

1 Laura Sullivan (Cal. Bar No. 220529)
2 LAW OFFICE OF LAURA SULLIVAN
3 423 South Estate Drive
4 Orange, CA 92869
5 Telephone: 714-744-15220
6 Email: laurasullivan@laurasullivanlaw.com

7 Jennifer Sarvadi (D.C. Bar. No. 490475)
8 (*pro hac vice application pending*)
9 HUDSON COOK, LLP
10 1909 K Street NW, 4th Floor
11 Washington, DC 20006
12 Telephone: 202-715-2002
13 Email: jsarvadi@hudco.com

14 *Attorneys for Proposed Amici,*
15 *Software & Information Industry Association and the*
16 *Coalition for Sensible Public Record Access*

17
18
19
20
21
22
23
24
25
26
27
28
**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION**

CAT BROOKS and RASHEED SHABAZZ,
individually and on behalf of all others
similarly situated,

Plaintiffs,

v.

THOMSON REUTERS CORPORATION,

Defendant.

Case No. 3:21-cv-01418-EMC

**AMICI CURIAE THE SOFTWARE &
INFORMATION INDUSTRY
ASSOCIATION AND THE COALITION
FOR SENSIBLE PUBLIC RECORDS
ACCESS' MOTION FOR LEAVE TO
FILE *AMICI CURIAE* BRIEF IN
SUPPORT OF DEFENDANT;
[PROPOSED] *AMICI CURIAE* BRIEF**

Judge: Hon. Edward M. Chen
Date: April 20, 2023
Time: 1:30 pm
Room: Courtroom 5, 17th Floor

The Software & Information Industry Association (“SIIA”) and Coalition for Sensible Public Records Access (“CSPRA”), together as putative *amici*, respectfully move for leave to file an amici curiae brief in support of Defendant Thomson Reuters Corporation’s Opposition to

1 Plaintiffs' Motion for Class Certification, and for grounds state:

2 1. SIIA is a trade association for those in the business of information that represents
3 approximately 600 member companies, among them publishers of software and information
4 products, including databases, enterprise and consumer software, and other products that combine
5 information with digital technology.
6

7 2. SIIA member companies serve nearly every segment of society, including business,
8 education, government, healthcare, and consumers. SIIA is dedicated to creating a healthy
9 environment for the creation, dissemination, and productive use of information.

10 3. SIIA has an interest in this matter and qualifications to assist this Court as it
11 considers Plaintiffs' motion because the availability of accurate public records is central to SIIA's
12 mission and many of its members rely on access to public records. Moreover, Plaintiffs' challenge
13 to the Defendant's business model has implications for other SIIA members and their businesses.
14

15 4. CSPRA is a non-profit organization dedicated to promoting the principle of open
16 public record access to ensure individuals, the press, advocates, and businesses the continued
17 freedom to collect and use the information made available in the public record for
18 personal, governmental, commercial, and societal benefit.

19 5. Members of CSPRA are among the many entities that comprise a vital link in the
20 flow of information for these purposes and provide services that are widely used by constituents in
21 every state. Collectively, CSPRA members alone employ over 75,000 persons across the U.S. The
22 economic and societal activity that relies on entities such as CSPRA members is valued in the
23 trillions of dollars and employs millions of people.
24

25 6. CSPRA has an interest in this matter and qualifications to assist this Court as it
26 considers Plaintiffs' motion because the availability of complete and accurate public records is
27 central to CSPRA's belief that the economy and society depend on value-added information and
28

1 services that include public record data for many important aspects of our daily lives, and to
2 CSPRA's work to protect those sensible uses of public records.

3 7. SIIA and CSPRA wish to be heard on this issue because consumers, law enforcement, and
4 a wide range of businesses rely on data that flows in and through Defendant's CLEAR product, and
5 other similar products, to function and fulfill their every-day obligations. The brief submitted by
6 SIIA and CSPRA will assist this Court in its understanding of the CLEAR product and the ways in
7 which open access to public records benefits virtually every facet of society.
8

9 8. SIIA and CSPRA have read the parties' briefs, and the attached amici brief is
10 necessary to fully and adequately address the issue of class certification.

11 Accordingly, SIIA and CSPRA request that they be granted permission to file the attached
12 amici brief.
13

14
15 Dated: February 2, 2023

Respectfully submitted,

16 /s/ Laura Sullivan
17

18 Laura Sullivan

19 *Attorney for Amici Curiae*
20 *The Software & Information Industry Association,*
21 *The Coalition for Sensible Public Records*
22
23
24
25
26
27
28

TABLE OF CONTENTS

STATEMENT OF INTEREST	1
SUMMARY OF THE ARGUMENT	2
ARGUMENT.....	4
I. VARYING BENEFITS TO THE PUBLIC THAT ARE UNSUITABLE FOR CLASSWIDE ADJUDICATION.....	4
II. THE COLLECTION AND SHARING OF PUBLICLY AVAILABLE INFORMATION IS PERMITTED UNDER A VARIETY OF FEDERAL AND STATE LAWS DEPENDING ON THE PARTICULAR CIRCUMSTANCES.....	8
A. The California Consumer Privacy Act Permits the Collection, Use, and Sharing of Public Domain Data.....	9
B. California Law Does Not Include the Right to Be Forgotten Nor Does it Require Consent Before Data Collection.....	11
C. The DPPA Preempts State Laws that Prevent Aggregators from Using Covered Data for Permitted Purposes.....	14
D. Data Aggregators Like Defendant Have a Constitutional Right to Collect, Maintain, and Sell This Information.....	15
III. THE PUTATIVE CLASS MEMBERS LACK STANDING.....	17
IV. CLASS MEMBERS’ CLAIMS CANNOT SATISFY THE COMMONALITY REQUIREMENTS NECESSARY FOR CLASS CERTIFICATION.....	19
V. CERTIFICATION OF A CLASS ON THIS NOVEL THEORY WILL HAVE DETRIMENTAL IMPACTS ON CALIFORNIA CONSUMERS.....	21
CONCLUSION.....	24

TABLE OF AUTHORITIES

Cases

<i>CBS, Inc. v. Block</i> , 42 Cal. 3d 646 P.2d 470 (1986)	5
<i>Farmer v. Phillips Agency, Inc.</i> , 285 F.R.D. 688 (N.D. Ga. 2012)	20
<i>Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzales</i> , 2014 E.C.R. 317	11
<i>Howard v. Criminal Info. Svc.</i> , p. 889	7, 14, 15
<i>Marcus v. BMW of N. Am., LLC</i> , 687 F.3d 583 (3d Cir. 2012)	19
<i>NASA v. Nelson</i> , 562 U.S. 134 (2011)	7
<i>Roth v. Guzman</i> , 650 F.3d 603 (6th Cir. 2011)	14, 15
<i>Seattle Times Co. v. Rhinehard</i> , 467 U.S. 20 (1984)	15
<i>Sorrell v. IMS Health Inc.</i> , 564 U.S. 552 (2011)	15, 16, 17
<i>Soutter v. Equifax Info. Servs., LLC</i> , 498 F. App'x 260 (4th Cir. 2012)	19
<i>State of Okl. ex rel. Oklahoma Dep't of Pub. Safety v. United States</i> , 161 F.3d 1266 (10th Cir. 1998)	15
<i>Taylor, et al., v. Axiom Corp., et al.</i> , 612 F.3d 325 (5 th Cir. 2010)	7, 14, 15, 22
<i>Trans Union, LLC v. Ramirez</i> , 141 S. Ct. 2190 (2021)	3, 18, 21
<i>U.S.W., Inc. v. F.C.C.</i> , 182 F.3d 1224 (10th Cir. 1999)	16
<i>Wal-Mart Stores, Inc. v. Dukes</i> , 564 U.S. 338 (2011)	19
<i>Ward v. Rock Against Racism</i> , 491 U.S. 781 (1989)	7, 16
<i>Zinser v. Accufix Rsch. Inst., Inc.</i> , 253 F.3d 1180 (9th Cir.)	20

Statutes

15 U.S.C. § 1681g	20
15 U.S.C. §§ 1681 <i>et seq.</i>	8, 22
18 U.S.C. § 2725	14
18 U.S.C. §§ 2721 <i>et seq.</i>	8, 10, 14, 22
Cal. Bus. & Prof. Code § 17204	17

1	Cal. Bus. & Prof. Code § 22581	16, 17
2	Cal. Civ. Code § 1798.105.....	16
3	Cal. Civ. Code § 1798.140.....	13, 14
4	Cal. Civ. Code § 1798.145.....	14, 15
5	Cal. Civ. Code § 7921.000.....	10
6	Cal. Civ. Code §§ 1798.100 <i>et seq.</i>	12
7	Cal. Gov. Code §§ 7920.000 <i>et seq.</i>	10
8	Cal. Penal Code § 11105.....	21

Other Authorities

11	Andrew J. Pincus, Miriam R. Nemetz, and Eugene Volokh, <i>Invalidity Under the First Amendment of the Restrictions on Dissemination of Accurate, Publicly Available Information Contained in the California Consumer Privacy Act of 2018</i> , https://fisd.net/wp-content/uploads/2021/06/Memo-re-CCPA-FINAL.pdf	12
14	Brooke Barnett, <i>Use of Public Record Databases in Newspaper and Television Newsrooms</i> , 53 Fed. Comm. L.J. 557 (2001).....	5
15	Comments of Gail H. Littlejohn, Vice President, Gov't Affairs, & Steven M. Emmert, Dir., Gov't Affairs, Reed Elsevier Inc., LEXIS-NEXIS Group (Mar. 31, 2000), <i>available at</i> http:// www.sec.gov/rules/proposed/s70600/littlej1.htm ; <i>see also Financial Information Privacy Act: Hearings on H.R. 4321 Before the H. Comm. on Banking and Financial Services</i> , 105th Cong. 100 (1998) (statement of Robert Glass).....	7
19	<i>Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations for Fiscal Year 2000: Hearings on H.R. 2670/S.1217 Before Subcomm. for the Dep'ts of Commerce, Justice, and State, the Judiciary, and Related Agencies of the S. Comm. on Appropriations</i> , 106th Cong. 280 (1999)	6
21	Gary E. Clayton, <i>The Public's Records: Open Access vs. Personal Privacy</i> . https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/the_publics_records.pdf	5
23	Grace Park, <i>The Changing Wind of Data Privacy Law: A Comparative Study of the European Union's General Data Protection Regulation and the 2018 California Consumer Privacy Act</i> , 10 UC Irvine L. Rev. 1455, 1479 (2020).....	11
25	Robert M. Jarvis, <i>John B. West: Founder of the West Publishing Company</i> , 50 Am. J. Legal Hist. 1 *5 (2010)	5

Rules

28	Federal Rule of Appellate Procedure 29	1
----	--	---

Regulations

Regulation 2016/679 (GDPR), Art. 17 12

Legislative Material

2018 Cal. Legis. Serv. Ch. 55 (A.B. 375)..... 13

1 The Software & Information Industry Association, together with the Coalition for Sensible
 2 Public Records Access (collectively, “*amici*”), respectfully submit this brief in support of
 3 Defendant’s Brief in Opposition to Plaintiffs’ Motion for Class Certification.¹

4 **STATEMENT OF INTEREST**

5 The Software & Information Industry Association (“SIIA”) is the principal trade association
 6 for those in the business of information. SIIA represents approximately 600 member companies,
 7 among them publishers of software and information products, including databases, enterprise and
 8 consumer software, and other products that combine information with digital technology. SIIA
 9 member companies serve nearly every segment of society, including business, education,
 10 government, healthcare, and consumers. It is dedicated to creating a healthy environment for the
 11 creation, dissemination, and productive use of information. Many of its members rely on access to
 12 public records.
 13

14 CSPRA is a non-profit organization dedicated to promoting the principle of open public
 15 record access to ensure individuals, the press, advocates, and businesses have the continued
 16 freedom to collect and use the information made available in the public record for
 17 personal, governmental, commercial, law enforcement, and societal benefit. Members of CSPRA
 18 are among the many entities that comprise a vital link in the flow of information for these purposes
 19 and provide services that are widely used by constituents in every state. Collectively, CSPRA
 20 members alone employ over 75,000 persons across the U.S. The economic and societal activity
 21 that relies on entities such as CSPRA members is valued in the trillions of dollars and employs
 22
 23
 24

25 ¹ Consistent with Federal Rule of Appellate Procedure 29(a)(2), *amici* represent that they requested
 26 Plaintiffs’ consent to the filing of this brief, but their consent was not obtained or refused. Further
 27 consistent with Federal Rule of Appellate Procedure 29(a)(4)(E), *amici* represent that no party or
 28 party’s counsel has authored this brief, in whole or in part, or contributed money intended to fund
 the preparation or submission of this brief. Further, no person other than *amici* and their non-party
 members contributed money that was intended to fund the preparation or submission of this brief.

1 millions of people. CSPRA has an interest in this case and qualifications to assist this Court
2 because the availability of complete and accurate public records is central to CSPRA's belief that
3 the economy and society depend on value-added information, and services that include public
4 record data for many important aspects of our daily lives, and to CSPRA's work to protect those
5 sensible uses of public records and the many public benefits that flow from their public and private
6 use.
7

8 In essence, Plaintiffs have lodged an attack on the core business activities of *amici's*
9 members which are data aggregators, like Defendant, who collect and share publicly available
10 information on consumers. While it is currently unclear as to exactly which activity/activities
11 Plaintiffs assert violate California law under this novel theory, what is clear is that a ruling in favor
12 of Plaintiffs could lead to disastrous results for government, businesses, and consumers alike.
13 *Amici* are uniquely qualified to assist this Court in understanding the larger data ecosystem of which
14 Defendant is a part, the comprehensive data privacy regime in which these products are offered for
15 sale, and the failure of the putative class members to establish standing, or demonstrate sufficient
16 commonality of putative plaintiffs and claims to satisfy Rule 23 class certification requirements.
17 *Amici* appreciate the opportunity to provide this information to the Court.
18

19 SUMMARY OF THE ARGUMENT

20 Class certification in this case is not appropriate because most of the information in products
21 like Defendant's is sourced from publicly available sources that provide huge benefits, not harms,
22 to California consumers and businesses alike. *Amici's* members publish information to public and
23 private entities to serve both commercial and public interests. California, while a leader in
24 consumer privacy, has specifically adopted laws to permit open access to public record information,
25 and in enacting the nation's first comprehensive data privacy law, carved out from its prohibitions
26 the very data used by *amici's* members in their products and services. The California General
27
28

1 Assembly, and Congress, have evaluated the degree to which such information may be accessed,
2 collected, and used, balancing the interests of consumer privacy against legitimate business and
3 public use cases, resulting in, among other laws, the California Consumer Protection Act/California
4 Privacy Rights Act, the California Sunshine Act, the federal Driver's Privacy Protection Act, the
5 Gramm-Leach Bliley Act, and the Fair Credit Reporting Act (hailed as the first federal consumer
6 privacy law).

7
8 As discussed below, each of these laws permit companies like the Defendant to collect, use,
9 and share publicly available information, and other information on consumers, without first
10 requiring the company to obtain the consumer's consent, and without compensating the consumer
11 for such use. Moreover, the fact that California has enacted this comprehensive data regulation
12 regime, and having considered whether to include a right to be forgotten by all persons who
13 maintain consumer data should be part of that scheme, evinces the fact that no such right exists in
14 the common law in California, and further, that California has weighed the risks and benefits of
15 such a right and decidedly rejected that one should exist.

16
17 As a result, to the extent that the information maintained by Defendant about consumers is
18 permitted to be collected and published without first obtaining consumer consent, and without
19 requiring remuneration to consumers, no class may be certified containing consumers on whom
20 such data is maintained as they have not been suffered concrete harm sufficient to confer Article
21 III standing to sue. Moreover, the Supreme Court in *Trans Union LLC v. Ramirez* has made clear
22 that standing requires that the information maintained both have a negative implication for or about
23 the consumer, but also must have been shared with a third party in order for the consumer to have
24 suffered any cognizable harm. The ensuing slog of mini-trials that would necessarily have to be
25 undertaken to parse the millions of data points and assess their redressability make class treatment
26
27
28

1 of these issues impracticable. Such mini-trials would not only overtake the larger matter but
 2 demonstrate why these consumers do not meet the commonality requirements of Rule 23.

3 Finally, *amici* urge this Court to consider the disastrous implications on consumers and
 4 business alike inflicted by a finding that consumers are entitled to monetary relief. Applications
 5 for housing and employment would come screeching to a halt, effectively delaying consumers'
 6 ability to find housing and jobs. Applications for mortgages would suddenly take far longer, and
 7 likely cost more, should every transaction require a personal trip by a title examiner to the
 8 courthouse to search for, and retrieve, relevant title records. And the courts and other state agencies
 9 might suffer the most, as every single potential user of public record information, department of
 10 motor vehicle records, professional and medical licensing boards, bar associations and others would
 11 experience a massive influx of researchers clamoring for attention, and likely, do not have sufficient
 12 resources to handle the flood. For all of these reasons, and those articulated by Defendant, *amici*
 13 respectfully request that this Court deny the Plaintiffs' Motion to Certify the Class in this case.
 14

15 ARGUMENT

16 **I. VARYING BENEFITS TO THE PUBLIC THAT ARE UNSUITABLE 17 FOR CLASSWIDE ADJUDICATION.**

18 Today, the United States runs on data. Americans' disparate daily lives are made better by
 19 timely and efficient access to varying information, whether accessed via their phone or home
 20 computer, or even through a physical newspaper. The U.S. economy depends on information made
 21 available by data aggregators in a variety of sectors. *Amici's* customers include both private sector
 22 and government clients, including arms of the state of California.
 23

24 This is the same data and information industry in which Defendant Thomson Reuters
 25 operates. That ecosystem has been in existence for decades, and *amici's* members play various
 26 roles within it: offering products that compete with Defendant's CLEAR product (the "Product" or
 27 "CLEAR"); offering technology platforms that connect data publishers to government and public
 28

1 interest users nationwide. Publishers in this industry collect information from sources similar—if
 2 not identical to—those described by Defendant, including government agencies who affirmatively
 3 share court and other records of the agency (the courts, departments of motor vehicles, departments
 4 of corrections, real property records, etc.), individuals who have made their content available
 5 voluntarily (whether online or otherwise), and other third-party sources.² While data sharing is
 6 now ubiquitous in the modern gig-economy, it has been commonplace for most of modern history.
 7 For example, courthouse records have been commercially collected and published for nearly 150
 8 years.³

10 Open access rights to public record information have been referred to as “a cornerstone of
 11 American democracy” and viewed as “central to electing and monitoring public officials,
 12 evaluating government operations, and protecting against secret government activities.”⁴ More
 13 specifically, “[t]he democratic process relies on open access to government records. An informed
 14 citizenry is crucial to a functioning democratic government, and access to information about the
 15 workings of the government is key to that process.”⁵ The Supreme Court of California has similarly
 16 recognized the inherent importance of open access to public records: “[i]mplicit in the democratic
 17 process is the notion that government should be accountable for its actions. In order to verify
 18 accountability, individuals must have access to government files. Such access permits checks
 19 against the arbitrary exercise of official power and secrecy in the political process.”⁶

23 ² See Defendant Thomson Reuter’s Opposition to Motion to Certify Class, pp. 2-3.

24 ³ See Robert M. Jarvis, *John B. West: Founder of the West Publishing Company*, 50 Am. J. Legal
 25 Hist. 1 *5 (2010).

26 ⁴ Gary E. Clayton, *The Public’s Records: Open Access vs. Personal Privacy*.
https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/the_publics_records.pdf.

27 ⁵ Brooke Barnett, *Use of Public Record Databases in Newspaper and Television Newsrooms*, 53
 Fed. Comm. L.J. 557, 558–59 (2001).

28 ⁶ *CBS, Inc. v. Block*, 42 Cal. 3d 646, 651, 725 P.2d 470, 473 (1986).

1 The California General Assembly (the “Legislature”) recognized the importance that open
 2 access to public records plays when it adopted the California Public Records Act.⁷ In so adopting
 3 the California Public Records Act, “the Legislature, mindful of the right of individuals to privacy,
 4 [found] and declar[ed] that access to information concerning the conduct of the people’s business
 5 is a fundamental and necessary right of every person in this state.”⁸ The Legislature thus recognized
 6 that the right of Californians to access public records outweighed Californians’ limited right to
 7 privacy, to the extent any exists with respect to public record information.

9 The real value in these data services, however, extends far beyond economic alone; they go
 10 to our core needs as a civilized, functioning society, and the benefits vary in numerous ways. Users
 11 of this information need timely and efficient access to this data for a variety of purposes, including,
 12 but not limited to:

- 14 • Law enforcement. Federal and local law enforcement agencies rely on the data
 15 contained in the Product, and other similar products, to locate suspects of
 16 criminal activity, as well as victims and witnesses to crimes. Agencies like the
 17 Federal Bureau of Investigation, rely on these types of products because they
 18 “[allow] FBI investigative personnel to perform searches from computer
 workstations and eliminates the need to perform more time consuming manual
 searches of federal, state, and local records systems, libraries, and other
 information sources.”⁹
- 19 • Fraud Prevention. Identity theft and other forms of fraud are a constant threat to
 20 consumers and businesses alike. Companies often leverage public record data
 21 to authenticate consumers in order to prevent identity theft and fraud. This can
 22 include an insurance company obtaining data from the DMV or a vendor
 23 reselling the same, in order to authenticate a consumer’s true identity and risks.
 This can also include asking “out of wallet” questions, which are those a
 fraudster would be unlikely to know, such as “Which of the following five
 addresses is a past home address of yours?” or “Which of the following cars did

24
 25 ⁷ Cal. Gov. Code §§ 7920.000 *et seq.*

26 ⁸ Cal. Civ. Code § 7921.000.

27 ⁹ *Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies*
Appropriations for Fiscal Year 2000: Hearings on H.R. 2670/S.1217 Before Subcomm. for the
Dep'ts of Commerce, Justice, and State, the Judiciary, and Related Agencies of the S. Comm. on
 28 *Appropriations*, 106th Cong. 280 (1999).

you once own?” The answers to these questions could be found in state real property records or publicly available Uniform Commercial Code filings.

- Child support enforcement. State and local agencies use data like that contained in the Product to locate individuals who are delinquent in paying their child support obligations. The Association for Children for Enforcement of Support reports that public record information provided through commercial vendors helped locate over 75 percent of the “deadbeat parents” they sought.¹⁰
- Credit extensions. Reliable and prompt access to public records like deeds and DMV records, are necessary to facilitate an active and competitive credit market, and to facilitate creditors’ securitization of collateral in support of such credit extensions.
- Insurance. Insurers of all shapes and sizes access such data each day to underwrite policies, and pay claims.
- Product Safety. Companies use this information to provide consumers and auto dealers with a vehicle’s accident history, alerting consumers to whether they are potentially buying a “lemon,” or to put both dealers and consumers on notice that the vehicle is subject to a safety recall.¹¹
- Tax Compliance. Governments use real estate records like those at issue in this case to detect tax avoidance.
- News-gathering and Publishing. Newspaper companies regularly obtain the Information used in these products to report on crimes, detect possible corruption or conflicts of interest, and publish stories involving the operation or safety of motor vehicles.¹²
- Employment and tenant screening. While this Product is not a consumer report itself, many consumer reporting agencies use public record data like that in the Product to prepare consumer reports for employment and tenant screening. The use of this information helps employers and others ensure a “competent, reliable workforce.”¹³

¹⁰ Comments of Gail H. Littlejohn, Vice President, Gov’t Affairs, & Steven M. Emmert, Dir., Gov’t Affairs, Reed Elsevier Inc., LEXIS-NEXIS Group (Mar. 31, 2000), *available at* <http://www.sec.gov/rules/proposed/s70600/littlej1.htm>; *see also Financial Information Privacy Act: Hearings on H.R. 4321 Before the H. Comm. on Banking and Financial Services*, 105th Cong. 100 (1998) (statement of Robert Glass).

¹¹ *See Taylor v. Acxiom Corp.*, 612 F.3d 325 (5th Cir. 2010).

¹² *See Howard v. Criminal Info. Svc.*, 654 F.3d 887, 889 (9th Cir. 2011).

¹³ *NASA v. Nelson*, 562 U.S. 134, 150 (2011).

1 Individuals, as well as government agencies and commercial enterprises, depend on timely
 2 access to this information, and its predictable transmission forms the backbone of billions of dollars
 3 in commerce and multiple important decisions in people’s everyday lives. For example, a parent
 4 searching for a private nanny may want to check state criminal records in the nanny’s prior home
 5 state to assure herself that the nanny is not a registered sex offender. She may also want to
 6 investigate whether a day care facility she is considering as an alternative has been cited for child
 7 safety violations. Prior to moving a parent into an assisted living facility, an adult child may want
 8 to examine the government-issued health and safety reports in different states. Timely access to
 9 this information helps consumers make informed decisions. Proclaiming a blanket prohibition
 10 against such use of data on a class-wide basis would be unjust and conceal the varying prosocial
 11 benefits of data sharing that can only be borne out by individual analysis of each data transaction.
 12

13
 14 **II. THE COLLECTION AND SHARING OF PUBLICLY AVAILABLE**
 15 **INFORMATION IS PERMITTED UNDER A VARIETY OF FEDERAL AND**
 16 **STATE LAWS DEPENDING ON THE PARTICULAR CIRCUMSTANCES.**

17 California has exhaustively regulated activity around the use of information, first through a
 18 comprehensive process in enacting the California Consumer Privacy Act,¹⁴ and then via ballot
 19 initiative in the California Privacy Rights Act.¹⁵ These laws also take into account (as they must),
 20 the federal Drivers Privacy Protection Act¹⁶ and the Fair Credit Reporting Act,¹⁷ among others.
 21 Each of these laws reflects a careful balancing of consumers’ right to privacy against the needs of
 22 third parties to access and use public information. Many State legislatures and Congress have
 23 undertaken the responsibility of reconciling those competing interests, creating laws to regulate the
 24

25 ¹⁴ Cal. Civ. Code §§ 1798.100 *et seq.* (the “Privacy Act”).

26 ¹⁵ California Privacy Rights Act of 2020 (modifying California’s data protection law) (the
 “CRPA”).

27 ¹⁶ 18 U.S.C. §§ 2721 *et seq.* (the “DPPA”).

28 ¹⁷ 15 U.S.C. §§ 1681 *et seq.*

1 data in such a way as each has seen fit (supported by constituents who elected their representatives
 2 based on such efforts). This exhaustive regulation not only dooms the Plaintiffs' claims, it makes
 3 certification of a class impossible, as determining whether the business practices of Defendant
 4 comply with these varied laws on a class-wide basis would be inappropriate.

5
 6 A. The California Consumer Privacy Act Permits the Collection, Use, and Sharing of Public Domain Data.

7 In 2020, via Proposition 24, Californians adopted the CPRA, which expanded the Privacy
 8 Act, and is sometimes referred to as "CCPA 2.0."¹⁸ In the face of this comprehensive statutory
 9 regime, Plaintiffs' novel theory that a company may only collect, maintain, and/or share the
 10 information used in the Product with the consumer's prior express consent or are somehow required
 11 to compensate individuals, must fail, and a class should not be certified.

12
 13 The CCPA does not regulate the collection and sharing of information obtained from third
 14 parties; instead, it regulates the maintenance and sharing of information collected directly from
 15 consumers by restricting the sharing (including sale) of "personal information," which is defined
 16 to include information "that identifies, relates to, describes, is reasonably capable of being
 17 associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or
 18 household."¹⁹ There is a wealth of data collected, sold, and shared by data providers that are not
 19 "personal information" under the CCPA.²⁰ Importantly, "personal information" does not include:

21 publicly available information or lawfully obtained, truthful information that
 22 is a matter of public concern. For purposes of this paragraph, "publicly
 23 available" means: information that is lawfully made available from federal,
state, or local government records, or information that a business has a
 24 reasonable basis to believe is lawfully made available to the general public by
the consumer or from widely distributed media; or information made

25
 26 ¹⁸ The CCPA and the CPRA are collectively referred to herein as the "CCPA."

27 ¹⁹ Cal. Civ. Code § 1798.140(v)(1).

28 ²⁰ See Cal. Civ. Code § 1798.140(v)(1).

1 available by a person to whom the consumer has disclosed the information if
 2 the consumer has not restricted the information to a specific audience.²¹

3 As detailed below, much of the information that flows into products like CLEAR are obtained
 4 directly from federal, state, and local government records, and/or are those which companies have
 5 a reasonable basis to believe is lawfully made available to the general public by the consumer or
 6 from widely distributed media (such as a traditional white pages telephone directory). As a result,
 7 that data is not subject to CCPA.

8 The Legislature also expressly exempted information regulated by several federal statutes
 9 that might otherwise meet the definition of personal information. For example, furnished
 10 information provided to a consumer reporting agency (“CRA”) is exempt from the CCPA
 11 requirements.²² The statute also does not apply to “personal information collected, processed, sold,
 12 or disclosed” pursuant to the Gramm-Leach Bliley Act,²³ and, for the most part, “personal
 13 information collected, processed, sold, or disclosed pursuant to the Driver’s Privacy Protection
 14 Act.”²⁴ These three exemptions, plus the exclusion from the definition, cover much of the
 15 information used in the Product, and similar products offered by, and used by, *amici*’s members
 16 and express a legislative intent that transmission of such information be exempt from ad hoc
 17 interference. The exemption of certain classes of information dovetails with the manner in which
 18 California’ legislature tailored consumer rights, including do-not-sell and deletion.
 19
 20

21 _____
 22 ²¹ Cal. Civ. Code § 1798.140(v)(2) (emphasis added).

23 ²² Cal. Civ. Code § 1798.145(d)(1) (“activity involving the collection, maintenance, disclosure,
 24 sale, communication, or use of any personal information bearing on a consumer's creditworthiness,
 25 credit standing, credit capacity, character, general reputation, personal characteristics, or mode of
 living by a consumer reporting agency,... by a furnisher of information ... who provides
 information for use in a consumer report, ... and by a user of a consumer report.”) (referred to as
 “FCRA Purposes”).

26 ²³ Cal. Civ. Code § 1798.145(e) (referred to as “GLB Purposes”).

27 ²⁴ Cal. Civ. Code § 1798.145(f) (“This title shall not apply to personal information collected,
 28 processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 ([18 U.S.C.](#)
[Sec. 2721 et seq.](#)). This subdivision shall not apply to [Section 1798.150.](#)”) (referred to as “DPPA
 Purposes”).

1 B. California Law Does Not Include the Right to Be Forgotten Nor Does it Require
 2 Consent Before Data Collection.

3 The definitions and exemptions above are key to the question of class certification because
 4 the novel theory presented by Plaintiffs here presumes a right exists under the common law that
 5 consumers must first grant permission to the collection, maintenance, or use of publicly available
 6 data, and/or are entitled to compensation for its collection, maintenance, or use.²⁵ The work of the
 7 Legislature in enacting the CCPA debunks the myth that these rights exist under the common law.

8 Plaintiffs implicitly argue that they have a general “right to be forgotten” under California
 9 law, a concept espoused in a 2014 European Court of Justice case – *Google Spain SL v. AEPD and*
 10 *Cotaja Conzales*.²⁶ “Simply put, the core provision of the right to be forgotten is that ‘if an
 11 individual no longer wants his personal data to be processed or stored by a data controller, and if
 12 there is no legitimate reason for keeping it, the data should be removed from their system.’”²⁷
 13 However, California law does not universally grant Californians a “right to be forgotten.” Where
 14 the Legislature has chosen to give such a right, it has enacted specific laws to grant such a right.²⁸
 15
 16

17 ²⁵ It is entirely unclear which business practice, precisely, Plaintiffs challenge as unlawful. In the
 18 First Amended Complaint, Plaintiffs ask questions such as “Does Thomson Reuters seek the class
 19 members’ consent or compensate them before making their personal information available for sale
 20 through CLEAR?” First Amended Complaint paragraph 77(a). This question raises more questions
 21 then it answers as to the nature of the alleged unfair practice. Is it the act of collecting the data at
 22 all that is an alleged violation? Is it the failure to obtain consent prior to collecting the information,
 23 or prior to “making the data available for sale,” or both? Is the fact that the data is maintained in a
 24 database that is “made available for sale” enough to impart liability, or does the data have to have
 25 actually been shared for a claim to exist? The claims are not well pled, and such vagueness concerns
 26 *amici’s* members given their possible engagement in one or more of such practices.

27 ²⁶ See generally Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*
 28 (*AEPD*) and *Mario Costeja Gonzales*, 2014 E.C.R. 317.

²⁷ Grace Park, *The Changing Wind of Data Privacy Law: A Comparative Study of the European Union’s General Data Protection Regulation and the 2018 California Consumer Privacy Act*, 10 UC Irvine L. Rev. 1455, 1479 (2020).

²⁸ See e.g., Cal. Bus. & Prof. Code § 22581 (which permits California minors to “request and obtain removal of, content or information posted on the operator’s Internet Web site, online service, online application, or mobile application by the user” regardless of its source). In contrast, the CCPA gives California consumers a “right to deletion” but only of non-exempt personal information “which the business has collected *from* the consumer.” Cal. Civ. Code § 1798.105(a) (emphasis added).

1 In fact, the drafters of the CCPA considered a broader-sweeping privacy rule, initially
 2 modeling the first version of CCPA after the European GDPR, which confers a right to be
 3 forgotten.²⁹ The GDPR grants data subjects the right to obtain “erasure of personal data concerning
 4 him or her without undue delay,” including where the personal data is no longer necessary for the
 5 purposes for which it was collected or processed, where the data subject has withdrawn consent for
 6 data processing, and where the personal data has been unlawfully processed.³⁰ California flatly
 7 rejected this approach, instead choosing only to grant consumers the right to request deletion of
 8 certain types of data collected directly from the consumer.³¹ These changes to the legislation were
 9 made not just because of the policy benefits, but also to comply with the demands of the First
 10 Amendment.³²

12 In any event, if the common law already conferred a right on consumers to require erasure
 13 of information that data aggregators like Defendant maintains, California would not have had to
 14 consider legislation expressly granting that right (or the right of a minor to demand information
 15 about them be removed,³³ etc.).

17
18
19 ²⁹ Regulation 2016/679 (GDPR), Art. 17(1).

20 ³⁰ *Id.*

21 ³¹ Cal. Civ. Code § 1798.105(a).

22 ³² Andrew J. Pincus, Miriam R. Nemetz, and Eugene Volokh, *Invalidity Under the First*
 23 *Amendment of the Restrictions on Dissemination of Accurate, Publicly Available Information*
 24 *Contained in the California Consumer Privacy Act of 2018*, [https://fisd.net/wp-](https://fisd.net/wp-content/uploads/2021/06/Memo-re-CCPA-FINAL.pdf)
 25 [content/uploads/2021/06/Memo-re-CCPA-FINAL.pdf](https://fisd.net/wp-content/uploads/2021/06/Memo-re-CCPA-FINAL.pdf).

26 ³³ See Cal. Bus. & Prof. Code § 22581 (“An operator of an Internet Web site, online service, online
 27 application, or mobile application directed to minors or an operator of an Internet Web site, online
 28 service, online application, or mobile application that has actual knowledge that a minor is using
 its Internet Web site, online service, online application, or mobile application shall do all of the
 following: (1) Permit a minor who is a registered user of the operator's Internet Web site, online
 service, online application, or mobile application to remove or, if the operator prefers, to request
 and obtain removal of, content or information posted on the operator's Internet Web site, online
 service, online application, or mobile application by the user.”).

1 California law is thereby unambiguous, and evinces zero legislative intent to proscribe or
 2 regulate the collection, maintenance, sharing, or use of information, other than personal
 3 information; or the collection, maintenance, sharing, and/or use of personal information for GLB
 4 Purposes, DPPA Purposes and FCRA Purposes; or impose a requirement that any business engaged
 5 in the use of such information or for such purposes first obtain consumer's consent before doing
 6 so. No personal right of publicity can exist in public data as it is not owned or controlled by the
 7 subject of the data but is in fact, owned and controlled by the public and managed by their elected
 8 and appointed representatives and made available according to public records laws of California.
 9 To say one can restrict the use of public data because they have not been compensated or consented
 10 presents a wholly incongruous misrepresentation of the very idea of public records and applicable
 11 law.
 12

13
 14 In the face of this comprehensive approach to protecting consumers' right to privacy and
 15 the right to control information, as amended by a vote of the citizens of California, there can be no
 16 claim related to activities that are intentionally permitted by carve-out from the CCPA, including
 17 the sale of services like the Product.³⁴ For the purpose of considering class certification, therefore,
 18 this Court will be required to examine the data at issue for each consumer and determine whether
 19 the collection and sharing of such information is expressly permitted by exemption, and over which
 20 the consumer lacks any right to demand deletion. In such cases, there can be no harm, and thus no
 21 standing, for which relief could be granted, and class certification would be inappropriate.
 22

23
 24 ³⁴ The Legislature could have, but did not, prohibit the collection, maintenance or sale of data as
 25 challenged in the First Amended Complaint, even though one of the primary purposes of the CCPA
 26 was to grant citizens "more control over their information." CALIFORNIA CONSUMER
 27 PRIVACY ACT, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375). The Legislature stated "California
 28 consumers should be able to exercise control over their personal information, and they want to be
 certain that there are safeguards against misuse of their personal information. It is possible for
 businesses both to respect consumers' privacy and provide a high-level transparency to their
 business practices." *Id.*

1 C. The DPPA Preempts State Laws that Prevent Aggregators from Using Covered Data
 2 for Permitted Purposes.

3 Fraud prevention tools, data verification, and other services, like the Product, often include
 4 information sourced from driver license records, access to which is regulated by the federal DPPA.
 5 Plaintiffs’ objection to the collection and resale of data regulated by the DPPA must fail, as the
 6 DPPA expressly contemplates that resellers such as Defendant may obtain, aggregate, and resell
 7 DPPA data.³⁵

8 Moreover, a series of cases raising legal challenges to data aggregators’ and individual
 9 companies’ rights to obtain, aggregate, and sometimes resell motor vehicle drivers’ “personal
 10 information” as defined by the DPPA³⁶ have all failed in this Circuit, as well as the Fifth and Sixth
 11 Circuits.³⁷ In *Howard*, the plaintiffs alleged that the defendants, which included a newspaper, a
 12 parking lot manager, and a consumer reporting agency, violated the DPPA by purchasing the data
 13 in bulk and “stockpiling” it for a future use.³⁸ Similarly, the plaintiffs in *Taylor* sought a declaration
 14 that the defendant users, including CRAs, utility companies, insurance companies, retailers,
 15 publishers, and auto dealers, among others, were prohibited from obtaining the DPPA information
 16 in bulk - whether they intended to use the information itself at a later date, or they intended to resell
 17 the information to third parties.³⁹ In each of these cases, the circuit courts found that the users did
 18
 19
 20
 21
 22

23 ³⁵ See 18 U.S.C. § 2721(c).

24 ³⁶ “Personal information” under the DPPA includes individuals’ “name, address, telephone number,
 25 vehicle description, Social Security number, medical information, and photograph.” 18 U.S.C. §
 2725.

26 ³⁷ *Howard v. Criminal Info. Svc.*, 654 F.3d 887 (9th Cir. 2011); *Taylor*, 612 F.3d 325 (5th Cir. 2010);
 27 and *Roth v. Guzman*, 650 F.3d 603 (6th Cir. 2011), respectively.

28 ³⁸ 654 F.3d at 889.

³⁹ 612 F.3d at 334.

1 not violate the DPPA's permissible purpose requirements by obtaining the data in bulk for future
2 use – whether internal or external.⁴⁰

3 To the extent the DPPA preempts state laws that are inconsistent with the DPPA's rules
4 regarding disclosure of this information,⁴¹ no state law claim may lie against Defendant, or any
5 other data provider, who aggregates and resells DPPA "personal information" for a purpose
6 permitted by the DPPA. Thus, any claim based on the collection and sharing of information
7 regulated by the DPPA would fail, unless Thomson Reuters is proven to have shared the
8 information with a third party who did not have a permitted purpose under the DPPA.
9

10 D. Data Aggregators Like Defendant Have a Constitutional Right to Collect, Maintain,
11 and Sell This Information.

12 The valuable public service performed by the Defendant's CLEAR database and similar
13 kinds of information services are not a happy accident, but the direct result of constitutional design.
14 Data aggregators have a right to access and use public record information and to communicate that
15 information to third parties under the First Amendment. The Supreme Court has held that the "right
16 to speak is implicated when information [one] possesses is subjected to restraints on the way in
17 which the information might be used or disseminated."⁴² Thus, data companies that collect and
18 maintain publicly available data have the right to communicate that information to third parties.
19 Absent some law requiring them to obtain consent prior to doing so, which does not exist, the
20 companies are not acting in violation of the law.
21

22 In *Sorrell*, a case which the Court did not cite in its earlier decision denying plaintiff's
23 motion to dismiss, Vermont attempted to limit the sharing and use of certain medical prescriber
24

25 ⁴⁰ *Taylor*, 612 F.3d at 340; *Howard* 654 F. 3d at 891; and *Roth*, 650 F.3d at 617-18.

26 ⁴¹ *State of Okl. ex rel. Oklahoma Dep't of Pub. Safety v. United States*, 161 F.3d 1266, 1269 (10th
27 Cir. 1998).

28 ⁴² *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 568 (2011) (quoting *Seattle Times Co. v. Rhinehard*,
467 U.S. 20, 32 (1984)).

1 information for marketing purposes (unless the prescriber first consented to the sharing).⁴³ The
 2 information was permitted to be shared and sold so long as it was not for a marketing purpose.⁴⁴
 3 The Supreme Court found that “[on] its face, Vermont’s law enacts content-and-speaker-based
 4 restrictions on the sale, disclosure and use of” the information, explaining that the “statute thus
 5 disfavors marketing, that is, speech with a particular content. More than that, the statute disfavors
 6 specific speakers, namely pharmaceutical manufacturers.”⁴⁵ The state defended the law on the
 7 basis that it was designed to promote public health interest, and to lower the costs of medical
 8 services.⁴⁶ However, the Supreme Court held that the law did “not advance [those goals] in a
 9 permissible way.” The Court explained:

11 The State seeks to achieve its policy objectives through the indirect means of
 12 restraining certain speech by certain speakers—that is, by diminishing detailers’
 13 ability to influence prescription decisions. **Those who seek to censor or burden**
 14 **free expression often assert that disfavored speech has adverse effects.** But the
 15 “fear that people would make bad decisions if given truthful information” cannot
 16 justify content-based burdens on speech.⁴⁷

17 Importantly here, the Supreme Court reiterated that the “First Amendment requires
 18 heightened scrutiny whenever the government creates ‘a regulation of speech because of
 19 disagreement with the message it conveys.’”⁴⁸ A general assertion of a right to privacy will not
 20 support heightened scrutiny’s requirement of an important interest, much less a compelling one.⁴⁹
 21 The Plaintiffs’ objections here are even broader: their objections are not limited to drug marketing
 22 (or even marketing at all), but to *any* commercial use of public domain information in public

23

 24 ⁴³ *Sorrell*, 564 U.S. at 558-559.

25 ⁴⁴ *Id.*

26 ⁴⁵ *Id.* at 563-564.

27 ⁴⁶ *Id.* at 576.

28 ⁴⁷ *Id.* at 577 (emphasis added) (citations omitted).

⁴⁸ *Id.* at 565, quoting *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989).

⁴⁹ *U.S.W., Inc. v. F.C.C.*, 182 F.3d 1224, 1235 (10th Cir. 1999).

1 records, social media, and elsewhere, including for purposes of child support, law enforcement,
 2 loan securitization, or investigative journalism. Plaintiff's cause of action cannot be tailored to any
 3 relevant state interest because the states sells the very same information to the same types of users
 4 and for the very same purposes that amici members' customers intend to make of the data.⁵⁰
 5 Allowing plaintiffs to proceed under California's Unfair Competition law against a private party
 6 where the state engages in the exact same conduct would amount to content-based and user-based
 7 restrictions on commercial speech in violation of *Sorrell*. Certification of such a class against this
 8 backdrop is impossible.

10 III. THE PUTATIVE CLASS MEMBERS LACK STANDING.

11 As explained above, myriad federal and state laws expressly regulate the kind of
 12 information that is included in the Product and permit that data to be sold without first obtaining
 13 the consumer's consent or without compensation. Thus, the putative class members have suffered
 14 no cognizable harm and lack standing to sue.

15 California's Unfair Competition Law limits standing in a section 17200 action to certain
 16 specified public officials and to "any person who has suffered injury in fact and has lost money or
 17 property as a result of ... unfair competition." Cal. Bus. & Prof. Code § 17204. Assuming, without
 18 admitting, that the named Plaintiffs here meet the "public officials" standard, the vast majority of
 19 consumers located in California whom Plaintiffs intend to bring in as class members would not.
 20
 21
 22
 23

24
 25 ⁵⁰ In fact, in California, this very same public record information must be aggregated by the local
 26 agencies that maintain the original records (i.e., the clerks of the court) who must then share that
 27 information with the California Department of Justice, which maintains and organizes the data for
 28 the sole purpose of selling reports on consumers in California. *See* Cal. Penal Code § 11105. These
 reports may be accessed by a number of persons as permitted by law, including certain state
 agencies, law enforcement officers, and other specifically identified persons. *Id.* There is nothing
per se untoward in the collection of such information, let alone illegal.

1 As a result, these individuals must be able to establish that they have suffered an injury in fact and
 2 lost money or property as a result of Defendant's sale of data.

3 Plaintiffs would be unable to show harm to the putative class members. Again, Plaintiffs
 4 cite no authority for the proposition that they are entitled to compensation for the collection and
 5 sharing of information available in the public domain. The CCPA does not require it. The DPPA
 6 does not require it. Nor does any law of which *amici* are aware. Thus, these individuals cannot
 7 have "lost" money to which they were never entitled.
 8

9 Moreover, the Supreme Court's analysis in an FCRA case sheds light on the question of
 10 putative class members' standing under Article III.⁵¹ In *Ramirez*, the Supreme Court considered
 11 whether putative class members had standing to sue under the FCRA where the sole basis for the
 12 claim was that the CRA maintained information in a database about them, but had not shared it
 13 with any third party.⁵² The Supreme Court held that consumers failed to show concrete harm
 14 required to confer Article III standing where the CRA maintained (presumably misleading and/or
 15 defamatory information)⁵³ but did not share the information with third parties. The Supreme Court
 16 likened the issue to one of defamation, and explained:
 17

18 The mere presence of an inaccuracy in an internal credit file, if it is not disclosed to
 19 a third party, causes no concrete harm. In cases such as these where allegedly
 20 inaccurate or misleading information sits in a company database, the plaintiffs' harm
 21 is roughly the same, legally speaking, as if someone wrote a defamatory letter and
 22 then stored it in her desk drawer. A letter that is not sent does not harm anyone, no
 23 matter how insulting the letter is. So too here.⁵⁴

23 ⁵¹ *Trans Union, LLC v. Ramirez*, 141 S. Ct. 2190 (2021).

24 ⁵² For the purpose of the standing analysis, the Supreme Court assumed that the CRA "violated its
 25 obligations under the Fair Credit Reporting Act to use reasonable procedures in internally
 26 maintaining the credit files." *Id.* at 2208.

26 ⁵³ The parties had stipulated, for the purpose of the case, that defendant had violated the law in
 27 including potential "OFAC" alerts, which signaled that the consumer's name was identified on a
 28 list that included, among others, potential terrorists. *Id.* at 2221, fn 5. The Supreme Court expressly
 took no position with regard to that claim. *Id.* at 2221, fn 5.

⁵⁴ *Id.* at 2210.

1 The fact that the FCRA provides for statutory damages did not, standing alone, satisfy the concrete
 2 harm requirement sufficient for standing to exist.⁵⁵ Something more was required.

3 Similarly, here, without some showing that an individual suffered concrete harm from the
 4 dissemination of information that would cause the consumer to be viewed in a negative light, the
 5 putative class members lack standing. As explained below, the exercise necessary to evaluate the
 6 nature of the information shared, to whom it was shared, and whether it would be viewed in such a
 7 way as to be defamatory or misleading, would overtake the entirety of the case, making class
 8 certification improper.
 9

10 **IV. CLASS MEMBERS' CLAIMS CANNOT SATISFY THE**
 11 **COMMONALITY REQUIREMENTS NECESSARY FOR CLASS**
 12 **CERTIFICATION.**

13 *Amici* agree with Defendant that there are a myriad of issues that this Court would be
 14 required to resolve to ensure that the class members' claims are sufficiently common so that the
 15 relief accorded would appropriately remedy the harm suffered by each member. Respectfully, the
 16 series of mini-trials that would ensue demonstrate why class treatment is inappropriate here.

17 “Commonality requires the plaintiff to demonstrate that the class members “have suffered
 18 the same injury.””⁵⁶ It is well-settled law that “if class members are impossible to identify without
 19 extensive and individualized fact-finding or ‘mini-trials,’ then a class action is inappropriate.”
 20 *Marcus v. BMW of N. Am., LLC*, 687 F.3d 583, 593 (3d Cir. 2012). As described above, the data
 21 used in such products combine “public record” data (criminal records, driver’s license data, etc.),
 22

23 _____
 24 ⁵⁵ *Id.* at 2205 (citations omitted) (“this Court has rejected the proposition that “a plaintiff
 25 automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory
 26 right and purports to authorize that person to sue to vindicate that right.” As the Court emphasized
 27 in *Spokeo*, “Article III standing requires a concrete injury even in the context of a statutory
 28 violation.”). Moreover, where statutory damages are available, an individualized inquiry of class
 members’ harms is required. *See Soutter v. Equifax Info. Servs., LLC*, 498 F. App’x 260, 265 (4th
 Cir. 2012) (reversing class certification where the representative plaintiff’s claims were only
 “typical” only on an “unacceptably general level.”).

⁵⁶ *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 349–50 (2011) (citation omitted).

1 as well as other data made available voluntarily by consumers to third parties through public means
 2 (i.e., social media platforms such as Facebook®, SnapChat®, etc.). Focusing on the front-end
 3 collection and maintenance of data, as to each consumer, one must consider the type of data, and
 4 its source, to determine if the collection and/or maintenance is unlawful (i.e., “unfair”). If the data
 5 is publicly available data (i.e., such as the results of a Google ® search, or a court lookup service
 6 available online), there can be no claim, and that consumer would not properly be part of a class.
 7 Next, the court would have to consider if Defendant has an affirmative right under the law to collect,
 8 maintain, and share that data (such as with the DPPA, FCRA, GLBA, CCPA, etc.). Further, class
 9 resolution of such claims is not superior where, as here “each class member has to litigate numerous
 10 and substantial separate issues to establish his or her right to recover individually.”⁵⁷

12 Given the complexity of this level of review, it is not surprising that other courts have held
 13 that similar putative class claims were not appropriate for class treatment. Under the FCRA, for
 14 example, consumers are entitled to a copy of their file from a consumer reporting agency (e.g., a
 15 credit bureau) and the CRA must include the source of certain kinds of information in that file
 16 disclosure.⁵⁸ In declining to certify a class of potential consumers who allegedly did not receive a
 17 complete file disclosure, given the “broad range” of the CRA’s data sources, the court trial
 18 explained:

20 the court would need to determine the source of each piece of adverse information
 21 in a consumer’s report and then evaluate the quality of that source. This will
 22 necessarily entail individualized inquiry for many reports, even if some of the record
 23 sources may be common to many potential class members and thus susceptible to
 24 class-wide proof.⁵⁹

25 ⁵⁷ *Zinser v. Accufix Rsch. Inst., Inc.*, 253 F.3d 1180, 1192 (9th Cir.), *opinion amended on denial of*
 26 *reh’g*, 273 F.3d 1266 (9th Cir. 2001).

26 ⁵⁸ 15 U.S.C. § 1681g(a).

27 ⁵⁹ *Farmer v. Phillips Agency, Inc.*, 285 F.R.D. 688, 703 (N.D. Ga. 2012) (where the district court
 28 denied certification under Rule 23(b)(3) because these issues predominated over any issues
 common to the class, but the point remains).

1 For the same reasons many of the putative class members lack Article III standing, namely,
 2 lack of any concrete injury resulting from the fact that their information has not be shared with third
 3 parties *and* caused some harm as a result, so too would their claims not be common to other
 4 members of the class. If the data were not shared with a third party, under the rationale in *Ramirez*,
 5 the consumer did not suffer a cognizable injury, and would not properly be members of a class.

6 Even if some data about a consumer had been shared, the Court would next have to consider
 7 the nature of the data, and the purpose for which it was shared in order to ascertain if the sharing
 8 caused harm. Consider the parent whose cell phone data was shared so that their child could be
 9 found safe by law enforcement. Certainly, the parent would not claim that they were injured by
 10 such use. Next, consider the parent who is severely behind in child support payments who is located
 11 by the state upon retrieval of their current address information (whether obtained via a copy of the
 12 white pages or a report provided by a data aggregator). While the parent forced to pay their legal
 13 obligation may object, the state's interests are actually vindicated by such sharing in that the
 14 individual can be forced to pay and relive the state of its burden to provide support for the child.
 15 Further, the parents and children benefitting from child support recovery and enforcement are
 16 themselves a class who would see actual injury in loss of support funds if the plaintiffs succeed in
 17 creating a class and restricting the use of the Product for this purpose. Under such facts, the debtor
 18 could hardly be said to have been harmed under the law.

19 The putative class, as proposed, is therefore impermissibly vague, overly inclusive, and fails
 20 to account for any of these factors. The Court's time would be utterly consumed by examination of
 21 the factors in each type of scenario. In short, class treatment would be practically impossible.

22 **V. CERTIFICATION OF A CLASS ON THIS NOVEL THEORY WILL**
 23 **HAVE DETRIMENTAL IMPACTS ON CALIFORNIA CONSUMERS.**

24 To the extent that Plaintiffs' novel theory essentially boils down to the following
 25 premise – the business practice of collecting and/or maintaining, and/or sharing publicly available
 26
 27
 28

1 information for profit is a violation of California law – such a rule would have devastating
 2 consequences for California consumers. Setting aside the fact that this business model has been in
 3 existence for nearly 150 years, facilitated by the efforts of federal and state government agencies
 4 alike, and subject to regulation by state and local legislators for at least the past 50 years,⁶⁰ and
 5 California legislators more recently, a ruling finding these business practices to be unlawful would
 6 bring businesses across California, and beyond, to a halt.

8 As the Ninth Circuit observed in *Taylor*, the consequences of a rule that information
 9 expressly permitted to be collected and shared may not in fact be collected and shared, would have
 10 severe consequences and lead to “absurd results”:

11 At a checkout line at a grocery store or similar establishment, when a customer
 12 wishes to pay by (or cash) a check, and presents a driver's license as identification,
 13 it is obviously wholly impractical to require the merchant for each such customer to
 14 submit a separate individual request to the state motor vehicle department to verify
 15 the accuracy of the personal information submitted by the customer, under section
 2721(b)(3). Any such process would obviously take way too long to be of any use
 16 to either the customer or the merchant, and would moreover flood the state
 department with more requests than it could possibly handle.⁶¹

17 The real-life consequences of such a ruling are far more extreme than mere delays at the grocery
 18 store checkout line:

- 19 • Significant delays would be likely in the processing of applications for insurance
 20 and other financial services, because consumer identities may not be able to be
 authenticated or application information verified;
- 21 • Law enforcement efforts would be hindered, delaying or preventing officers
 22 from locating suspects, or locating missing persons, and other victims of crimes;

25 ⁶⁰ The FCRA was enacted in 1970. 15 U.S.C. §§ 1681 *et seq.* Again, the Product itself is not a
 26 consumer report, and is therefore not subject to the FCRA; however, it is viewed as the nation’s
 first privacy law.

27 ⁶¹ *Taylor*, 612 F.3d at 337. Instead, the Ninth Circuit explained, “the merchant buys the state
 28 department's entire data base and from it extracts on that occasion that particular customer's
 information, and later performs the same task as to the next such customer in the line.” *Id.*

- 1 • The state would be unable to locate persons who fail to pay child support, or
- 2 who are engaged in tax fraud, causing the State to incur more expenses over
- 3 time;
- 4 • Consumers could be unable to quickly and easily obtain employment because
- 5 their background checks would not be able to be completed and consumers
- 6 would remain out of work, and unable to secure housing; and
- 7 • Consumers and businesses alike would have no defense against sophisticated
- 8 fraudsters and other bad actors whose actions would go undetected were
- 9 products like CLEAR be banned from industry.

10 In sum, Plaintiffs seek to create new standards, effectively outlawing certain business
11 practices that the California Legislature had every opportunity to prohibit, but chose not to. If there
12 are to be enhanced privacy rights in California that might reach providers like Defendant, it is the
13 job of the Legislature to create them. This Court should deny Plaintiffs' Motion for Class
14 Certification.

CONCLUSION

For the foregoing reasons, *amici* the Software & Information Industry Association and the Coalition for Sensible Public Records Access respectfully request that this Court deny Plaintiffs' Motion for Class Certification.

Dated: February 2, 2023

Respectfully submitted,

/s/ Laura Sullivan

Laura Sullivan (Cal. Bar No. 220529)
LAW OFFICE OF LAURA SULLIVAN
423 South Estate Drive
Orange, CA 92869
Telephone: (714) 744-1522
Email: laurasullivan@laurasullivanlaw.com

Jennifer L. Sarvadi
Hudson Cook, LLP
1909 K Street, N.W., Suite 400
Washington, D.C. 20006
(202) 715-2002
jsarvadi@hudco.com
Motion for Admission Pro Hac Vice pending

Attorneys for Amicus Curiae
The Software & Information Industry Association,
The Coalition for Sensible Public Records Access