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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Dated: February 2, 2023

Respectfully submitted,

/s/ Laura Sullivan

Laura Sullivan

Attorney for Amici Curiae
The Software & Information Industry Association,
The Coalition for Sensible Public Records

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

Regulations

Legislative Material

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

STATEMENT OF INTEREST

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

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

[1] Consistent with Federal Rule of Appellate Procedure 29(a)(2), *amici* represent that they requested Plaintiffs' consent to the filing of this brief, but their consent was not obtained or refused. Further consistent with Federal Rule of Appellate Procedure 29(a)(4)(E), *amici* represent that no party or 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.

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

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

SUMMARY OF THE ARGUMENT

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

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

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

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

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

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

ARGUMENT

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

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

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

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

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

---

[2] *See* Defendant Thomson Reuter's Opposition to Motion to Certify Class, pp. 2-3.

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

[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.

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

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

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

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

- Law enforcement. Federal and local law enforcement agencies rely on the data contained in the Product, and other similar products, to locate suspects of criminal activity, as well as victims and witnesses to crimes. Agencies like the Federal Bureau of Investigation, rely on these types of products because they "[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]

- Fraud Prevention. Identity theft and other forms of fraud are a constant threat to consumers and businesses alike. Companies often leverage public record data to authenticate consumers in order to prevent identity theft and fraud. This can include an insurance company obtaining data from the DMV or a vendor 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

[7] Cal. Gov. Code §§ 7920.000 *et seq.*

[8] Cal. Civ. Code § 7921.000.

[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 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).

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

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

California has exhaustively regulated activity around the use of information, first through a comprehensive process in enacting the California Consumer Privacy Act,[14] and then via ballot initiative in the California Privacy Rights Act.[15] These laws also take into account (as they must), the federal Drivers Privacy Protection Act[16] and the Fair Credit Reporting Act,[17] among others. Each of these laws reflects a careful balancing of consumers' right to privacy against the needs of third parties to access and use public information. Many State legislatures and Congress have undertaken the responsibility of reconciling those competing interests, creating laws to regulate the

[14] Cal. Civ. Code §§ 1798.100 *et seq.* (the "Privacy Act").

[15] California Privacy Rights Act of 2020 (modifying California's data protection law) (the "CRPA").

[16] 18 U.S.C. §§ 2721 *et seq.* (the "DPPA").

[17] 15 U.S.C. §§ 1681 *et seq.*

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

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

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

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

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

[18] The CCPA and the CPRA are collectively referred to herein as the "CCPA."

[19] Cal. Civ. Code § 1798.140(v)(1).

[20] *See* Cal. Civ. Code § 1798.140(v)(1).

> available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.[21]

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

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

---

[21] Cal. Civ. Code § 1798.140(v)(2) (emphasis added).

[22] Cal. Civ. Code § 1798.145(d)(1) ("activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's creditworthiness, 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").

[23] Cal. Civ. Code § 1798.145(e) (referred to as "GLB Purposes").

[24] Cal. Civ. Code § 1798.145(f) ("This title shall not apply to personal information collected, 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").

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

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

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

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

[26] *See generally* Case C-131/12, *Google Spain SL v. Agencia Española de Protecciòn de Datos (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).

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

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

---

[29] Regulation 2016/679 (GDPR), Art. 17(1).

[30] *Id.*

[31] Cal. Civ. Code § 1798.105(a).

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

[33] *See* Cal. Bus. & Prof. Code § 22581("An operator of an Internet Web site, online service, online application, or mobile application directed to minors or an operator of an Internet Web site, online 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.").

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

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

[34] The Legislature could have, but did not, prohibit the collection, maintenance or sale of data as challenged in the First Amended Complaint, even though one of the primary purposes of the CCPA was to grant citizens "more control over their information." CALIFORNIA CONSUMER PRIVACY ACT, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375). The Legislature stated "California 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.*

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

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

Moreover, a series of cases raising legal challenges to data aggregators' and individual companies' rights to obtain, aggregate, and sometimes resell motor vehicle drivers' "personal information" as defined by the DPPA[36] have all failed in this Circuit, as well as the Fifth and Sixth Circuits.[37] In *Howard*, the plaintiffs alleged that the defendants, which included a newspaper, a parking lot manager, and a consumer reporting agency, violated the DPPA by purchasing the data in bulk and "stockpiling" it for a future use.[38] Similarly, the plaintiffs in *Taylor* sought a declaration that the defendant users, including CRAs, utility companies, insurance companies, retailers, publishers, and auto dealers, among others, were prohibited from obtaining the DPPA information in bulk - whether they intended to use the information itself at a later date, or they intended to resell the information to third parties.[39] In each of these cases, the circuit courts found that the users did

[35] *See* 18 U.S.C. § 2721(c).

[36] "Personal information" under the DPPA includes individuals' "name, address, telephone number, vehicle description, Social Security number, medical information, and photograph." 18 U.S.C. § 2725.

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

[38] 654 F.3d at 889.

[39] 612 F.3d at 334.

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

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

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

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

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

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

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

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

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

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

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

---

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

[44] *Id*.

[45] *Id.* at 563-564.

[46] *Id.* at 576.

[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).

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

III. THE PUTATIVE CLASS MEMBERS LACK STANDING.

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

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

[50] In fact, in California, this very same public record information must be aggregated by the local agencies that maintain the original records (i.e., the clerks of the court) who must then share that information with the California Department of Justice, which maintains and organizes the data for 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.

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

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

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

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

---

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

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

[53] The parties had stipulated, for the purpose of the case, that defendant had violated the law in including potential "OFAC" alerts, which signaled that the consumer's name was identified on a 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.

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

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

IV. CLASS MEMBERS' CLAIMS CANNOT SATISFY THE COMMONALITY REQUIREMENTS NECESSARY FOR CLASS CERTIFICATION.

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

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

[55] *Id.* at 2205 (citations omitted) ("this Court has rejected the proposition that "a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right." As the Court emphasized in *Spokeo*, "Article III standing requires a concrete injury even in the context of a statutory 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).

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

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

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

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

[58] 15 U.S.C. § 1681g(a).

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

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

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

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

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

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

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

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

> At a checkout line at a grocery store or similar establishment, when a customer wishes to pay by (or cash) a check, and presents a driver's license as identification, it is obviously wholly impractical to require the merchant for each such customer to submit a separate individual request to the state motor vehicle department to verify 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 to either the customer or the merchant, and would moreover flood the state department with more requests than it could possibly handle. [61]

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

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

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

[61] *Taylor*, 612 F.3d at 337. Instead, the Ninth Circuit explained, "the merchant buys the state 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.*

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

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