No. 23-2969

United States Court of Appeals for the Ninth Circuit

NETCHOICE, LLC,

Plaintiff-Appellee,

v.

ROB BONTA, IN HIS OFFICIAL CAPACITY AS ATTORNEY GENERAL OF THE STATE OF CALIFORNIA,

Defendant-Appellant.

On Appeal from the United States District Court
for the Northern District of California
No. 5:22-cv-08861-BLF
The Honorable Beth Labson Freeman, Judge

BRIEF OF THE INSTITUTE FOR LAW, INNOVATION & TECHNOLOGY AS *AMICUS CURIAE* IN SUPPORT OF NEITHER PARTY

John Paul Schnapper-Casteras
Counsel of Record
Rachael Yocum
SCHNAPPER-CASTERAS PLLC
1717 K Street NW, Suite 900
Washington, D.C. 20006
(202) 630-3644
jpsc@schnappercasteras.com

Attorneys for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, counsel for *amicus* certify the following:

Amicus do not have a parent corporation and no publicly held corporation owns 10% or more of their stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

—

INTEREST OF *AMICUS CURIAE*[1]

The Institute for Law, Innovation & Technology (iLIT) is a collaborative technology hub at the Temple University Beasley School of Law. The mission of iLIT is to inform new approaches to technological innovation in the public interest, to bridge academic and practical boundaries, and to promote equity and advancement for underrepresented minorities in technology fields. iLIT provides students educational and professional opportunities at the intersection of technology and society. Additionally, iLIT partners with industry, government, and civil society, including Temple University's Center for Compliance and Ethics and the Institute for International Law and Public Policy. Specifically, iLIT has provided formal comments to the National Institute of Standards and Technology as well as public guidance and commentary on a range of issues, including public interest technology, international cybernorms, and human rights in the context of digital surveillance.

iLIT offers its technical expertise in this case because it implicates a widely used and flexible regulatory tool that is useful for companies, public institutions, consumers, and members of the public. Moreover, the case could have far-reaching

[1] This brief is submitted with the consent of all parties. Pursuant to F.R.A.P. 29(a)(4)(E) and Local Rule 29.1, counsel for *amicus* affirm that this brief was not authored by any party's counsel in whole or in part. The Tech Justice Law Project plans to contribute money that is intended to fund preparing or submitting the brief.

implications for state, national, and international practices involving data protection and technology regulation.

SUMMARY OF THE ARGUMENT

A central component of the California Age-Appropriate Design Code Act (CAADCA) is a risk management requirement known as a Data Protection Impact Assessment (DPIA), which is undertaken by companies with respect to certain data management practices and design features. A DPIA functions as a foundation for demonstrating compliance with data privacy requirements and as a standardized risk management tool for data controllers.

The district court decision below held that CAADCA was unconstitutional on several grounds, including because DPIAs involve commercial speech and cannot withstand the applicable level of First Amendment scrutiny. Specifically, the district court reasoned that the DPIA requirement did not directly advance the government's substantial interest in mitigating risks posed to children by the design of digital products, services, and features. Consequently, the district court ruled that DPIAs were not severable from the CAADCA, and issued a preliminary injunction for the entirety of the statute.

Amicus weigh in to demystify and describe DPIAs, which are increasingly common across the United States and abroad. The district court impliedly treated

DPIAs as an unusual form of commercial speech which impose rare burdens and necessitate a level of scrutiny which is strict in theory, and fatal in fact. But this fundamentally misunderstands what DPIAs entail, how they are used, where they originated, when they are necessary – and the central fact that they are widespread and commonly used.

In reality, DPIAs are first and foremost a straightforward and flexible way of analyzing the features and risks of certain technical products and the data processing they entail. They typically involve a half dozen analytic steps. The analysis is not necessarily long or burdensome, and in many instances, constitutes a commonsense way to understand a company's own product before it collects or uses large volumes of sensitive data. In the context of consumer products, DPIAs are typically kept on file internally (within a company), and yield benefits for how a product is designed and how data is collected, stored, and used. This, in turn, can help improve customer's user experience and their trust of the company. California's DPIA provision is similarly flexible and straightforward. Although CAADCA is focused on child protection, DPIAs are not unique to that context.

Second, DPIA requirements are increasingly commonplace – both across the United States and abroad. Today 23 states – nearly half the country – either require DPIAs as part of existing state law (11 states) or are poised to require them as part

of pending legislation (at least 12 states). Similar DPIA provisions have already been routinely applied by scores of American companies spanning a wide variety of industries and use cases. In the European Union, since 2018, DPIA requirements have been applied across a continent of hundreds of millions of users – including by large U.S. businesses – without creating serious implementation problems or leading to wider technological calamity. Legally, DPIA requirements have normally been treated as uncontroversial risk management requirements. For good reason: the government has historically required technical assessments and risk mitigation in many circumstances (e.g., airplane and automobile safety), which have not generated an outcry about unconstitutionality.

Third, DPIAs trace their origins to federal privacy law from the 1970s onwards, which emerged amid increased computerized records across government and industry. Notably, the Privacy Act of 1974 and the E-Government Act of 2002 set out similar requirements for federal agencies developing new systems of records and data processes that may impact data privacy. For the last 20 years, large federal agencies have regularly conducted privacy impact assessments, which are similar to DPIAs. These requirements help to ensure that federal agencies consider appropriately tailored data collection and processing tied to the purposes for which such records are created and maintained. DPIAs are not an entirely novel or foreign creation, contrary to how they are sometimes misperceived.

Ultimately, *amicus* take no position on district court's remedy or treatment of CAADCA provisions other than the DPIA, and do not file in support of either Appellant or Appellee. However, that the district court took a notably broad view of commercial speech (as opposed to conduct) and determined that essentially all aspects of CAADCA were facially unconstitutional (and practically futile). For the sake of doctrinal integrity alone, this Court may choose to revise, remand, or reign in aspects of the decision below. But under all circumstances, *amicus* respectfully urges the Court to carefully consider what DPIAs actually are – and where and how they are used. Categorically invalidating a state law with potentially national and international implications should, at the very least, be premised on an accurate and nuanced understanding of this important and widely used technical tool.

ARGUMENT

I. DATA PROTECTION IMPACT ASSESSMENTS ARE FLEXIBLE AND STRAIGHTFORWARD.

A Data Protection Impact Assent (DPIA) is a common risk management requirement that generally applies to large companies using sensitive consumer data. The overall purpose of DPIAs is to understand and manage risks of deploying digital products or services and processing personal data. *See* Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for*

the purposes of Regulation 2016/679 at 4 (adopted Apr. 4, 2017; revised Oct. 4, 2017) (hereinafter "Article 29 Working Party"), https://ec.europa.eu/newsroom/article29/items/
611236 at 4 ("DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them."). *Accord* International Association of Privacy Professionals (IAPP), *Data Protection Impact Assessment* (last accessed Dec. 17, 2023), https://iapp.org/resources/article/data-protection-impact-assessment-2/ (defining DPIA as the "process by which companies can systematically assess and identify the privacy and data protection impacts of any products they offer and services they provide," enabling "them to identify the impact and take the appropriate actions to prevent or, at the very least, minimise the risk of those impacts."). The purpose of DPIA is also in line with U.S. federal law and the basic principles of data privacy laws in other jurisdictions, namely Fair Information Practices (FIPS) (sometimes called Fair Information Practice Principles (FIPPS)) and the Privacy Act of 1974 which embody foundational principles of risk management and data privacy. *See generally* FPC.gov, *Fair Information Practice Principles (FIPPs)*,

https://www.fpc.gov/resources/fipps/ (last accessed Dec. 17, 2023); *infra* § III (discussing history of Privacy Act).

DPIAs are straightforward and significant. They "are designed to be a flexible and scalable tool that you can apply to a wide range of sectors and projects. Conducting a DPIA does not have to be complex or time-consuming in every case, but there must be a level of rigour in proportion to the privacy risks arising." Information Commissioner's Office, *What is a DPIA?* (last accessed Dec. 17, 2023), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/what-is-a-dpia/. *Accord* Information Commissioner's Office, *How do we do a DPIA?* (last accessed Dec. 17, 2023), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how1 ("You can also scale the time and resources needed for a DPIA to fit the nature of the project. It does not need to be a time-consuming process in every case.").

Within this flexible framework, standardized templates and best practices have emerged. *See e.g.*, IAPP, *Data Protection and Privacy Impact Assessments Topic Page*, *supra* (collecting templates). Companies regularly benchmark how they perform DPIAs against one another and treat these assessments as an

increasingly important part of risk management and product design. *See, e.g.*, International Association of Privacy Professionals et al., *Measuring Privacy Operations 2019* at 10 (2019), https://iapp.org/media/pdf/resource_center/measuring_privacy_operations_2019.pdf; Centre for Information Policy Leadership, *Global Readiness Benchmarks for GDPR*, https://cdn.avepoint.com/pdfs/en/Infographic/GDPR_benchmark_report_infographic.pdf (last accessed Dec. 18, 2023); "Privacy impact assessments and data protection impact assessments are valuable tools to gauge the ways projects, systems, programs, products or services impact the data an organization holds . . . ." International Association of Privacy Professionals, *Data Protection and Privacy Impact Assessments Topic Page* (last accessed Dec. 17, 2023), https://iapp.org/resources/topics/privacy-impact-assessment-2/.

In many jurisdictions, "[t]here is no formal method to conducting a DPIA, which should give organizations comfort in delivering templates that work best for their needs as long as it meets the primary goal of demonstrating that you have thoroughly considered any risks (including legal, corporate, civil and reputational) and taken actions to mitigate those risks." Adam Schlosser, *The increasing importance of a DPIA*, International Association of Privacy Professionals (Aug. 18, 2020), https://iapp.org/news/a/the-increasing-importance-of-a-dpia/.

Typically, a DPIA involves a half-dozen analytical steps, including:

> Step 1: identify the need for a DPIA
> Step 2: describe the processing [e.g., map information flows]
> Step 3: consider consultation [including with key stakeholders]
> Step 4: assess necessity and proportionality
> Step 5: identify and assess risks
> Step 6: identify measures to mitigate the risks
> Step 7: sign off and record outcomes

Information Commissioner's Office, *How do we do a DPIA?*, *supra*. Companies flexibly "design a [DPIA] process that fits with [its] existing approach to managing risks and projects, as long as it contains these key elements." *Id. See also id.* (detailing each of the seven steps for a typical assessment).

In the European Union, a landmark framework called the General Data Protection Regulation was adopted in 2016 and took effect in 2018, and includes a DPIA requirement. Under this provision, a basic assessment should include:

> (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
>
> (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
>
> (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
>
> (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned . . . .

GDPR Article 35(7). This provision is expanded upon by GDPR Recital 84, *Risk Evaluation and Impact Assessment*: "In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk." *Available at* https://gdpr-info.eu/recitals/no-84/. *See also* European Commission, *When is a Data Protection Impact Assessment (DPIA) required?* (last accessed Dec. 17, 2023), https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_en.

A common concern for companies is knowing when a DPIA is required. Authoritative guidance exists on this question to help advise decisionmakers, which generally focuses on factors that would increase the risks associated with specific data processing operations — for example, processing operations involving the use of highly sensitive information like biometrics or information related to young children (without parental consent). The precise grounds for triggering a DPIA can vary by jurisdiction. For example, in the United Kingdom, a

DPIA is required in various circumstances, including if a company decides to: "process genetic data," "track individuals' location or behaviour," "profile children or target marketing or online services at them," or "process data that might endanger the individual's physical health or safety in the event of a security breach," Information Commissioner's Office, *Data protection impact assessments* (last accessed Dec. 17, 2023), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-impact-assessments/. *See also* IAPP, *What Triggers a Data Impact Protection Assessment* (last accessed Dec. 17, 2023), https://iapp.org/media/pdf/resource_center/WhatTriggersDPIA_Final.pdf. *See also* Article 29 Working Party, *supra* at 9-12 (outlining approximately nine criteria that trigger a DPIA under the GDPR if two or more factors are present, including the use of sensitive personal data (e.g., biometrics) or data on vulnerable categories such as children).

DPIAs yield various benefits for companies, governmental institutions, consumers, and members of the public.

> In general, consistent use of DPIAs increases the awareness of privacy and data protection issues within your organisation. It also ensures that all relevant staff involved in designing projects think about privacy at the early stages and adopt a 'data protection by design' approach.

> A DPIA also brings broader compliance benefits, as it can be an effective way to assess and demonstrate your compliance with all data protection principles and obligations.
>
> However, DPIAs are not just a compliance exercise. An effective DPIA allows you to identify and fix problems at an early stage, bringing broader benefits for both individuals and your organisation.
>
> It can reassure individuals that you are protecting their interests and have reduced any negative impact on them as much as you can. In some cases the consultation process for a DPIA gives them a chance to have some say in the way their information is used. Conducting and publishing a DPIA can also improve transparency and make it easier for individuals to understand how and why you are using their information.
>
> In turn, this can create potential benefits for your reputation and relationships with individuals. Conducting a DPIA can help you to build trust and engagement with the people using your services, and improve your understanding of their needs, concerns and expectations.
>
> There can also be financial benefits. Identifying a problem early on generally means a simpler and less costly solution, as well as avoiding potential reputational damage later on. A DPIA can also reduce the ongoing costs of a project by minimising the amount of information you collect where possible, and devising more straightforward processes for staff.

Information Commissioner's Office, *What is a DPIA*, *supra.*

Often DPIAs are kept on file internally by a company and periodically updated or conducted anew in light of new data, new technology, or security breaches. *Id*. Sometimes, DPIAs are submitted to (or requested by) government officials, for example, in service of investigations or legal compliance. *See e.g.*, Information Commissioner's Office, *Data protection impact assessments* (last accessed Dec. 17, 2023),

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-impact-assessments/ ("You don't need to send every DPIA to the ICO and we expect the percentage sent to us to be small. But you must consult the ICO if your DPIA identifies a high risk and you cannot take measures to reduce that risk. . . . ."). In Europe, courts and regulators have occasionally imposed orders and enforcement actions – including against government agencies themselves – for failure to conduct DPIAs or failure to appropriately mitigate risks.[2]

---

[2] *See, e.g.*, *R. (on the application of Bridges) v. Chief Constable of South Wales Police* [2020] EWCA Civ 1058 (citing paragraph 155); Conseil d'Etat, No. 406122 (May 10, 2017), https://www.asylumlawdatabase.eu/en/case-law/france-council-state-conseil-d%E2%80%99%C3%A9tat-10th-may-2017-no-406122; Information Commissioner's Office, *ICO find Metropolitan Police Service's Gang Matrix breached data protection laws* (Nov. 16 2018), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-finds-metropolitan-police-service-s-gangs-matrix-breached-data-protection-laws/; ICO, *Royal Free – Google DeepMind trial failed to comply with data protection law* (July 3, 2017), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/; Information Commissioner's Office, *Royal Free NHS Foundation Trust update*, *July 2019* (July 31, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/royal-free-nhs-foundation-trust-update-july-2019/; Datatilsynet, *Administrative fine imposed on Municipality of Oslo, the Education Agency* (June 2, 2020; updated Sept. 8, 2020), https://www.datatilsynet.no/en/regulations-and-tools/regulations/avgjorelser-fra-dat

Viewed in this broader context, California's DPIA requirements are similarly flexible and straightforward. *See generally* CAADCA §1798.99.31(a)(1) (DPIAs are required for covered business for certain services offered to children);§1798.99.31(a)(1)(A)–(B) (DPIA must address purpose of service, use of data, and risks to children); 1798.99.31(a)(1)(B)(i)–(iv) (DPIA must address design and certain impacts on children); §1798.99.31(a)(1)(B)(v)–(vii) (DPIA must address other algorithms, design features, and data uses that could harm children); §1798.99.31(a)(2) (DPIA must create risk mitigation plan); §1798.99.31(a)(1)(A) (DPIAs must be periodically reviewed); §1798.99.31(a)(4)(B) (DPIAs are internal); §1798.99.31(a)(3) (California Attorney General has authority to request a list of DPIAs); §1798.99.31(a)(4) (California Attorney General has authority to request specific DPIA). Moreover, the CAADCA envisions the formation of a working group that would further advise the California legislature about operationalizing the statute (including DPIA implementation), §1798.99.32, although the facial challenge at bar did not allow that process to unfold. In sum, "DPIAs are nothing new for any company that has kept an eye on the CCPA/CPRA or its European cousin, the GDPR. They're a central element in the CAADCA as well, so businesses should become well-versed in carrying out DPIAs." Osano,

---

atilsynet/2019/administrative-fine-imposed-on-the-municipality-of-oslo-the-education-agency/.

What is the California Age-Appropriate Design Code Act (CAADCA)?, JD Supra (Mar. 14, 2023), https://www.jdsupra.com/legalnews/what-is-the-california-age-appropriate-7756671/.

II. DATA PROTECTION IMPACT ASSESSMENTS ARE WIDELY USED AND LEGALLY UNCONTROVERSIAL.

California's DPIA requirements fit comfortably within the mainstream of other states and major industrial nations, which require DPIAs in a wide and growing number of circumstances and jurisdictions. Since 2020, in the wake of the General Data Protection Regulation established in the EU, there has been a growing wave of U.S. states enacting generally applicable laws (i.e., not industry-specific) governing the privacy of personal information. To date, at least 23 states (including California) feature highly comparable DPIA requirements in current state consumer protection laws (11 states) and in pending consumer protection legislation (at least 12 states). This Court should be aware that nearly half the country is requiring or contemplating requiring DPIAs to protect consumer privacy before rendering any decision and that there is considerable substantive overlap with CAADCA.

All of the eleven state consumer protection laws that have materially similar DPIA requirements to the CAADCA provide that "[a] controller shall conduct and

document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer," Colorado Privacy Rights Act ("CPA"), § 6-1-1309(1) (emphasis added). *See also* California Consumer Privacy Act ("CCPA"), as amended by the California Privacy Rights Act, Cal. Civ. Code § 1798.185(15); Connecticut Data Privacy Act ("CTDPA"), Conn. Gen. Stat. §42-522(a); Florida Digital Bill of Rights ("FDBR"), Fla. St. 501.713(1); Fla. SB 262 (2023) (creating Fla. St. 501.713); Indiana Consumer Data Protection Act ("ICDPA"), Ind. Code § 24-15-6-1(b); Oregon Consumer Privacy Act ("OCPA"), SB 619-B Section 8(1)(a) (signed into law July 19, 2023); Montana Consumer Data Privacy Act ("MCDPA"), SB 0384, Section 9(1) (signed into law May 19, 2023); Tennessee Information Protection Act ("TIPA"), Tenn. Code Ann. § 47-18-3206(a); Texas Data Privacy and Security Act ("T1DPSA"), Tex. Bus. & Com. Code § 541.101(a); Virginia Consumer Data Protection Act **("**VCDPA"), § 59.1-80(a); Delaware Personal Data Privacy Act ("DPDPA"), Del. Code. tit. 6, §12D-109(a) (adding that DPIAs should be done "on a regular basis").

Five of these state laws provide an essentially identical list of processing activities that present a heightened risk of harm to a consumer, and, therefore, require a DPIA:

(1) the processing personal data for the purposes of targeted advertising;
(2) the sale of personal data;

> (3) the processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of:
>
> > (a) unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
> >
> > (b) financial, physical, or reputational injury to consumers;
> >
> > (c) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or
> >
> > (d) other substantial injury to consumers;
>
> (4) the processing of sensitive data; and
>
> (5) any processing activities involving personal data that present a heightened risk of harm to a consumer.

CPA, § 6-1-1309(2). *See also* CTDPA, Conn. Gen. Stat. §42-522(a); DPDPA, Del. Code. tit. 6, §12D-109(a); MCDPA, SB 0384, Section 9(1); OCPA, SB 619-B Section 8(1). The other six state laws include "processing activities that present a heightened risk of harm to consumers" as an additional category that requires conducting a DPIA. *See e.g.*, CCPA, Cal. Civ. Code § 1798.185(15); FDBR, Fla. St. 501.713(1); ICDPA, Ind. Code § 24-15-6-1(b); TIPA, Tenn. Code Ann. § 47-18-3206(a); T1DPSA, Tex. Bus. & VCDPA, § 59.1-80(A).

Further, ten of the existing state consumer protection laws provide that the required DPIAs:

> must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that the controller can employ to reduce the risks. The controller shall factor into this assessment

> the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

CPA § 6-1-1309(3). *See also* CTDPA, Conn. Gen. Stat. §42-522(b); DPDPA, Del. Code. tit. 6, §12D-109(b); FDBR, Fla. St. 501.713(2); ICDPA, Ind. Code § 24-15-6-1(c); MCDPA, SB 0384, Section 9(2); OCPA, SB 619-B Section 8(2); TIPA, Tenn. Code Ann. § 47-18-3206(b); T1DPSA, Tex. Bus. & Com. Code § 541.101(b); VCDPA, § 59.1-80(B). Similarly, California's Consumer Privacy Act, as amended by the California Privacy Rights Act, provides that a DPIA must "identify[ ] and weigh [ ] the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public." Cal. Civ. Code § 1798.185(15)(B).

In addition, like the CAADCA (Cal. Code § 1798.99.30(c)(1)), nine of these broad state consumer protection laws provide that "[i]f a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment shall be deemed to satisfy the requirements established in this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would

otherwise be conducted pursuant to this section." CTDPA § 42-522(e). *See* DPDPA, Del. Code. tit. 6, §12D-109(e); Fla. St. 501.713(5); ICDPA, Ind. Code § 24-15-6-1(e); MCDPA, SB 0384, Section 9(5); OCPA, SB 619-B Section 8(4); TIPA, Tenn. Code Ann. § 47-18-3206(e); T1DPSA, Tex. Bus. & Com. Code § 541.101(e); VCDPA, § 59.1-80(E).

Finally, all of these broad state consumer protection laws, like the CAADCA (Cal. Code § 1798.99.31(a)(3)), which requires that DPIA reports must be provided to the California Attorney General upon request, indicate that the required DPIAs be provided to their respective attorney general. Most of these state laws require that a DPIA be provided to the Attorney General upon request, and that the Attorney General may evaluate the DPIA for compliance with the law. *See* CPA § 6-1-1309(4); CTDPA § 42-522(c); Fla. St. 501.713 and 501.72; MCDPA, SB 0384, Section 9(3)(b); OCPA, SB 619-B Section 8(6) (and requiring that all DPIAs be retained for "at least five years" (*id.* at 8(3)). *See also* CCPA, Cal Code § 1798.185(15)(B) (DPIAs must be submitted to "the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information"). The other state consumer protection laws provide that the attorney general may request DPIAs by a civil investigative demand. *See* ICDPA, Ind. Code § 24-15-6-2; TIPA, Tenn. Code Ann. § 47-18-3206(c); T1DPSA, Tex. Bus. & Com. Code § 541.101(f); VCDPA, § 59.1-80(C).

In addition to the eleven states that have already enacted broad consumer data protection acts with comparable DPIA requirements to that of the CAADCA, at least twelve (12) other states have pending consumer protection legislation with materially similar DPIA requirements and government oversight mechanisms.[3]

Similarly, the European Union has applied DPIA requirements far and wide for the last five years. These applications of the DPIA (as part of the GDPR) span 27 countries, comprising 448 million people, over $15 trillion in gross domestic product. *See* European Union, *Facts and figures on life in the European Union* (last

[3] Hawaii Consumer Data Protection Act, HB No. 1497 (introduced Jan. 20, 2023); Illinois Data Privacy and Protection Act, HB 3385 (introduced Feb. 17, 2023); Louisiana Consumer Privacy Act, Senate Bill No. 199 (introduced Aug. 1, 2023); Maine Consumer Privacy Act, LD1973 (introduced in May 2023); Maine Data Privacy and Protection Act, LD1977 (introduced in May 2023); Massachusetts Data Privacy Protection Act, S.25 (based on the American Privacy Protection Act, introduced Jan. 18 & 19, 2023); Massachusetts Information Privacy and Security Act, S.227 (introduced Jan. 20, 2023); Massachusetts Internet Bill of Rights, H.1555 (closely tracks the GDPR, introduced Jan. 20, 2023); Michigan Personal Data Privacy Act**,** Senate Bill 1182 (introduced Sept. 27, 2022); Minnesota House Bill Concerning Data Privacy, H.F. No. 2309 (introduced March 15, 2023); New Hampshire Bill Relative to the Expectation of Privacy, SB255 (introduced Jan. 19, 2023); New Jersey Disclosure and Accountability Transparency Act, Assembly Bill A505 (introduced on Jan. 11, 2022); New York Child Data Privacy and Protection Act, Assembly Bill A-4967 (introduced Feb. 27, 2023); New York Data Protection Act, Assembly Bill No. A-7423a (introduced May 19, 2023); New York Privacy Act, Assembly Bill A-2587 (introduced Feb. 3, 2023); Pennsylvania Consumer Data Protection Act, House Bill 708 (introduced Mar. 27, 2023); Rhode Island Data Transparency And Privacy Protection Act, S0754 (introduced on March 23, 2023); Rhode Island Personal Data and Online Privacy and Protection Act**,** H5745 (introduced on March 2, 2023). One such piece of legislation tracks the CAADCA, the Minnesota Age-Appropriate Design Code Act, House Bill H.F. No. 2257 (introduced Feb. 27, 2023).

accessed Dec. 17, 2023), https://european-union.europa.eu/principles-countries-history/key-facts-and-figures/life-eu_en; European Union, *Facts and figures on the European Union economy* (last accessed Dec. 17, 2023), https://european-union.europa.eu/principles-countries-history/key-facts-and-figures/economy_en. In recent years, there has been robust growth in Internet usage and data consumption across Europe. Eurstat, *Digital economy and society statistics - households and individuals* (Dec. 15, 2023), https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals; Dr. Nejc Jakopin et al., *The evolution of data growth in Europe* (May 2023), https://www.adlittle.com/en/insights/report/evolution-data-growth-europe.

DPIAs are increasingly common in other advanced industrial nations too. The United Kingdom, even after formally withdrawing from the European Union, continues to consider DPIAs as a best practice and require them as a matter of UK law in some circumstances. *See generally* Information Commissioner's Office, *Data protection impact assessments*, *supra*; Information Commissioner's Office, Overview – *Data Protection and the EU* (last accessed Dec. 17, 2023), https://ico.org.uk/for-organisations/data-protection-and-the-eu/overview-data-protection-and-the-eu/; International Association of Privacy Professionals, *ICO: Sample*

DPIA Template (last accessed Dec. 17, 2023), https://iapp.org/resources/article/ico-sample-dpia-template/.

Singapore also has promoted DPIAs as part of the Data Protection Provisions of the Personal Data Protection Act (as passed in 2018 and amended in 2020). *See* Personal Data Protection Commission Singapore, *Guide to Data Protection Impact Assessments* (Sept. 14, 2021), https://www.pdpc.gov.sg/Help-and-Resources/2017/11/Guide-to-Data-Protection-Impact-Assessments; *See* Personal Data Protection Commission Singapore, *PDPA Overview* (last accessed Dec. 17, 2023), https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act; *see also* International Association of Privacy Professionals, *PDPC – Guide to Data Protection Impact Assessments* (last accessed Dec. 17, 2023), https://iapp.org/resources/article/pdpc-guide-to-data-protection-impact-assessments/. *Amicus*' experience in technology and public interest issues confirm that a notable consensus is emerging around the principles that undergird DPIAs.

In the United States and abroad, these DPIA requirements have not been legally controversial. *Amicus* is aware of no other successful challenges to a DPIA requirement on the basis that it constitutes a facially unconstitutional restriction on free speech. This Court may find it useful to carefully examine and apply precedent about when the government may require businesses to make certain disclosures,

particularly *Zauderer v. Off. of Disciplinary Couns. of Supreme Ct. of Ohio*, 471 U.S. 626 (1985), and its progeny in other contexts. *See e.g.*, *id.* at 651 ("purely factual and uncontroversial information about the terms under which [a company's] services will be available" are evaluated less stringently than laws that compel disclosure of other forms of speech); *Nat'l Inst. of Family and Life Advoc. v. Becerra*, 138 S. Ct. 2361, 2376 (2018) ("[W]e do not question the legality of health and safety warnings long considered permissible, or purely factual and uncontroversial disclosures about commercial products."); *Pac. Gas & Elec. Co. v. Pub. Util. Comm'n of California*, 475 U.S. 1, 16 n.12 (1986) (plurality op.) ("The State, of course, has substantial leeway in determining appropriate disclosure requirements for business corporations." (citing *Zauderer*)).

Indeed, the uncontroversial legal treatment of DPIAs makes sense, since the government imposes many other reporting requirements and risk assessments in the context of other conduct, services, and products. For example, the federal

government requires various technical assessments for airplanes[4] and automobiles,[5] which are also designed to assess and minimize product risks. It would be surprising to see all these mechanisms – which in many instances have existed for decades and are widely relied upon by consumers and companies alike – be suddenly struck down as facially unconstitutional.

III. FEDERAL LAW IS THE ORIGIN OF IMPACT ASSESSMENTS

It is important to understand that DPIAs are neither a foreign nor an entirely new creation, contrary to how they are sometimes misperceived. In fact, DPIAs trace their origins to federal privacy law from the 1970s onwards, which emerged in light of the increasing computerization of records across government and

---

[4] *See, e.g.*, Federal Aviation Administration (FAA), U.S. Department of Transportation, System Safety Assessments, 87 Fed. Reg. 75424 (Dec. 8, 2022), https://www.federalregister.gov/documents/2022/12/08/2022-26369/system-safety-assessments; Congressional Research Service, Legislative Reforms to Commercial Aircraft Certification, R46904 at 31 (Sept. 9, 2021) (discussing safety system assessments), https://sgp.fas.org/crs/misc/R46904.pdf.

[5] *See, e.g.*, National Highway Traffic Safety Administration, U.S. Department of Transportation, *New Car Assessment Program*, 87 Fed. Reg. 13452 (Mar. 9, 2022), https://www.federalregister.gov/documents/2022/03/09/2022-04894/new-car-assessment-program; Congressional Research Service, *Motor Vehicle Safety: Issues for Congress*, R46398 at 8 n.41 (June 8, 2020) ("The 5-star safety rating program, formally known as the New Car Assessment Program (NCAP), has since 1978 provided consumers with information on each vehicle's safety performance based on a series of crash scenario test conducted by NHTSA. NCAP was authorized by Congress in the Motor Vehicle Information and Cost Savings Act of 1973 (P.L. 92-513)."), https://crsreports.congress.gov/product/pdf/R/R46398/2.

industry during that era. In particular, the Privacy Act of 1974 and the E-Government Act of 2002 set out similar requirements for federal agencies developing new systems of records and data processes that may impact data privacy.

Namely, the Privacy Act of 1974 established foundations of U.S. privacy law – for the federal government and subsequently, the private sector – such as data minimization, individual consent, use limitations, disclosure, and reporting. *See generally* U.S. Department of Justice, *Overview of The Privacy Act of 1974* (2020 ed.), https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition. These principles established by the Privacy Act also underpin the core features of modern-day DPIAs.

Moreover, under Section 208 of the E-Government Act of 2002, federal agencies have been widely required to conduct privacy impact assessments (PIAs), which are closely related to DPIAs. *See* P.L. 107-347; 116 Stat. 2899; 44 U.S.C. Ch 36. These assessments are intended to "ensure sufficient protections for the privacy of personal information when the information is in an identifiable form." Congressional Research Service, *The Privacy Act of 1974: Overview and Issues for Congress*, R47863 at 17 (Dec. 7, 2023), https://crsreports.congress.gov/product/pdf/R/R47863. The 2002 Act defines "identifiable form" as "any

representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." 44 U.S.C. § 3501. A PIA analysis is rather similar to a DPIA, and basic questions include:

- what information is to be collected,
- why the information is being collected,
- the information's intended agency use,
- with whom the information will be shared,
- what notice or opportunities for consent would be provided to individuals regarding information collection and sharing,
- how the information will be secured, and
- whether a system of records is being created.

Congressional Research Service, *supra*, at 17 (citing 44 U.S.C. § 3501). "PIAs are to be reviewed by the agency CIO [Chief Information Officer], or equivalent official, as determined by the head of the agency." *Id.* "In the accompanying OMB Memorandum M-03-22, a PIA is required to be performed and 'updated as necessary' when a change creates new privacy risks . . . ." *Id. See also* OMB, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 at 4 (Sept. 26, 2003), https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2003/m03_22.pdf.[6] Public records

[6] "In 2010, OMB provided additional guidance on PIAs for agency use of third-party websites and applications." Congressional Research Service, *supra* at 18 (citing Kevin Neyland, *Model Privacy Impact Assessment for Agency Use of Third-Party Websites and Applications*, OMB (Dec. 29, 2011), https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/inforeg/inforeg/info_policy/model-pia-agency-use-third-party-websites-and-applications.pdf).

catalog dozens of PIAs conducted at many large federal agencies. *See, e.g.*, U.S. Department of Homeland Security, *Privacy Impact Assessments (PIA) Collection* (last accessed Dec. 18, 2023), https://www.dhs.gov/publications-library/collections/privacy-impact-assessments-%28pia%29. The history of PIAs and the E-Government Act of 2002 have had a lasting impact that continues to shape risk management practices more broadly. *See generally* R. Clarke, *Privacy impact assessment: its origin and development*, 25(2) Computer Law & Security Review. 123-135 (Apr. 2009); David Tancock et al., *The Emergence of Privacy Impact Assessments*, HP Laboratories, HPL-2010-63 (May 21, 2010), https://www.hpl.hp.com/techreports/2010/HPL-2010-63.pdf.

Much like DPIAs, their predecessors in federal law help to ensure that a range of agencies and government actors consider appropriately tailored data collection and processing tied to the purposes for which such records are created and maintained. These federal requirements have proven workable, lasting, and standardized. *Accord* Sujoy Chatterjee, *Automation is not a silver bullet for underlying PIA process issues*, International Association of Privacy Professionals (June 28, 2022), https://iapp.org/news/a/automation-is-no-silver-bullet-for-underlying-pia-process-issues/ ("For over two decades, a privacy impact assessment has been an essential part of the privacy professional's toolkit for understanding and mitigating privacy

risks.").[7] To the extent that the district court or the parties in this case were laboring under the misimpression that DPIAs are a completely novel – or perhaps foreign – legal requirement, the history simply does not bear that out.

[7] Since 2008, the International Standards Organisation has promulgated standards for PIAs. *See, e.g.*, ISO 22307:2008, *Financial services—Privacy impact assessment*; ISO 31000:2009, *Risk management — Principles and guideline*s; ISO 29134:2017, *Information technology — Security techniques — Guidelines for privacy impact assessment*.

CONCLUSION

At bottom, *amicus* respectfully urges the Court to carefully consider what DPIAs actually are, where they originated, and how they are used. *Amicus* take no position on district court's remedy or treatment of statutory features of CAADCA other than the DPIA. This Court may opt to remand, revise, or reign in aspects of the decision below – which took an expansive view of commercial speech and implicitly seemed to treat DPIAs as an extraordinary burden. Under all circumstances, however, categorically striking down a state law with potentially nationwide and global implications should, at the very least, be predicated on a precise and nuanced understanding of an important and widely used technical tool.

December 20, 2023

Respectfully submitted,

/s/ John Paul Schnapper-Casteras
John Paul Schnapper-Casteras
Counsel of Record
Rachael Yocum
SCHNAPPER-CASTERAS PLLC
1717 K Street NW, Suite 900
Washington, D.C. 20006
(202) 630-3644
jpsc@schnappercasteras.com

Counsel for Amicus Curiae

CERTIFICATE OF COMPLIANCE

This brief complies with the word limit of Federal Rule of Appellate Procedure Rule 32(a)(7)(B) and because it contains [__] words, excluding the portions exempted by Federal Rule of Appellate Procedure 32(f), and Circuit Rule 32-1. The brief also complies with the typeface and type-style requirements of Federal Rule of Appellate Procedure 32(a)(5) and (6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Times New Roman font.

Dated: December 20, 2023

/s/ John Paul Schnapper-Casteras
John Paul Schnapper-Casteras

CERTIFICATE OF SERVICE

I hereby certify that on December 20, 2023, this brief was filed electronically with the Clerk of the Court for the U.S. Court of Appeals for the Ninth Circuit through the Court's CM/ECF system. I certify that all participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

Dated: December 20, 2023

/s/ John Paul Schnapper-Casteras
John Paul Schnapper-Casteras