPA.
3 Back in 2018, this Legislature passed CCPA to give consumers real control over
4 their data using a modern opt out approach. Suing under CIPA for activity that's
5 already governed by the CCPA goes against legislative intent, creates confusion,
6 punishes compliance, and doesn't make Californians any safer. A private
7 settlement doesn't create stronger protections for consumer or clearer rules for
8 business.”

9
10 SB 690's stated purpose indicates that CIPA was not intended to apply to website
11 tracking tools. Instead, such conduct is intended by the Legislature to be covered by the CCPA
12 and CPRA. The CCPA provides certain defined rights and compliance obligations for data
13 collection via internet connectivity. Under the CCPA, consumers have the right to: (1) know
14 what personal information a business collects (Civ. Code § 1798.110), (2) delete the personal
15 information collected (Civ. Code § 1798.106), (3) opt-out of the sale of personal information
16 (Civ. Code § 1798.120), (4) limit disclosure and use of sensitive information (Civ. Code §
17 17898.121), and (5) to non-retaliation for exercising their CCPA rights (Civ. Code § 1798.125).

18 Notably, the CCPA expressly contemplates businesses will collect and use personal data
19 so long as a regulatory framework is followed. (Civ. Code §§ 1798.100 et seq.) Importantly, the
20 CCPA does not require that users provide express consent prior to the collection of data. (*Ibid.*)
21 This regime does not require prohibit such data collection or require a court order. Plaintiff's
22 expansive reading of CIPA, criminalizing web based analytical tools, would seemingly render
23 CCPA void. Specifically, if website analytic tools are interpreted to fall within the ambit of Penal
24 Code § 638.51, using them without a court order would violate CIPA. However, CCPA presumes
25 that such tools will be employed so long as the proper procedures such as notice, opt-out, and
26 deletion are followed.

1 In *Licea v. Hickory Farms, LLC* (2024) 2024 WL 1698147, the court found that “public
2 policy strongly disputes Plaintiff’s potential interpretation of privacy laws as one rendering every
3 single entity voluntarily visited by a potential plaintiff, thereby providing an IP address for
4 purposes of connecting the website, as a violator. Such a broad-based interpretation would
5 potentially disrupt a large swath of internet commerce without further refinement as the precise
6 basis of liability, which the court declines to consider.” This Court finds that reasoning
7 persuasive and adopts it here.

8 The pen register statute did not, and does not, criminalize the process by which websites
9 communicate with users who choose to access them. Penal Code § 638.50 states that a pen
10 register does not include a “process used by a provider or customer of [an] ... electronic
11 communication service for ... communications service provided by such provider ... or other
12 similar services in the ordinary course of business.” (Pen. Code, § 638.50, subd. (b).) “Electronic
13 communication” is broadly defined to include “any transfer of signs, signals, writing, images,
14 sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic,
15 photoelectric or photo-optical system.” (Pen. Code, § 629.51, subd. (a)(2).) The broad definition
16 of “electronic communications” reasonably indicates that an electronic communications service
17 provider includes website operators. Moreover, even if the process of collecting IP addresses is
18 deemed a pen register, there is no liability when an electronic communication service does so to
19 “operate, maintain, and test [an] ... electronic communication service” or to “record the fact that
20 [an] ... electronic communication was initiated or completed” to protect against unlawful or
21 abusive use of the service. (Pen. Code, § 638.51, subd. (b).) Ink America’s website is an
22 electronic communication service under the terms of the statute, and obtaining IP addresses from
23 ordinary user access does not violate the pen register statute.

24 Accordingly, if the Legislature wishes to criminalize the use of the analytical tools at
25 issue in this case, it may do so by amending or adding to CIPA’s statutory scheme. As stated
26 above, the Court finds that Penal Code § 638 does not clearly apply to the web functions at issue
27 in this case and refuses to expand the interpretation of the statute in ways not clearly intended by
28

1 the Legislature. As such, the FAC fails to allege a cause of action for violation of California
2 Invasion of Privacy Act ("CIPA"), Penal Code section 638.51.

3
4 **Conclusion**

5 Based on the foregoing, the Court GRANTS Ink America's motion for judgment on the
6 pleadings without leave to amend.

7 Ink America is ordered to give notice of this Order. *Ink America is ordered to*
8 *file & serve a proposed judgment within 10 days of this Order.*

9 ATED: December 10, 2025

Teresa A. Beaudet

Hon. Teresa A. Beaudet
Judge, Los Angeles Superior Court

10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28