

NO. 22-15815

**IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

BRANDON BRISKIN,
ON BEHALF OF HIMSELF AND THOSE SIMILARLY SITUATED,

PLAINTIFF-APPELLANT,

V.

SHOPIFY INC., ET AL.,

DEFENDANTS-APPELLEES.

On Appeal from the United States District Court
for the Northern District of California
Case No. 4:21-cv-06269-PJH
The Honorable Phyllis J. Hamilton

**BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION AND
UC BERKELEY CENTER FOR CONSUMER LAW & ECONOMIC
JUSTICE IN SUPPORT OF PLAINTIFF-APPELLANT AND
REVERSAL**

Seth E. Mermin
David S. Nahmias
UC BERKELEY CENTER FOR CONSUMER
LAW & ECONOMIC JUSTICE
305 Berkeley Law
Berkeley, CA 94720-7200
Email: tmermin@law.berkeley.edu
dnahmias@law.berkeley.edu
Telephone: (510) 643-3519

*Counsel for Amicus Curiae
UC Berkeley Center For
Consumer Law & Economic Justice*

F. Mario Trujillo
Victoria J. Noble
Corynne McSherry
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Email: mario@eff.org
Telephone: (415) 436-9333
Fax: (415) 436-9993

*Counsel for Amicus Curiae
Electronic Frontier Foundation*

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *amici* state that they do not have a parent corporation and that no publicly held corporation owns 10% or more of their stock.

Dated: July 2, 2024

By: /s/ F. Mario Trujillo
F. Mario Trujillo

TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENT	i
TABLE OF CONTENTS	ii
TABLE OF AUTHORITIES.....	iv
STATEMENT OF INTEREST OF <i>AMICI CURIAE</i>	1
INTRODUCTION.....	2
ARGUMENT	4
I. Large Companies Form Relevant Contacts With The Jurisdiction From Which They Extract Personal Data—Before, During, And After Collection.....	4
A. Many Players In The Data Processing Ecosystem Target And Profit From Personal Data Collected From A Specific Jurisdiction.....	4
B. The Personal Jurisdiction Analysis Should Consider Whether The Defendant Has Allegedly Structured Its Data Processing Activities In Light Of Specific State Laws.....	7
II. Large Scale, Location-Aware Targeting And Data Extraction Alleged In This Case Satisfies Constitutional Specific Jurisdiction Requirements.	8
A. Shopify Purposefully Targeted California For Data Collection.	9
1. Shopify’s Allegedly Tortious Data Collection Occurred In California.....	10
2. Shopify Intentionally Formed Business Relationships And Data Policies, Giving It Access To Californians’ Personal Data.....	12
3. Shopify Used Personal Data It Collected To Individually Profile California Consumers.....	13
4. Extending Personal Jurisdiction Over Shopify Would Not Create Universal Jurisdiction For Online Platforms.	14

B. Briskin’s Privacy Claims “Arise Out Of Or Relate To” Shopify’s California Business Contacts Formed To Gain Access To Personal Data.	15
CONCLUSION	16
CERTIFICATE OF COMPLIANCE	18
CERTIFICATE OF SERVICE.....	19

TABLE OF AUTHORITIES

Cases

<i>Briskin v. Shopify, Inc.</i> , 87 F.4th 404 (9th Cir. 2023)	10
<i>Burger King Corp. v. Rudzewicz</i> , 471 U.S. 462 (1985).....	8, 12
<i>Calder v. Jones</i> , 465 U.S. 783 (1984).....	5, 10, 14
<i>Chien v. Bumble Inc.</i> , 641 F. Supp. 3d 913 (S.D. Cal. 2022).....	13
<i>Davis v. Cranfield Aerospace Sols.</i> , 71 F.4th 1154 (9th Cir. 2023)	4
<i>Doe v. WebGroup Czech Republic, a.s.</i> , 93 F.4th 442 (9th Cir. 2024)	14, 15
<i>Ford Motor Co. v. Montana Eighth Jud. Dist. Ct.</i> , 592 U.S. 351 (2021).....	16
<i>Glob. Commodities Trading Grp., Inc. v. Beneficio de Arroz Choloma, S.A.</i> , 972 F.3d 1101 (9th Cir. 2020)	4
<i>Herbal Brands, Inc. v. Photoplaza</i> , 72 F.4th 1085 (9th Cir. 2023)	8, 10, 11
<i>In re W. States Wholesale Nat. Gas Antitrust Litig.</i> , 715 F.3d 716 (9th Cir. 2013)	15
<i>Intercon, Inc. v. Bell Atl. Internet Sols., Inc.</i> , 205 F.3d 1244 (10th Cir. 2000)	11
<i>Keeton v. Hustler Mag.</i> , 465 U.S. 770, (1984).....	8
<i>MacDermid, Inc. v. Deiter</i> , 702 F.3d 725 (2d Cir. 2012)	11
<i>Mavrix Photo, Inc. v. Brand Techs., Inc.</i> , 647 F.3d 1218 (9th Cir. 2011)	5, 10, 15
<i>Myers v. Bennett L. Offs.</i> , 238 F.3d 1068 (9th Cir. 2001)	11, 14

Schwarzenegger v. Fred Martin Motor Co.,
374 F.3d 797 (9th Cir. 2004)12

UMG Recordings, Inc. v. Kurbanov,
963 F.3d 344 (4th Cir. 2020)10

Walden v. Fiore,
571 U.S. 277 (2014).....10

Will Co., Ltd. v. Lee,
47 F.4th 917 (9th Cir. 2022)14, 15

Yamashita v. LG Chem, Ltd.,
62 F.4th 496 (9th Cir. 2023)15

Statutes

Cal. Civ. Code § 1798.100(d).....7, 13

Cal. Code Regs. tit. 11 § 7020.....8

Cal. Code Regs. tit. 11 § 7050(c)8

Other Authorities

Andrew Folks, *US State Privacy Legislation Tracker*, IAPP.....7

Bennett Cyphers and Gennie Gebhart, *Behind the One-Way Mirror*,
EFF (2019).....2, 6

California Privacy Protection Agency, *FAQs, 4. Who must comply
with the CCPA*5

California Privacy Protection Agency, *What General Notices Are
Required By The CCPA?*8

EFF, *Geolocation Privacy*.....1

EFF, *Location Privacy*6

EFF, *Privacy Badger*1

EFF, *Privacy First: A Better Way to Address Online Harms* (Nov. 14, 2023).....1

IAB, *Location-based Marketing Playbook for Retailers* (April 2017)7

IAPP, Resource Center, *Data Processing*5

Jennifer Lynch, *Is This the End of Geofence Warrants?*, EFF (Dec. 13, 2023)7

Kashmir Hill, *Automakers Are Sharing Consumers’ Driving Behavior With
Insurance Companies*, NYT (March 13, 2024)7

Meta, Retargeting starts with finding people who have engaged with your business14

Omer Tene and Gabe Maldoff, CNIL sets parameters for processors’ reuse of data for product improvement, IAPP6

Shopify Data Processing Addendum13

Shopify help center, US state privacy laws13

Shopify, Privacy Policy, (Updated March 2, 2023)13

Shopify, Shopify Data Processing Addendum7

STATEMENT OF INTEREST OF *AMICI CURIAE*¹

The Electronic Frontier Foundation (“EFF”) is a non-profit civil liberties organization with more than 30,000 active donors that has worked for more than 30 years to ensure that technology supports freedom, justice, and innovation for all people of the world. As part of that mission, EFF has supported the introduction and enforcement of consumer data privacy laws that balance the public rights of both privacy and free expression. In addition to litigation² and legislative advocacy,³ EFF develops free data privacy tools⁴ and works to educate the public regarding the potential threat unconstrained data processing may pose to civil

¹ Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(4)(E), *amici* certify that no person or entity, other than amici curiae, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part. The parties have consented to the filing of this brief. EFF files this brief pursuant to Federal Rule of Appellate Procedure 29(a)(2) and Circuit Rule 29-2(a).

² See EFF, *Geolocation Privacy*, <https://www.eff.org/cases/geolocation-privacy>; *Stark v. Patreon*, Case. 3:22-cv-03131, ECF. 95-1 (ND Cal. Dec. 20, 2023), https://www.eff.org/files/2024/01/04/095-1_amicus_curiae_brief_of_eff_cdt_and_aclu_filed_2023-12-20.pdf; *In Re: Marriott International Customer Data Security Breach Litigation*, No. 22-1744, ECF 53-1 (4th Cir. Nov. 22, 2022), https://www.eff.org/files/2022/11/30/2022-11-22_-_in_re_marriott_4th_cir._-_amicus_brief_of_eff_and_epic.pdf.

³ EFF, *Privacy First: A Better Way to Address Online Harms* (Nov. 14, 2023), <https://www.eff.org/wp/privacy-first-better-way-address-online-harms>.

⁴ EFF, *Privacy Badger*, <https://privacybadger.org>.

liberties and human rights.⁵

The Center for Consumer Law and Economic Justice, housed at the UC Berkeley School of Law, is the leading law school research and advocacy center dedicated to ensuring safe, equal, and fair access to the marketplace, including on digital and e-commerce platforms. Through regular participation as *amicus curiae* in the U.S. Supreme Court, this Court, and other appellate courts around the nation, the Center seeks to develop and enhance protections for consumers and to foster economic justice. Third-party data collection and data harvesting, like the conduct at issue in this case, frequently occur without consumers' knowledge or consent and can result in significant harm to consumer privacy, access to credit, and equal treatment in the market. The Center appears in this proceeding to underscore the importance of establishing a viable regime of personal jurisdiction over digital defendants that will allow consumers meaningful access to the judicial system.

INTRODUCTION

In applying the Supreme Court's traditional personal jurisdiction standard to conduct on the internet, courts must tie the factual analysis to the type of unlawful conduct alleged. When, as alleged in this case, a corporation knowingly collects and processes vast amounts of personal data from consumers who reside inside a

⁵ Bennett Cyphers and Gennie Gebhart, *Behind the One-Way Mirror*, EFF (2019), https://www.eff.org/files/2019/12/11/behind_the_one-way_mirror-a_deep_dive_into_the_technology_of_corporate_surveillance.pdf.

jurisdiction, and uses that data to build profiles based in part on their location, the company forms different and much stronger in-state contacts than would a mere online publisher. Those robust contacts are more than enough to support a finding of personal jurisdiction in any state where those contacts were formed.

The in-state contacts arising from personal data collection and processing happen at each stage of the data lifecycle. They are formed when companies enter business relationships in the state to gain access to in-state consumers data; create state-specific policies that govern data processing; collect data directly from consumers within the state; and use that data to form individual profiles that can later be used to target residents based in part upon their locations within the state.

Here, Brisken alleges that Shopify Inc., Shopify (USA) Inc., and Shopify Payments (USA) Inc. (collectively “Shopify” or “Defendants”) knowingly targeted and profited from the California personal data market. Shopify’s sophisticated data collection activities included the extensive, intentional extraction of personal information from Californians’ computers; installation of Shopify-created tracking code on Californians’ devices; development of strategic relationships with California retailers to support data collection of Californians along with others; formation of California-specific data policies to gain access to the market; and monetization of known California users’ personal information.

Amici do not suggest that data processing and sales confer universal

jurisdiction. But where, as here, a company is credibly alleged to have knowingly collected consumer data from a particular state, it cannot fairly claim it has not expressly aimed its conduct toward that jurisdiction. The district court therefore properly may exercise jurisdiction over data collectors like Shopify.

ARGUMENT

I. LARGE COMPANIES FORM RELEVANT CONTACTS WITH THE JURISDICTION FROM WHICH THEY EXTRACT PERSONAL DATA—BEFORE, DURING, AND AFTER COLLECTION.

A. Many Players In The Data Processing Ecosystem Target And Profit From Personal Data Collected From A Specific Jurisdiction.

In keeping with Supreme Court precedent, this Court has held that, if it is reasonable to do so, a court may exercise specific personal jurisdiction over a case that arises from intentional, harmful activities that the defendant “expressly aimed” into the forum over the internet.⁶ *Mavrix Photo, Inc. v. Brand Techs., Inc.*, 647

⁶ While the parties focused on the purposeful direction test in this case, the purposeful availment test is equally relevant and would also be satisfied. There is no “rigid dividing line” that dictates applying purposeful availment to contract claims and purposeful direction to tort claims. *Davis v. Cranfield Aerospace Sols.*, 71 F.4th 1154, 1162 (9th Cir. 2023) (quoting *Glob. Commodities Trading Grp., Inc. v. Beneficio de Arroz Choloma, S.A.*, 972 F.3d 1101, 1107 (9th Cir. 2020)). Instead, when assessing minimum contacts courts must “comprehensively evaluate the extent of the defendant’s contacts with the forum state and those contacts’ relationship to the plaintiffs’ claims—which may mean looking at both purposeful availment and purposeful direction.” *Id.* See also Supp. Br. for Plaintiff-Appellant at 8, n.2.

F.3d 1218, 1227–29 (9th Cir. 2011). In the digital world, this typically involves the operation of an online service plus “something more.” *Id.* at 1229; *see also Calder v. Jones*, 465 U.S. 783, 789 (1984).

A company’s sourcing of data, collection of data, and profiling of consumers, especially based upon their location in a jurisdiction, may suffice to establish that “something more.”

To see why, it is helpful to understand how the data processing ecosystem works. The term “data processing” has become a shorthand that encompasses various stages of a company’s activities, including collection, use, retention, and transfer of consumers’ personal data.⁷ The ecosystem is made up of connected entities including consumers, businesses, service providers, and third-parties like data brokers.⁸ For example, in addition to facilitating online ordering, a service provider such as Shopify can generate additional profits by collecting personal data, including their geographic locations, from consumers, which it can use to build online profiles of those consumers.

Consumers—within the jurisdiction they reside—are the ultimate source of data collection. For example, large service providers that specialize in personal

⁷ IAPP, Resource Center, *Data Processing*, <https://iapp.org/resources/article/data-processing/>.

⁸ California Privacy Protection Agency, FAQs, 4. *Who must comply with the CCPA*, <https://cppa.ca.gov/faq>.

data processing can contract with a business that has an attractive user base that is likely to generate particularly valuable information.⁹ Under the terms of a contract, the service provider can then instruct the business to insert code onto the business's website or app, which allows the service provider to directly track a consumer.¹⁰ The nature of this tracking necessarily means that data is extracted directly from the consumer's device located within the relevant jurisdiction.¹¹ Only after collection from a consumer in a specific jurisdiction can the data be stored and used in other jurisdictions where the company's headquarters and servers reside.

That personal data can then be used to identify the consumer, including the consumer's home address, IP address, and other real-time geolocation information.¹² Location data can thus be used to build a profile and target that person based specifically on their jurisdiction for purposes of fraud detection, as

⁹ Omer Tene and Gabe Maldoff, *CNIL sets parameters for processors' reuse of data for product improvement*, IAPP, <https://iapp.org/news/a/cnil-sets-parameters-for-processors-reuse-of-data-for-product-improvement>.

¹⁰ *Behind the One-Way Mirror* at 15-17, https://www.eff.org/files/2019/12/11/behind_the_one-way_mirror-a_deep_dive_into_the_technology_of_corporate_surveillance.pdf (describing "identifiers created by trackers").

¹¹ *Id.*

¹² EFF, *Location Privacy*, <https://www.eff.org/issues/location-privacy>.

alleged here, but also advertising,¹³ predictive profiling,¹⁴ or to respond to unconstrained law enforcement requests.¹⁵

B. The Personal Jurisdiction Analysis Should Consider Whether The Defendant Has Allegedly Structured Its Data Processing Activities In Light Of Specific State Laws.

In order to protect the privacy interests of their residents, an increasing number of states, including California, have imposed additional requirements regulating these complex data processing relationships.¹⁶ When collecting personal data in California, for example, some companies must first enter into specialized contracts between businesses that set the terms of California-specific data processing.¹⁷ Companies must then create additional policies for processing

¹³ IAB, *Location-based Marketing Playbook for Retailers* (April 2017), https://www.iab.com/wp-content/uploads/2017/04/IAB_Location-Playbook-for-Retail-Marketers_FINAL.pdf.

¹⁴ Kashmir Hill, *Automakers Are Sharing Consumers' Driving Behavior With Insurance Companies*, NYT (March 13, 2024), <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.

¹⁵ Jennifer Lynch, *Is This the End of Geofence Warrants?*, EFF (Dec. 13, 2023), <https://www.eff.org/deeplinks/2023/12/end-geofence-warrants>.

¹⁶ Andrew Folks, *US State Privacy Legislation Tracker*, IAPP (Last Updated June 17, 28, 2024), <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>.

¹⁷ Cal. Civ. Code § 1798.100(d); *see also* Shopify, *Shopify Data Processing Addendum*, <https://www.shopify.com/legal/dpa>.

California-specific data.¹⁸ And companies must set up a process to handle the specific consumer privacy requests allowed by California law, like the right to know, correct, delete, port, or limit processing.¹⁹

As a result of this legal regime, companies collecting data from California consumers must know from whom, and from where, they are collecting data so that they can comply with California-specific requirements. Simply put, they must enter into “carefully structured” business relationships, *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 480 (1985), and exercise a significant “level of control” over the collection of data those relationships facilitate. *Herbal Brands, Inc. v. Photoplaza*, 72 F.4th 1085, 1094 (9th Cir. 2023). At the same time, the existence of these requirements puts businesses on fair notice that California has an express interest in redressing privacy-related injuries to its residents. *Keeton v. Hustler Mag.*, 465 U.S. 770, 777 (1984).

II. LARGE SCALE, LOCATION-AWARE TARGETING AND DATA EXTRACTION ALLEGED IN THIS CASE SATISFIES CONSTITUTIONAL SPECIFIC JURISDICTION REQUIREMENTS.

Based on the allegations in the Complaint, Shopify should be subject to suit

¹⁸ California Privacy Protection Agency, *What General Notices Are Required By The CCPA?*, https://cppa.ca.gov/pdf/general_notices.pdf.

¹⁹ *See* Cal. Code Regs. tit. 11 § 7020 (rules for businesses); Cal. Code Regs. tit. 11 § 7050(c) (rules for service providers).

in California for violations of a Californian’s privacy rights. Briskin alleges that Shopify installed tracking code on consumers’ devices located within California to collect personal data directly from California consumers. ER-93, ¶¶ 4-5. In order to gain access to these California consumers, Shopify allegedly courted and formed contracts with thousands of California merchants that set the terms of the data processing within the state. ER-97, ¶ 15. Shopify allegedly collected information that revealed users were located in the forum, such as shipping and billing address, IP address, and geolocation data. ER-106, ¶ 40. Among other things, this data allegedly enabled Shopify and other entities to form profiles on individual identifiable California consumers. ER-98, ¶ 17; ER-109, ¶¶ 42-43, 46-47.

Moreover, Shopify likely targeted its conduct to match California’s unique privacy regime. If, as alleged, Shopify is subject to the CCPA, ER-136, ¶ 139, it would have attempted to design its contracts and policies concerning data collected in California to meet California laws.

The allegations are more than enough to establish specific jurisdiction.

A. Shopify Purposefully Targeted California For Data Collection.

The “crux of this case” is whether Shopify “expressly aimed” its conduct at California by allegedly collecting, processing, and sharing personal data belonging to California consumers. *Briskin v. Shopify, Inc.*, 87 F.4th 404, 412-13 (9th Cir.

2023).²⁰ It did so by doing “something more” than passively offering a website to the world at large. *Mavrix Photo*, 647 F.3d at 1229.²¹

In data privacy cases like this one, several facts help to support the exercise of personal jurisdiction in states where these contacts are formed—including the place of collection, jurisdiction-specific business relationships and data policies, and the creation of individualized profiles. These facts differ from those in many personal jurisdiction cases about website publishers.

1. Shopify’s Allegedly Tortious Data Collection Occurred In California.

Personal jurisdiction is appropriate when “the defendants’ intentional tort actually occurred” within the forum. *Walden v. Fiore*, 571 U.S. 277, 287–88 (2014). The “strength” of the connection between the forum and defendants is “largely a function of the nature” of the alleged tort. *Id.* at 287.

Shopify’s alleged collection of personal data within the state comprised a “necessary element,” *id.* at 288, of the privacy claims. Specifically, Briskin alleges

²⁰ The Panel correctly held that Shopify’s conduct satisfied the first and third prongs of the *Calder* effects test because Plaintiff adequately alleged that Shopify (1) “committed intentional acts,” (3) causing “privacy-related harm that it knew was likely to be suffered in the forum state.” *Briskin*, 87 F.4th at 412.

²¹ The allegations that Shopify developed its own tool to extract consumer data makes its service highly interactive. *Herbal Brands*, 72 F.4th at 1092; *see also UMG Recordings, Inc. v. Kurbanov*, 963 F.3d 344, 353 (4th Cir. 2020) (noting “the Websites are certainly interactive to a degree, since they collect certain personal information from visitors”).

that Shopify surreptitiously installed code on California users' devices to extract personal data directly from them when Shopify knew they were located in California. ER-106, ¶ 40. *MacDermid, Inc. v. Deiter*, 702 F.3d 725, 730 (2d Cir. 2012) (defendant who retrieved confidential information from servers she knew were physically located in forum purposefully directed allegedly tortious activity at the forum); *Intercon, Inc. v. Bell Atl. Internet Sols., Inc.*, 205 F.3d 1244, 1247-48 (10th Cir. 2000) (defendant expressly aimed conduct at forum by intentionally misappropriating server located in forum).

The Ninth Circuit has held that a defendant “expressly aimed” its conduct at the forum by obtaining confidential credit reports on individuals that the defendant knew lived in the forum. *Myers v. Bennett L. Offs.*, 238 F.3d 1068, 1073–75 (9th Cir. 2001). The forum was “the focal point both of the credit report inquiry and of the harm suffered.” *Id.* at 1074–75 (cleaned up). Similar here. California is the focal point of Shopify’s alleged data collection from Briskin.²²

²² Extracting personal data directly from the forum state may not confer jurisdiction in every case. This Court has recognized that it can be unreasonable for a state’s courts to exercise jurisdiction over smaller online platforms in unfair circumstances—for example, when their purposeful direction or availment of a state is limited or when it would be very burdensome for them to defend themselves. *Herbal Brands*, 72 F.4th at 1097.

2. Shopify Intentionally Formed Business Relationships And Data Policies, Giving It Access To Californians' Personal Data.

Shopify also expressly aimed its injurious conduct at California by strategically exploiting the market through business contacts and California-specific policies, giving it access to personal data in California.

Briskin alleges that, as of 2018, Shopify formed contractual relationships and facilitated online orders for more than 80,000 California retailers, which have California consumers like Briskin. ER-96, ¶ 10, 12-13. Some of Shopify's largest customers are California companies, including a dense customer base in Los Angeles. *Id.* These contracts with California merchants show Shopify's contacts with the state. *See Burger King*, 471 U.S. at 480; *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 802 (9th Cir. 2004).

Those business relationships with California retailers—who have California customers—directly facilitated Shopify's alleged consumer privacy violations. Shopify's contracts with each California merchant expressly allowed Shopify to “collect, use, process and disclose” personal information from the consumers who placed online orders on the merchant's website. ER-97, ¶ 15. Additionally, processing payments for these retailers furnished the opportunity to install code on consumers' devices—the technical means used to extract personal information and surveil users' interactions with “thousands, if not millions” of websites. ER-116, ¶

63.

Shopify also had to develop California-specific data policies before it could exploit the market for California residents’ personal data—helping prove that its entry was targeted and not fortuitous. *Chien v. Bumble Inc.*, 641 F. Supp. 3d 913, 929-30 (S.D. Cal. 2022) (considering state-specific data policies in “something more” analysis). The data processing provisions in Shopify’s merchant contracts, ER-97, ¶ 15, are likely a necessary legal step to enter the California market under the state’s comprehensive data privacy law. *See* Cal. Civ. Code § 1798.100(d). Shopify’s other required California-specific data policies—many of which are public—could be a source of jurisdictional discovery, if the court allowed it.²³

3. Shopify Used Personal Data It Collected To Individually Profile California Consumers.

Shopify used Californians’ personal information—including their geographic location and addresses—to create products that it provided to customers, such as risk mitigation tools and extensive “user profiles” of individuals’ online activities. ER-106–108. After collection, the personal data that Shopify allegedly used and shared “concerned the California activities of a

²³ See e.g., Shopify, *Shopify Data Processing Addendum*, <https://www.shopify.com/legal/dpa> (citing CCPA); Shopify, *Privacy Policy*, (Updated March 2, 2023), <https://www.shopify.com/legal/privacy> (Citing CCPA); Shopify help center, *US state privacy laws*, <https://help.shopify.com/en/manual/privacy-and-security/privacy/us-state-privacy-laws> (citing CCPA).

California resident.” *Calder*, 465 U.S. at 788. Here, it even contained information identifying their residency, including their address, IP address, and other geolocation information. In this case, online profiling of individual California consumers is allegedly done for financial risk profiling. ER-109, ¶ 46. In others, it could be done for the purpose of online behavioral advertising.²⁴ This type of “individualized targeting” indicates that Shopify directly aimed its conduct into the forum. *See Myers*, 238 F.3d at 1074.

4. Extending Personal Jurisdiction Over Shopify Would Not Create Universal Jurisdiction For Online Platforms.

Exercising personal jurisdiction over Shopify here would not set a precedent effectively authorizing jurisdiction over all internet platforms everywhere. With regard to online publishers in suits based on their publication of content, the Court has held that a defendant is subject to specific jurisdiction where it has “both actively appealed to and profited from an audience” in the forum. *Will Co., Ltd. v. Lee*, 47 F.4th 917, 922–23 (9th Cir. 2022) (cleaned up); *see also Doe v. WebGroup Czech Republic, a.s.*, 93 F.4th 442, 453 (9th Cir. 2024) (quoting *Will Co.*, 47 F.4th at 922–23).²⁵

²⁴ *Meta, Retargeting starts with finding people who have engaged with your business*, <https://www.facebook.com/business/goals/retargeting>.

²⁵ Website operators can satisfy this test by: attempting to attract forum users by publishing content with a forum-specific focus or adopting technical measures that ensured a superior viewing experience in the forum than offered elsewhere; and

That framework for publishing activity is not always useful in data collection cases. Online data privacy cases often arise from data extraction allegedly performed *in the forum* through the internet. The defendant aims its business operations towards a forum when it extracts data from users that it knows are located in the forum, creates bespoke tools designed to facilitate data collection from forum residents, adopts policies designed to comply with unique requirements of a forum’s privacy regime, and creates individual profiles. Because these contacts arise from the *defendant’s* willful conduct in the relevant forum—not those of plaintiffs or third parties—specific jurisdiction is appropriate.

B. Briskin’s Privacy Claims “Arise Out Of Or Relate To” Shopify’s California Business Contacts Formed To Gain Access To Personal Data.

Contrary to the Panel’s holding, this lawsuit directly arises out of Shopify’s alleged business contacts in California, which gave it access to consumers’ personal data. In other words, a “direct nexus” exists between the two. *Yamashita v. LG Chem, Ltd.*, 62 F.4th 496, 504 (9th Cir. 2023) (quoting *In re W. States Wholesale Nat. Gas Antitrust Litig.*, 715 F.3d 716, 742 (9th Cir. 2013)).

There is a straightforward causal link: California merchants have California consumers; Shopify allegedly formed business relationships with California

adopting an advertising structure that intentionally exploited the forum market. *See, e.g., Will Co.*, 47 F.4th at 922–23 (citing *Mavrix Photo*, 647 F.3d at 1221–24, 1230–31); *Doe*, 93 F.4th at 454–56.

merchants, signed contracts, and created policies in order to gain access to those California consumers; Shopify then collected data from those California consumers; Shopify then created profiles about those California consumers using the data it collected. *See Supra* Section II.A.

Without Shopify's business relationships with merchants, Shopify's collection of personal data and the resulting harm could not exist. This is the type of "proof of causation" or relationship between Shopify's in-state activity and the litigation that the Supreme Court has articulated. *Ford Motor Co. v. Montana Eighth Jud. Dist. Ct.*, 592 U.S. 351, 362 (2021). The "whole point" of Shopify's alleged activities in the state, according to the Complaint, is to gain access to consumers' personal data. *Id.* at 374 (J. Alito, concurring) (describing "causal in a broad sense").

CONCLUSION

For the reasons stated above, this Court should hold that the U.S District Court for the Northern District of California has personal jurisdiction over the Defendant. The judgment of the district court should be reversed.

Dated: July 2, 2024

By: /s/ F. Mario Trujillo
F. Mario Trujillo
Victoria J. Noble
Corynne McSherry

ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Email: mario@eff.org
Telephone: (415) 436-9333
Fax: (415) 436-9993

*Counsel for Amicus Curiae
Electronic Frontier Foundation*

Seth E. Mermin
David S. Nahmias
UC Berkeley Center For
Consumer Law & Economic
Justice
305 Berkeley Law
Berkeley, CA 94720-7200
Email: tmermin@law.berkeley.edu
dnahmias@law.berkeley.edu
Telephone: (510) 643-3519

*Counsel for Amicus Curiae
UC Berkeley Center For
Consumer Law & Economic
Justice*

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g), I certify as follows:

1. This Brief of *Amici Curiae* Electronic Frontier Foundation and UC Berkeley Center For Consumer Law & Economic Justice in Support of Plaintiff-Appellant and Reversal with the type-volume limitation of Fed. R. App. P.

32(a)(7)(B) because this brief contains 3,462 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 365, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: July 2, 2024

By: /s/ F. Mario Trujillo
F. Mario Trujillo

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on July 2, 2024.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: July 2, 2024

By: /s/ F. Mario Trujillo
F. Mario Trujillo