

12-31-2020

Easing the Burdens of a Patchwork Approach to Data Privacy Regulation in Favor of a Singular Comprehensive International Solution—The International Data Privacy Agreement

Scott Resnick

Follow this and additional works at: <https://brooklynworks.brooklaw.edu/bjil>



Part of the [Communications Law Commons](#), [Computer Law Commons](#), [Consumer Protection Law Commons](#), [European Law Commons](#), [Intellectual Property Law Commons](#), [International Law Commons](#), [Internet Law Commons](#), [Privacy Law Commons](#), and the [Transnational Law Commons](#)

Recommended Citation

Scott Resnick, *Easing the Burdens of a Patchwork Approach to Data Privacy Regulation in Favor of a Singular Comprehensive International Solution—The International Data Privacy Agreement*, 46 *Brook. J. Int'l L.* 277 (2020).

Available at: <https://brooklynworks.brooklaw.edu/bjil/vol46/iss1/8>

This Note is brought to you for free and open access by the Law Journals at BrooklynWorks. It has been accepted for inclusion in Brooklyn Journal of International Law by an authorized editor of BrooklynWorks.

EASING THE BURDENS OF A PATCHWORK APPROACH TO DATA PRIVACY REGULATION IN FAVOR OF A SINGULAR COMPREHENSIVE INTERNATIONAL SOLUTION – THE INTERNATIONAL DATA PRIVACY AGREEMENT

INTRODUCTION

Online Privacy. Hackers. Data Breach. Today, any uttering of the aforementioned phrases elicits fear in the minds of the public. Among lawmakers worldwide, it conjures conflicting attitudes and debate.¹ Most importantly, for players at every level of the consumer technology ecosystem, it has become synonymous with vague compliance, confusion, and economic inefficiency in adhering to a patchwork approach to data privacy regulation.²

The online data landscape is global in nature and gravely influential on some of the deepest pockets and most recognizable brand names in today's consumer-driven society.³ The passen-

1. Bart Custers, Francien Dechesne, Alan M. Sears, Tommaso Tani, Simone van der Hof., A Comparison of Data Protection Legislation and Policies Across the EU, 34 *COMPUT. L. & SEC. REV.* 234, 238 (2017) (“While there is some level of political debate on this issue in France, the strongest debates are found in the Netherlands, Germany, Sweden, the UK, and Italy. In some countries, such as the Netherlands and Italy, the debate is also initiated by supervisory authorities who have legal rights to advise on legislative proposals in which the processing of personal data plays a role.”).

2. See generally Frank Ready, *US Companies Among Most GDPR Compliant, But Privacy Burden Grows*, *LAW.COM*, (May 22, 2019), <https://www.law.com/legaltechnews/2019/05/22/us-companies-among-most-gdpr-compliant-but-privacy-burden-grows/?slreturn=20190919132524> (discussing the burdens facing businesses in complying with the GDPR as well as the hardships in ensuring IP-security while divulging privacy details to customers).

3. See Ivan De Luce, *10 companies that spent more than \$1billion in ads so you'd buy their products*, *BUS. INSIDER*, (Oct. 4, 2019), <https://www.businessinsider.com/10-biggest-advertising-spenders-in-the-us-2015-7> (“Collectively, the top 200 advertisers in the US spent a record \$163 billion on advertising in 2018, up 3.6% year on year, according to Ad Age’s annual Leading National Advertisers report. That growth is coming solely from internet ads . . .”).

gers filling the seats of this digital rollercoaster are endless: publishers, brands, ad exchanges, and data brokers all vie for a piece of the behemoth pie that is digital marketing partnership generation.⁴ Over the past decade, fledgling companies from all pockets of the globe have gained traction on a seemingly daily basis, labeling themselves with attention-grabbing slogans that position these companies as the go-to solution for marketers.⁵ Ultimately, these companies turn a profit on the procurement and sale of what marketers refer to as behavioral data—a valuable resource that has transcended the walls of jurisdictions and geography—and found a home in the transnational abyss of the Internet.⁶

Behavioral data refers to the information produced as a result of consumer actions, typically commercial behavior using a range of devices connected to the internet, such as a personal computer, tablet, or smartphone.⁷ This particular type of data is not static; it does not represent slowly changing features such as education, income, occupation, or residential location.⁸ Behavioral data provides marketers with a glimpse into moment-to-moment consumer activity, or more aptly put, behaviors. This data is then packaged and sold to front-end advertisers—including some of the most recognizable brands in the world—in order to better identify and reach the audience segment most likely to buy their product, at the most opportune time in the sales funnel,⁹ otherwise known as the customer acquisition process.

4. *See id.*

5. *See* Damien Geradin & Dimitrios Katsifis, An EU Competition law Analysis of Online Display Advertising in the Programmatic Age, 15 EUR. COMPETITION J. 55, 62 (2019) (“Third, programmatic advertising has given rise to so-called “ad tech” companies, that is operators that use dedicated software to intermediate between the two sides of the chain, i.e. publishers and advertisers, and facilitate the process of ad inventory buying and delivery of ads to the user.”); *See generally* THE TRADE DESK, thetradedesk.com, (last visited Oct. 14, 2020) (“Our mission is to transform media for the benefit of humankind. How? By helping brands deliver a more insightful and relevant ad experience for consumers, and setting a new standard for global reach, accuracy, and transparency. Learn what makes us different.”).

6. *See generally* Shane Greenstein, *Behind the Buzz of Behavioral Data*, DIGITOPOLY, (May 14, 2015), <https://digitopoly.org/2015/05/14/behind-the-buzz-of-behavioral-data/>.

7. *See id.*

8. *See id.*

9. *See id.*

Along with the explosion of digital media and the ubiquitous nature of behavioral data over the past decade-plus, various laws and regulations linger in the background of this ecosystem—especially in Europe.¹⁰ The European Union’s (EU) legislative actions, most notably the passage of the 1995 EU Data Protection Directive, were aimed at curbing the practice of utilizing consumer data without consent, notice, and accessibility.¹¹ Although the Data Protection Directive did not completely capture the intricacies of the digital world, it would lay the seeds for the enactment of the General Data Protection Regulation (GDPR) in 2016.¹²

Domestically, California, armed with the fifth largest economy in the world,¹³ followed suit two years later, hastily proposing and passing its own data privacy regulation, the California Consumer Privacy Act (CCPA), within one week in 2018.¹⁴ The CCPA, which went into effect on January 1, 2020, is the first of an anticipated onslaught of American data privacy regulations aimed at ensuring data transparency and holding companies accountable for what data they collect and how they obtain it.¹⁵

With a great deal of credit owed to the scalability of behavioral data, the digital advertising industry is currently a \$333

10. See generally *The History of the General Data Protection Regulation*, EUR. DATA PROT. SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en, (last visited Oct. 19, 2019).

11. See generally Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. L 281/31 [hereinafter DPD].

12. *The History of the General Data Protection Regulation*, *supra* note 10.

13. Kieran Corcoran, *California’s economy is now the 5th-biggest in the world, and has overtaken the United Kingdom*, BUS. INSIDER (May 5, 2018), <https://www.businessinsider.com/california-economy-ranks-5th-in-the-world-beating-the-uk-2018-5>.

14. Akin Gump, *California Passes Landmark Consumer Privacy CCPA – What it Means for Businesses*, JD SUPRA (July 9, 2018), <https://www.jdsupra.com/legalnews/california-passes-landmark-consumer-87324/>.

15. Jeff John Roberts, *Here Comes America’s First Privacy Law: What the CCPA Means for Business and Consumers*, FORTUNE (Sept. 13, 2019), <https://fortune.com/2019/09/13/what-is-ccpa-compliance-california-data-privacy-law/> (quoting Hayley Tsukayama, “In the past, firms adopted a “data is gold” mentality and made an effort to collect as much personal information as possible, but that is now changing”).

billion global competition comprised of companies with various roles throughout the digital advertising ecosystem.¹⁶ Today, digital advertising accounts for over half of the global ad market.¹⁷ For an industry that thrives on the free-flowing exchange of data, the onslaught of data privacy regulations poses a unique challenge to many of its' companies' core businesses.¹⁸ Most importantly, for companies that must become compliant with the CCPA only one year after altering their systems to become GDPR-compliant, implementation guarantees the stark reality of increased burdens on both employee resources and economic efficiencies.¹⁹

GDPR compliance cost the world's 500 largest corporations \$7.8 billion.²⁰ In a study conducted by PricewaterhouseCoopers (PwC), 40% of international companies surveyed reported spending more than \$10 million on compliance (it should be noted that the survey did not offer an option for a higher-spending category).²¹ Regarding the CCPA, a May 2019 survey of the information technology departments of a variety of companies with a digital presence reported that 71% of companies would spend in excess of \$100,000 to become compliant with the regulation, while 39% said it would take more than

16. Ethan Cramer-Flood, *Global Digital Ad Spending Update Q2 2020*, EMARKETER (Jul. 6, 2020), <https://www.emarketer.com/content/global-digital-ad-spending-update-q2-2020>.

17. *Id.*

18. See generally Tal Z. Zarsky, *Incompatible: the GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995 (2017).

19. See *Changes to employee data management under the GDPR*, TAYLORWESSING (Mar. 2017), <https://globaldatahub.taylorwessing.com/article/changes-to-employee-data-management-under-the-gdpr> ("As well as the obligation to provide comprehensive, clear and transparent privacy policies, if the employer has more than 250 employees, it must maintain additional internal records of its processing activities. This is likely to place further cost and administrative burdens on employers."). See also White & Case LLP, *California Consumer Privacy Act Guide*, JDSUPRA (Aug. 20, 2020), <https://www.jdsupra.com/legalnews/california-consumer-privacy-act-guide-42202/>.

20. Mehreen Khan, *Companies face high cost to meet new EU data protection rules*, FINANCIAL TIMES (Nov. 19 2017), <https://www.ft.com/content/0d47ffe4-ccb6-11e7-b781-794ce08b24dc>.

21. *Survey: One-fifth of large companies will spend over \$100 million, add over 50 staff on CCPA*, PRICEWATERHOUSECOOPERS, <https://www.pwc.com/us/en/services/consulting/cybersecurity/california-consumer-privacy-act/pulse-survey-large-companies-spend-over-100-million.html>.

\$500,000.²² Perhaps most telling, another PwC survey of Chief Information Officers at companies with at least \$1 billion in revenue found that 43% expected to spend over \$10 million to become CCPA compliant, with 20% anticipating CCPA budgets in excess \$100 million.²³

Indubitably, it is a near certainty that very few privacy-focused entities nor citizens—especially not the governments who are enacting the data privacy regulations—are going to feel sorry for businesses who must spend money in order to achieve optimal efficacy in safeguarding consumer data. Despite the likelihood of apathetic sentiments, when considering the monetary investments and hinderances on productivity, it is clear that there must be a more efficient path forward for businesses. A path that does not require companies to continuously pay large sums and expend human resources to adapt to each data privacy regulation that is passed into law. A path that solidifies the data privacy aims of the GDPR and CCPA in a more efficient manner. A path that adapts to the breadth and global nature of the digital advertising ecosystem.

First, this Note will present the intricacies of the digital advertising ecosystem. This will showcase the need for a more effective regulation that encompasses the diverse set of tasks fundamental to the transfer of online data and the innumerable parties who perform them. Next, this Note will analyze two landmark data privacy regulations, the GDPR and the CCPA, and present the challenges inherent to companies who must become compliant with both. It will then argue against a patchwork approach to global data privacy regulation and ultimately propose the creation of a more uniform, less onerous and singular data privacy regulation—the International Data Privacy Agreement.

Given the transnational and open-access nature of the Internet, and the lack of jurisdictional cyber boundaries between countries, it is imperative that governments avoid a patchwork approach to data privacy regulation. It would be more prudent and economically efficient for international businesses if governments around the world came together to formulate one

22. TRUSTARC, CCPA AND GDPR COMPLIANCE REPORT: RESEARCH INTO U.S. COMPLIANCE STATUS AND PLANS FOR CALIFORNIA CONSUMER PRIVACY ACT AND EU GENERAL DATA PROTECTION REGULATION 3 (2019).

23. *Survey: One-fifth of large companies will spend over \$100 million, add over 50 staff on CCPA*, *supra*, note 21.

singular data privacy regulation to govern the Internet. The international community has shown the ability to formulate a comprehensive regulatory approach to global technology issues, as evidenced by the enactments of The Internet Corporation for Assigned Names and Numbers (ICANN)²⁴ and the World Intellectual Property Organization (WIPO).²⁵ In line with ICANN's official motto, law makers and society as a whole must view global data privacy regulation through the guise of "One World. One Internet."²⁶ This Note argues for the benefits of creating an International Data Privacy Agreement, while utilizing the arduous processes and economic burdens of becoming CCPA-compliant for previously GDPR-compliant European companies as a vehicle to show the shortcomings of the current makeshift application.

I. THE DIGITAL ADVERTISING ECOSYSTEM AND THE ROLE OF DATA

The days of Don Draper and *Mad Men*²⁷ representing the go-to destination for advertising services are long gone. Prior to the advent of the Internet, marketers optimized the reach of their advertising efforts in a significantly less dynamic and analytical manner than in today's digitally focused and behavior-

24. See Generally *The Internet Corporation for Assigned Names and Numbers Resources*, ICANN, <https://www.icann.org/resources/pages/welcome-2012-02-25-en>[hereinafter ICANN] (ICANN is a nonprofit and non-government affiliated organization responsible for the distribution and functioning of the domain name system across the internet through its contracts with registries (such as dot-com or dot-info) and registrars (companies that sell domain names to individuals and organizations)).

25. See Generally WORLD INTELL. PROP. ORG., www.wipo.int, (last visited Oct. 3, 2019) [hereinafter WIPO] (WIPO is the global forum for intellectual property (IP) services, policy, information and cooperation. They are a self-funding agency of the United Nations, with 192 member states. WIPO's mission is to lead the development of a balanced and effective international IP system that enables innovation and creativity for the benefit of all).

26. *The Internet Corporation for Assigned Names and Numbers Resources*, *supra* note 24.

27. "Mad Men" was a hit American television series airing on AMC from 2007-2015. See *Mad Men*, IMDB, <https://www.imdb.com/title/tt0804503/> (last visited Dec. 3, 2019). The series depicted the fictitious life of successful advertising industry executive Don Draper in 1960's New York, a period referred to as the "golden age" of advertising. *Id.* Advertising executives during the time period were referred to as "Mad Men" due to Manhattan's Madison Avenue being the home to several of the world's largest advertising agencies. *Id.*

al-driven campaigns. Marketers bought television, newspaper, and billboard advertising space on channels, in publications and in physical locations in which static market research indicated their target audience as likely to be exposed.²⁸ This approach is widely referred to as “traditional advertising.”²⁹ While these methods still persist, sometimes in conjunction with digital advertising campaigns and other times completely separate, they have one fatal flaw: there is no guarantee that the advertiser’s target audience will be exposed to the advertisement.³⁰

Today, advertising is fueled by data, a process that helps to increase the likelihood ads are seen by their target audience.³¹ Advertisers and marketers can tap into the data created by users in the online world and leverage it to get their message in front of the right person, at the right time, with precision.³² Because this data lives online, digital media has emerged as the most expedient avenue toward an advertiser realizing its return on investment. In fact, analysts anticipate digital advertising to comprise more than two-thirds of total media advertising spend by 2023.³³

There are three main ways in which companies collect online user data: (1) Asking customers directly (e.g., registration forms); (2) indirectly tracking; (3) or through third-party data

28. Maciej Zawadziński, *The Truth About Online Privacy: Your Data is Collected, Shared and Sold*, CLEARCODE, <https://clearcode.cc/blog/online-privacy-user-data/>.

29. Lynn Lauren, *Examples of Traditional Advertising*, CHRON, <https://smallbusiness.chron.com/examples-traditional-advertising-24312.html>.

30. Millie Wright, *Offline Advertising in the Digital Age: Why traditional advertising isn't dead*, DAVIES + SCOTHORN (Nov. 16, 2018), <https://www.daviesscothorn.com/2018/11/16/offline-advertising-in-the-digital-age-why-traditional-advertising-isnt-dead/>.

31. Jasmine Enberg, *Digital Ad Spending 2019 Global*, EMARKETER (Mar. 28, 2019), <https://www.emarketer.com/content/global-digital-ad-spending-2019> (“Armed with data that will help them more fully understand the customer journey, they can better target their audiences and personalize messages cohesively across the marketing landscape.”).

32. Zawadziński, *supra* note 28.

33. Dade Hayes, *Digital Ad Spending Will Start To Outpace Traditional Ad Spending in 2019 – Report*, DEADLINE, (Feb. 20, 2019), <https://deadline.com/2019/02/digital-ad-spending-to-start-outpacing-traditional-ad-spending-in-2019-emarketer-1202560394/>.

brokers.³⁴ Regarding companies indirectly tracking customer data, the most frequent display of this practice centers on the implementation of web cookies, or simply “cookies.” Cookies are a piece of web text sent to a user’s browser (e.g. Google Chrome, Safari, etc.) by a website that the user visits.³⁵ Web beacons may also be used in place of, or in conjunction, with cookies.³⁶ From an advertising standpoint, web cookies’ main function is to track the activity of users across the web to better identify whether a given user fits into the advertiser’s precise demographic.³⁷ There are two broad categories of cookie implementation; first-party cookies are issued by the website the user is visiting, while third-party cookies track users across different websites by companies that have no relationship with consumers (i.e., advertisers or data brokers).³⁸ Additionally, cookies may be repackaged and resold from one data broker to another, proliferating the sheer volume of personal data in the hands of various technology platforms across the internet.³⁹

Cookies serve myriad purposes, including innocuous functions such as remembering login information or storing user preferences for a specific site.⁴⁰ More importantly for a company’s business interests, the company can utilize the user data that cookies collect to deliver retargeted ads.⁴¹ Many companies buy targeted ad space on larger platforms such as Google or Facebook through pixels that are implemented into the cookies that a company “drops” on their own proprietary website.⁴² For

34. William Goddard, *How Do Big Companies Collect Consumer Data?*, IT CHRONICLES, <https://www.itchronicles.com/big-data/how-do-big-companies-collect-customer-data/>.

35. See *Google Privacy and Terms, How Google Uses Cookies*, GOOGLE, <https://policies.google.com/technologies/cookies?hl=en-US>.

36. Goddard, *supra* note 34.

37. Chris Jay Hoofnagle, Ashkan Soltani, Nathan Good, Dietrich James Wambach & Mika D Ayenson, *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARV. L. & POL'Y REV. 273, 276 (2012) (“One way that websites track users is through “cookies,” small text files that typically contain a string of numbers that can be used to identify a computer.”).

38. *Id.*

39. Zawadzinski, *supra* note 28.

40. Cookie Definition, Techterms.com, <https://techterms.com/definition/cookie>, (last visited Sept. 20, 2019).

41. Zawadzinski, *supra* note 28.

42. See generally Cade Metz, *How Facebook’s Ad System Works*, N.Y. TIMES (Oct. 12, 2017), <https://www.nytimes.com/2017/10/12/technology/how-facebook-ads-work.html>.

example, when a user is shopping for a pair of sneakers at Nike.com, and hours later an ad appeared on their Facebook.com user page for Nike sneakers, it is likely that Nike leveraged user data collected from their cookies to “retarget” that advertisement to the user.

Web beacons are small images that are embedded into a webpage, usually in the form of a 1x1 pixel tracker.⁴³ When a browser connects to a company’s webpage that contains a web beacon image, the user’s browser requests to download the web beacon to the company’s webserver.⁴⁴ Once the request is made, the server logs information via the web beacon, including a user’s IP address and activity on the site.⁴⁵ Companies leverage this data to better inform their marketing strategies, including whom their most valuable customers are and where they are located in the sales funnel.⁴⁶ This enables companies to be more efficient in their advertising, resulting in a greater return on their investment—an integral metric used to gauge the success of advertising campaigns.⁴⁷

While companies themselves take a leading role in collecting user data, it has become near industry-standard that companies will also lean on third-party data brokers in order to collect user data to enhance their advertising tactics.⁴⁸ These brokers play such a prevalent role in the digital advertising ecosystem that they generate upwards of \$200 billion annually.⁴⁹ Data brokers are companies that either collect online data

43. James Frew, *How Advertisers Use Web Beacons to Track You on the Web and in Emails*, MAKEUSEOF (Dec. 21, 2016), <https://www.makeuseof.com/tag/how-web-beacons-track-web/>.

44. See *What is a Webserver?*, NGINX, <https://www.nginx.com/resources/glossary/web-server/> (explaining the function of a webserver, mainly that it stores and delivers the content for a website – such as text, image, video and application data – to clients who request it via their web browsers).

45. Frew, *supra* note 43.

46. For an overview of the consumer purchase funnel, see generally Takeshi Moriguchi, Guiyang Xiong, & Xueming Luo, *Retargeting Ads for Shopping Cart Recovery: Evidence from Online Field Experiments* (Simon Bus. Sch. Working Paper No. FR 15-21, 2016).

47. Frew, *supra* note 43.

48. Geradin & Katsifis, *supra* note 5, at 22 (explaining the role of third-party data ad exchanges in the advertising ecosystem).

49. See *What Are Data Brokers – And What Is your Data Worth? [Infographic]*, WEBFX (Mar. 16, 2020), <https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/>.

themselves or buy it from other companies, and aggregate that data with offline sources (e.g. driver's license, census data, credit card information, birth certificates, etc.).⁵⁰ Data brokers crawl the internet for useful information such as data found on social media profiles, user web history, and even acquire credit card or government record information from third parties.⁵¹ Data brokers collect and sell these user data points to marketers so that advertisers can more efficiently reach their preferred "buyer persona"—i.e., their ideal customer.⁵²

Brokers then package that data into groups known as "audience segments"⁵³ and sell them either directly to advertisers or to advertising technology companies who may narrow the segments into more niche audiences.⁵⁴ Advertising technology companies offer various services such as data management platforms (DMP)⁵⁵ or programmatic advertising exchanges.⁵⁶ Both of these platforms house customer data in defined audience segments—e.g., "sports fans" or "designer clothing enthusiasts"—to better assist an advertiser's digital advertising campaign in real time.⁵⁷

50. See Michal Wlosik, *What Is a Data Broker and How Does it Work?*, CLEARCODE, <https://clearcode.cc/blog/what-is-data-broker/>.

51. See *id.*

52. See *Customer Segmentation & Targeting – A Guide*, DIG. MKTG. INST., <https://digitalmarketinginstitute.com/en-us/blog/2018-04-24-customer-segmentation-targeting-a-guide>.

53. See *id.* (defining "audience segment" as: "when you divide your audience into different groups based on various criteria, such as demographics and media use. Digital marketers segment audiences as a key part of a targeted marketing strategy).

54. See Steven Melendez & Alex Pasternack, *Here are the data brokers quietly buying and selling your personal information*, FAST COMPANY (Mar. 2, 2019), <https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information>.

55. See *The Complete Guide to Digital Ad Technology*, THE APP SOL., <https://theappsolutions.com/blog/development/what-why-how-adtech/> (defining a DMP as technology that analyzes and categorizes incoming data in order to segment the audiences and optimize live advertising campaigns accordingly).

56. See Charlotte Rogers, *Programmatic Advertising & Media Buying*, MKTG. WEEK (Mar. 27, 2017), <https://www.marketingweek.com/programmatic-advertising/> ("Put very simply, programmatic is buying digital advertising space automatically, with computers using data to decide which ads to buy and how much to pay for them, often in real time.").

57. Zawadziński, *supra* note 28.

Altogether, the process of data collection online is not simply a quid pro quo exchange between customer and advertiser. There are a multitude of players in the ad tech space who have their hands in consumer data. These companies play a significant role in the collection, processing, and distribution of society's most closely guarded data—the very information that the industry-altering data privacy regulations seek to protect.

A. Introduction to the General Data Protection Regulation

On May 25, 2018, the EU's GDPR came into force.⁵⁸ The occasion marked the culmination of years of efforts to morph the European Union's privacy laws into a comprehensive regulation fit for the digital age.⁵⁹ After initially being approved by the European Parliament in April 2016, the EU granted a two-year transition period to enable companies to adjust to the regulations and become compliant before the GDPR's official May 2018 launch.⁶⁰

The GDPR, which grew out of 1995's EU Data Protection Directive,⁶¹ provides a rigid standard relating to the protection of natural persons with regard to the processing and free movement of personal data.⁶² Specifically, the regulation applies to controllers and processors that process the personal data of "data subjects"—the term used to refer to individuals in the text of the GDPR—and are either: (1) established in the EU or (2) established outside the EU, but offer goods or services to, or monitor the behavior of, data subjects in the EU.⁶³ Personal data is defined as "any information relating to an identified or identifiable subject."⁶⁴ In accordance with the GDPR, personal data can include a name, identification number, location data, or one or more factors specific to the physical, physiological,

58. *What is GDPR, the EU's new data protection law?*, GDPR.EU, <https://gdpr.eu/what-is-gdpr/?cn-reloaded=1> (last visited July 8, 2020).

59. *See generally The History of the General Data Protection Regulation*, EUR. DATA PROT. SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited July 8, 2020).

60. *What is GDPR, the EU's new data protection law?*, *supra* note 58.

61. *See generally* DPD, *supra* note 11.

62. Regulation 2016/679, at 1, 95/46/EC, 2016 O.J. (L 119) 1 [hereinafter GDPR].

63. *Id.* art. 3(2).

64. *Id.* art. 4(1).

genetic, mental, economic, cultural, or social identity of that person.⁶⁵

Further, the GDPR enables EU citizens to take control of, or garner insight into, the methods in which their personal data is handled.⁶⁶ The GDPR labels the organizations that are responsible for the handling of consumer data as “Data Controllers” and “Data Processors.”⁶⁷ Data Controllers are defined as “a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of processing of personal data.”⁶⁸ On the other hand, “Data Processors” are labeled as a “natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.”⁶⁹ Importantly, this distinction widens the jurisdictional net of the GDPR, as it enables the EU to hold each member of the digital advertising ecosystem responsible for the handling of user data— e.g., advertising technology companies, advertisers, etc.—not just those front-end hosts who initially collect the data⁷⁰

The key tenets of the GDPR, however, are the data privacy rights that it grants to consumers. Specifically, the GDPR provides data subjects with eight rights:⁷¹ (1) the right to be informed; (2) the right to access; (3) the right to rectification; (4) the right to erasure; (5) the right to restrict processing; (6) the right to data portability; (7) the right to object; and (8) rights related to automated decision making including profiling.⁷²

Chief among these rights is the data subject’s right to object to their data being shared unless the controller can show a “compelling legitimate ground.”⁷³ The GDPR lists “compelling legitimate grounds” as any of six various scenarios facing businesses, and in doing so sets forth the necessary conditions in order for the processing of personal information to be deemed

65. *Id.*

66. *See generally*, Emmanuel Salami, *An Analysis of the Gen. Data Prot. Regulation (EU) 2016/679* (Ottawa Fac. of L. Working Paper No. 2020-26, 2017).

67. GDPR, *supra* note 62, art. 4.

68. *Id.* art. 4(7).

69. *Id.* art. 4(8).

70. Rogers, *supra* note 56 (generally describing the various players in the digital advertising ecosystem).

71. GDPR, *supra* note 62, art. 15(2).

72. *Id.* art. 15-22.

73. *Id.* art. 21.

as legal: (1) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (2) processing is necessary for the performance of a contract in which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract; (3) processing is necessary for compliance with a legal obligation to which the controller is subject; (4) processing is necessary in order to protect the vital interest of the data subject or of another natural person; (5) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and (6) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.⁷⁴

In regard to the consent requirement, the GDPR has set a strict standard for the ways in which controllers can obtain valid legal consent from data subjects.⁷⁵ Most notably, the request for consent must be presented in a clearly distinguishable manner, in an intelligible and easily accessible form, and using clear and plain language.⁷⁶ This is most often seen in the form of cookie consent requests or cookie notices on websites of data controllers operating within the EU. These notices often include links to additional information regarding a website's privacy and cookie policies. Further, the GDPR sets forth restrictions on conditioning consent on provisions of a service. For example, the UK's Information Commissioner's Office (ICO), the nation's lead enforcement body of the GDPR, recently provided an official warning to the Washington Post that the company could not condition consent to the processing of personal data by allowing users to opt-out of cookies and other trackers only under its paid subscription feature.⁷⁷

Importantly, while a data subject does have the right to withdraw his or her consent at any time, the consent does not

74. *Id.* art. 8.

75. *Id.* art. 7.

76. *Id.*

77. See Rebecca Hill, *Washington Post offers invalid cookie consent under EU rules – ICO*, THE REGISTER (Nov. 19, 2018, 09:49 UTC), https://www.theregister.com/2018/11/19/ico_washington_post/.

affect the lawfulness of processing based on consent before its withdrawal.⁷⁸ As discussed above, once a data subject withdraws their consent, the data controller must be able to point to one of the other bases for a “compelling legitimate ground” in order to maintain lawfulness of processing.⁷⁹

For any data processor or controller who does not comply with the requirements set forth in the GDPR, there are two tiers of fines that may be handed down from the appropriate Data Protection Authority (DPA) located within each EU member state.⁸⁰ First, less severe violations may result in fines up to €10 million or 2% of the company’s worldwide annual revenue from the preceding year, whichever is higher.⁸¹ Alternatively, more egregious violations may result in fines up to the greater of €20 million or 4% of a company’s worldwide annual revenue from the preceding year.⁸² The GDPR also provides for a private right of action for the breach of a data subject’s unencrypted information.⁸³ Data subjects may file complaints directly to the DPA within the member state of his or her habitual residence, place of work, or place of the alleged data infringement.⁸⁴

B. Introduction to the California Consumer Privacy Act

The CCPA went into effect on January 1, 2020. It has been widely viewed as the first American response to the GDPR due to California’s premier economic and political position in the US and the first of an anticipated onslaught of state-enacted data privacy regulations in the country.⁸⁵ Currently, a sweeping federal data privacy regulation in the US does not appear to be on the horizon.⁸⁶ Therefore, a state-by-state approach is

78. GDPR, *supra* note 62, art. 7.

79. *Id.* art. 21.

80. *Id.* art. 83.

81. *Id.*

82. *Id.*

83. *Id.* art. 82.

84. *Id.* art. 77.

85. Tony Romm, *California adopted the country’s first consumer privacy law. Now, Silicon Valley is trying to rewrite it.*, WASH. POST (Sept. 3, 2019, 11:26 A.M. EDT), <https://www.washingtonpost.com/technology/2019/09/02/california-adopted-countrys-first-major-consumer-privacy-law-now-silicon-valley-is-trying-rewrite-it/>.

86. See David McCabe, *Congress and Trump Agreed They Want a National Privacy Law. It is Nowhere in Sight.* N.Y. TIMES (Oct. 1, 2019),

the likely the path forward for data privacy regulations in the US for the foreseeable future.⁸⁷

The CCPA requires both disclosure obligations as well as information governance. It applies to any for-profit enterprise that collects consumers' personal information or determines the purposes and means of the processing of consumers' personal information, does business in the state of California, and satisfies one or more of the following thresholds: (1) has annual gross revenues in excess of \$25 million; (2) alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or (3) derives 50% percent or more of its annual revenues from selling consumers' personal information.⁸⁸ The CCPA purports to task both advertisers and the long-tail advertising ecosystem—i.e., back-end technology and data partners—with liability for the mishandling of personal information.⁸⁹ Under the CCPA, personal information includes identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.⁹⁰

The CCPA empowers consumers with several rights in regard to the handling of their data privacy.⁹¹ These rights include: (1) the right to receive information on privacy practices and access

<https://www.nytimes.com/2019/10/01/technology/national-privacy-law.html> (noting that while there is pressure from industry groups, there does not appear to be an imminent presentment of a federal data privacy proposal).

87. *See id.*

88. CAL. CIV. CODE § 1798.140.

89. *See* Tim Peterson, 'We're not going to play around': Ad industry grapples with California's ambiguous privacy law, DIGIDAY (Dec. 9, 2019), <https://digiday.com/marketing/not-going-play-around-ad-industry-grapples-californias-ambiguous-privacy-law/> (quoting Thomas Chow, general counsel and secretary at PubMatic, "There are still some in the ecosystem that want to take the approach that passing personal information with respect to advertising is not a sale, but I think the statute as drafted covers every use case that the ad tech ecosystem has to deal with."); *see also* CAL. CIV. CODE § 1798.140(t) (explaining the "service provider exception" which obligates service providers who receive an opt-out request from a consumer to cease from further collecting of that consumer's information, selling, or using the personal information except as necessary to perform the business purpose.").

90. CAL. CIV. CODE § 1798.140(o)(1)(A).

91. Roberts, *supra* note 15.

information;⁹² (2) the right to deletion;⁹³ (3) information required to be provided as part of an access request;⁹⁴ (4) the right to receive information about onward disclosures;⁹⁵ (5) the right to prohibit the sale of their information;⁹⁶ and (6) no price discrimination based upon the exercise of the opt-out right.⁹⁷

Under the CCPA, businesses who do not comply with the regulations set forth may face fines of either \$7,500 or \$2,500 per violation.⁹⁸ The California Attorney General has the enforcement authority to seek penalties against a business of up to \$7,500 per intentional violation, subject to giving the business a thirty-day period to cure a violation before bringing action.⁹⁹ A business's inability or unwillingness to correct a violation during a grace period may provide strong evidence of intent and therefore the business would likely face the \$7,500 violation.¹⁰⁰ Companies that are able to cure a violation would face the lesser \$2,500 penalty per violation.¹⁰¹

Additionally, the CCPA enables private citizens to bring suit for the breach of their "non-encrypted or non-redacted personal information," even in the absence of actual damages.¹⁰² For these violations, citizens may recover between \$100 and \$750 per violation.¹⁰³ Similar to the GDPR, a citizen's private right of action stems strictly from breaches of consumer data.¹⁰⁴

92. CAL. CIV. CODE § 1798.100.

93. CAL. CIV. CODE § 1798.105.

94. CAL. CIV. CODE § 1798.110.

95. CAL. CIV. CODE § 1798.115.

96. CAL. CIV. CODE § 1798.120.

97. CAL. CIV. CODE § 1798.125.

98. CAL. CIV. CODE § 1798.155(b).

99. *Id.*

100. *California Consumer Privacy Act (CCPA) Fines and Consumer Damages*, CLARIP, <https://www.clarip.com/data-privacy/california-consumer-privacy-act-fines/>, (last visited Oct. 1, 2019).

101. *See id.*

102. CAL. CIV. CODE §1798.150

103. *Id.*

104. *See* Todd Ehret, *Data privacy and GDPR at one year, a U.S. perspective. Part Two – U.S. challenges ahead*, REUTERS (May 29, 2019), <https://www.reuters.com/article/us-bc-finreg-gdpr-report-card-2/data-privacy-and-gdpr-at-one-year-a-us-perspective-part-two-us-challenges-ahead-idUSKCN1SZ1US> ("A new risk emerging from GDPR is the risk of private litigation. Under GDPR, individuals are able to claim for "material or non-material damage" as a result of the breach of the GDPR. The CCPA and other state laws also create a private right of action similar to GDPR.").

II. KEY DIFFERENCES BETWEEN THE GDPR AND THE CCPA, AND THE BURDENS BUSINESSES ARE FACED WITH IN COMPLYING WITH BOTH

To the general public, the GDPR and the CCPA purport to rectify identical data privacy issues in a uniform and consistent manner.¹⁰⁵ In fact, the CCPA is often referred to as “GDPR-lite.”¹⁰⁶ Despite this description, there are several key differences between the two regulations which render simultaneous compliance a rather taxing process for international businesses. Namely, these areas include the scope of compliance, the extensiveness of personal data, and the breadth of consumer rights.¹⁰⁷

A. *Personal Information & Data Mapping*

The threshold issue for any company with an online presence is whether they are required to comply with the GDPR and CCPA.¹⁰⁸ In regard to the dual-compliance burden, this question does not pose a significant inconvenience to companies, although the CCPA standard does leave considerably more am-

105. See Anupam Chander, Margot E. Kaminski & William McGeeveran, *Catalyzing Privacy Law*, 2190 GEO. L. FAC. PUBL'N & OTHER WORKS 1, 14 (2019) (“At first glance, too, some core elements of the CCPA echo aspects of the GDPR. Both laws define personal information very broadly, far beyond most existing U.S. privacy laws. Both laws foundationally emphasize transparency...And both laws share the contours of a number of additional individual rights.”).

106. See *Generally California Consumer Privacy Act: What You Need to Know About “GDPR Lite”*, MEDIUM, (June 17, 2019), <https://medium.com/the-regtech-hub/california-consumer-privacy-act-what-you-need-to-know-about-gdpr-lite-c20c4a62aa1b>.

107. Chander, Kaminski, & McGeeveran, *supra* note 105, at 19.

108. See Elaine F. Harwell, *What Businesses Need to Know about the California Consumer Privacy Act*, THE AMERICAN BAR ASSOCIATION, (Oct. 7, 2019), https://www.americanbar.org/groups/business_law/publications/blt/2019/10/ca-consumer-privacy/.

biguity¹⁰⁹ when compared to the bright-line delineation supplied by the GDPR.¹¹⁰

Once it is determined compliance is required, the more pressing and burdensome issue is what that compliance looks like in practice. Sometimes, though, compliance with one of the GDPR or CCPA can make compliance with the other easier—although that is rarely the case. For example, the GDPR requirement of data mapping may result in a rare seamless transition in a micro-sense for companies facing dual-compliance. For nearly all international businesses who have already become compliant with the GDPR,¹¹¹ data mapping is likely already an integral part of their daily process, in accordance with Article 30 of the GDPR.¹¹² Article 30 provides that organizations that control personal data must maintain a record of their processing activities.¹¹³ According to *Techopedia*, “[d]ata mapping is a process used in data warehousing by which different data models are linked to each other using a defined set of methods to characterize the data in a specific definition . . . data mapping serves as the initial step in data integration.”¹¹⁴ In other words, data mapping is a business’s practice of organizing its acquired user data and information flows in order to assess privacy risks, of-

109. See generally *Does the CCPA Apply to Your Business?* THE NATIONAL LAW REVIEW (Aug. 14, 2019), <https://www.natlawreview.com/article/does-ccpa-apply-to-your-business> (explaining the uncertain “does business” standard in the CCPA, as well as the requirements for compliance for a subsidiary or parent company of a business that is tasked with compliance).

110. See *id.* (analyzing the difficulty in assessing whether compliance with the CCPA is a necessity for companies due to the ambiguity of the “does business” standard).

111. See *The Importance of Article 30 of the General Data Protection Regulation of the European Union (GDPR)*, VERASAFE (Mar. 9, 2018), <https://www.verasafe.com/blog/the-importance-of-article-30-of-the-general-data-protection-regulation-of-the-european-union-gdpr/> (“the obligations under Article 30 apply to every organization regulated by the GDPR unless all of the following criteria apply to the organization simultaneously: (1) the processing is occasional; (2) the processing it carries out is not likely to result in a risk to the rights and freedoms of data subjects; (3) the processing includes no specific categories of data, as referred to in Article 9(1) and no personal data relating to criminal convictions and offences referred to in Article 10, and; (4) the organization employs fewer than 250 employees.”).

112. GDPR, *supra* note 62, art. 30.

113. *Id.*

114. *Data Mapping*, TECHOPEDIA, https://www.techopedia.com/definition/6750/data-mapping_ (last visited Nov. 12, 2019).

ten producing an output in a visual format or excel document.¹¹⁵ The key elements of data mapping include understanding the information flow (i.e., from inside to outside the EU), describing the information flow (i.e., determining any unforeseen uses of data throughout the data lifecycle), and identifying the key elements of the information flow (i.e., data items, formats, transfer methods, location, accountability, access, lawful basis for using data).¹¹⁶ Additionally, for international businesses complying with the GDPR, Article 30 requires the appointment of a “data protection officer.”¹¹⁷

Conversely, the CCPA does not require data mapping within its guidelines, but a key provision of the CCPA is the obligation of businesses to respond to the requests of California consumers to: (1) access their personal information; (2) have their personal information deleted from a business’ systems, as well as any third parties who the business might have sold the information to, and; (3) to opt out of the sale of their personal information.¹¹⁸ In essence, this means that in order to have consumer data readily available for request, data mapping is a necessity.

Much to the dismay of these international businesses, this is likely where ease of dual-compliance ends. One such contrast can be gleaned from the two regulations’ disclosure rights. The CCPA provides for an on-demand disclosure right,¹¹⁹ as businesses must respond within forty-five days to any verified consumer request for a portable copy of the data a business holds about them that was collected in the twelve months prior to the request.¹²⁰ The GDPR, on the other hand, requires the disclo-

115. See *GDPR – Data Mapping: What is it and how to comply*, ITGOVERNANCE, <https://www.itgovernance.co.uk/gdpr-data-mapping> (last visited Nov. 11, 2019).

116. See *id.*

117. See *id.*

118. See generally Dan Goldstein, *Where to begin to operationalize CCPA compliance*, INT’L ASS’N OF PRIV. PRO. (Jan. 29, 2019), <https://iapp.org/news/a/where-to-begin-to-operationalize-ccpa-compliance/> (explaining the necessity for CCPA-complaint businesses to undertake data mapping in order to fulfill the rights granted to consumers).

119. See Catherine D. Meyer, Steven Farmer, Fusae Nara & Rafi Azim-Khan, *Countdown to CCPA #2: GDPR Compliance Does Not Equal CCPA Compliance*, PILLSBURY L. (June 3, 2019), <https://www.pillsburylaw.com/en/news-and-insights/ccpa-compliance-gdpr.html>.

120. CAL. CIV. CODE §1798.130(a)(3)(B).

sure of all data collected without a definitive time limit within one month of the request.¹²¹

Another important distinction is the varying depth of the definitions of personal information inherent in the two regulations.¹²² Under the GDPR, data subjects are identifiable if they can be directly or indirectly identified, by reference to a name, identification number, location data, an online identifier, or one of several special characteristics which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons.¹²³ The CCPA extends the protection of personal information to a group of potential identifiers if they are capable of being associated with, or can be reasonably linked, either directly or indirectly, with a particular consumer or *household*. As mentioned above, these identifiers include: a real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.¹²⁴ While there has been no definitive announcement from the Attorney General of California regarding the definition of "household," its inclusion in the CCPA diverges from the singular consumer-focused trend set forth by the GDPR. Therefore, CCPA-compliant multinational companies will have to account for data that may identify a household, but not a particular individual—a departure from the GDPR's focus.¹²⁵

Because the depth of data that must be disclosed varies between the GDPR and the CCPA,¹²⁶ the need for separate data mapping in compliance with both regulations is further necessitated. Due to the intricate differences between personal information under the CCPA and personal data within the

121. GDPR, *supra* note 62, art. 12.

122. See Jon Fielding, *Four differences between the GDPR and the CCPA*, HELP NET SEC., (Feb. 4, 2019), <https://www.helpnetsecurity.com/2019/02/04/gdpr-ccpa-differences/> (explaining the differences between the coverage of personal data in the CCPA as opposed to the GDPR – "The GDPR is specifically focused on all data related to the EU consumer/citizen whereas the CCPA considers both the consumer and household as identifiable entities").

123. GDPR, *supra* note 62, art. 4.

124. CAL. CIV. CODE § 1798.140(o)(1)(A), *supra* note 90.

125. GDPR, *supra* note 62 art. 4(1).

126. Fielding, *supra*, note 122.

GDPR,¹²⁷ the data mapping processes installed by an international business currently complying with the GDPR will have to be replicated under the CCPA. In turn, this process will command twice the workload, and divert employees from more pressing matters, including contributing to the operational functionality of the business itself.¹²⁸

Whereas international businesses that underwent data mapping under the GDPR likely set aside U.S. data and focused squarely on EU citizen data, the task of encompassing U.S. consumer data within the confines of the consumer rights set forth in the CCPA will prove to be a cumbersome exercise.¹²⁹ Given the stringent requirements for personal information set forth in the CCPA, data mapping will incorporate the necessity for these businesses to map any personal information that relates to California residents. This includes all internet activity, including click stream, interactions with the website, browsing history, IP addresses, and mobile device ID.¹³⁰ Additionally, companies will likely want to include inferences drawn¹³¹ from any personal information to create a profile about a consumer reflecting their preferences, characteristics, behavior, or attitude, as well as all “household” and “device” data¹³² given the broader definition of “personal information” fundamental to the

127. See Eric Goldman, *An Overview of the California Consumer Privacy Act* (June 12, 2019), Santa Clara University School of Law Legal Studies Research Paper Series, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3211013 (“As with the GDPR, attempts to distinguish personal information from non-personal information are likely to be under- or over-inclusive. The CCPA took the (massively) over-inclusive route.”).

128. See generally Damon W. Silver & Catherine R. Tucciarello, *CCPA: Expansive Array of Consumer Rights Imposes Rigorous Compliance Burden* (Sept. 18, 2019), JACKSON LEWIS P.C., <https://www.workplaceprivacyreport.com/2019/09/articles/california-consumer-privacy-act/ccpa-expansive-array-of-consumer-rights-imposes-rigorous-compliance-burden/> (highlighting the burdens facing companies in regard to complying with the CCPA’s consumer rights).

129. See *id.*

130. See Odia Kagan, *If at First You GDPR, CCPA, CCPA Again*, Fox Rothschild LLP (May 8, 2019), <https://www.foxrothschild.com/publications/if-at-first-you-gdpr-ccpa-ccpa-again/> (analyzing the areas in which data mapping for the CCPA should be focused in accordance with the Act’s guidelines).

131. See *id.*

132. GDPR, *supra* note 62, art. 15(2) (right to access creates an obligation for the business to maintain all data used in connection with a consumer).

CCPA¹³³ as opposed to the corresponding definition within the GDPR.¹³⁴

Given the inherent differences within the territorial scope, consumer rights, and pertinent personal information of the two regulations, the task of replicating or broadening the existing GDPR data mapping schematics to apply to the CCPA will prove to be a burden on international businesses. For example, since the GDPR does not include the term “household” in its definition of personal data, international companies who previously became compliant with the GDPR cannot recycle their compliance programs for the CCPA, which will incur significant costs on the business.¹³⁵ Furthermore, companies will have to plan accordingly knowing that the CCPA is likely the first of many US state-specific data privacy laws.¹³⁶

B. Opt-In vs. Opt-Out

While both the GDPR and CCPA require detailed privacy notices, in order to obtain consumer consent, the content of those notices differ.¹³⁷ Therefore, a notice that satisfies the GDPR will not satisfy the requirements set forth by the CCPA.¹³⁸ The core operational difference between the two mandates in this regard centers on the CCPA’s requirement for a consumer opt-out, while the GDPR provides data subject consent as a lawful grounds for processing under an opt-in feature.¹³⁹

Under the CCPA, a business’ privacy policy must notify consumers about their right of erasure, collections regarding the sale or disclosure of personal information, the opt-out right for data sales, and restrictions on privacy-based discrimination.¹⁴⁰ Specifically, businesses are required to provide a clear and con-

133. CAL. CIV. CODE § 1798.140(o)(1)(A), *supra* note 90.

134. GDPR, *supra* note 62 art. 4(1).

135. Goldman, *supra* note 127.

136. *See generally* Jeewon Kim Serrato & Susan Ross, *Nevada, New York and other states follow California’s CCPA*, NORTON ROSE FULBRIGHT (June 6, 2019), <https://www.dataprotectionreport.com/2019/06/nevada-new-york-and-other-states-follow-californias-ccpa/>.

137. *See* Carol A.F. Umhoefer & Tracy Shapiro, *CCPA vs. GDPR: the same, only different*, DLA PIPER (Apr. 11, 2019), <https://www.dlapiper.com/en/us/insights/publications/2019/04/ipt-news-q1-2019/ccpa-vs-gdpr/>

138. *See id.*

139. Meyer, Farmer, Nara & Azim-Khan, *supra* note 119.

140. CAL. CIV. CODE § 1798.130(a)(5).

spicuous link on the homepage of websites and mobile applications titled “Do Not Sell My Personal Information.”¹⁴¹ The link’s landing page must be the business’s online privacy policy page, setting forth the new rights afforded to California residents.¹⁴² Additionally, the CCPA calls for the development and use of a uniform opt-out logo at the behest of the Attorney General,¹⁴³ further adding to the complication for companies who wish to simply recycle their GDPR-specific procedures into compliance with the CCPA.¹⁴⁴ Importantly, businesses that maintain a separate homepage dedicated to California consumers can forego putting the Do Not Sell My Personal Information link on their homepage, as long as the link is available on the California-specific page.¹⁴⁵

Regarding the GDPR, consent provided by the data subject is one of six grounds that data collectors can point to for the lawful processing of personal data.¹⁴⁶ Consent of the data subject is defined in the GDPR as “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”¹⁴⁷ The ICO has stated that active opt-in boxes are required under the regulation¹⁴⁸ and that “any opt-out options are essentially the same as pre-ticked boxes, which are banned.”¹⁴⁹ Often, GDPR-compliant businesses will provide opt-in consent boxes in the form of “cookie notices” on webpages, that prompt users to click “Accept Cookies” or “I Understand” before the website collects or utilizes personal data.¹⁵⁰

141. CAL. CIV. CODE § 1798.135

142. *See id.*

143. *See Do Not Sell My Personal Information Link for California*, CLARIP, <https://www.clarip.com/data-privacy/do-not-sell-my-personal-information/>, (last visited Nov. 20, 2019).

144. Meyer, Farmer, Nara & Azim-Khan, *supra* note 119.

145. CAL. CIV. CODE § 1798.135, *supra* note 141.

146. GDPR, *supra* note 62, art. 6.

147. *Id.* art. 4(11).

148. *Consultation: GDPR consent guidance*, INFO. COMM’N OFF. (Mar. 2, 2017), <https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>.

149. *Id.*

150. *See generally Cookie consent banner – what is it and how do I make it GDPR compliant?*, COOKIEBOT, <https://www.cookiebot.com/en/cookie-banner/>, (last visited Dec. 1, 2019).

Often included in a “cookie notice” is a link to a GDPR-compliant privacy policy detailing the specific purposes for which a data subject’s personal data will be used for.¹⁵¹

Therefore, consumer consent must be generated in a different manner under the GDPR than under the CCPA, an inconvenience for international businesses. Businesses can choose to adopt the highest common denominator between the two regulations’ requirements,¹⁵² but the CCPA’s requisite “Do Not Sell My Personal Information” link will still need to be visible, which contravenes the required opt-in language of the GDPR.¹⁵³ Further, the CCPA’s requirements signal the need for an additional privacy policy to be included on a company’s website, or at the very least a revamp of the existing GDPR-compliant policy to encompass the CCPA’s standards. Often, this onerous task requires not only the attention of internal resources, but also the hiring of outside legal counsel to ensure compliance. This task would become increasingly more burdensome as more states enact their own specific data privacy regulation passed into law.

It is conceivable that companies may turn to geo-targeting in order to comply with both the GDPR and the CCPA’s homepage opt-in and opt-out requirements.¹⁵⁴ This brings to light the inherent complications of web design solutions, such as geo-targeting different sets of webpages to users in California and users within the EU, with more targeting responsibilities to come as an increasing number of jurisdictions set forth their own data privacy regulations.¹⁵⁵

Geo-targeting is a method made popular by the digital advertising community, in which advertisers utilize user IP addresses to identify consumer location before serving an advertisement tailor-made for that specified geographic area.¹⁵⁶ For ex-

151. *See id.*

152. Meyer, Farmer, Nara & Azim-Khan, *supra* note 119.

153. GDPR, *supra* note 62, art. 7.

154. *See* Kyle Pucko, *How to Easily Geotarget Your Existing Website*, GEOFLI, (June 3, 2018), <https://www.geofli.com/blog/geotargeting-your-website-easily/> (explaining that geo-targeting allows companies to change and replace content on their existing website based on their website visitor’s location.)

155. Serrato & Ross, *supra* note 136.

156. *See generally* Lauryn Chamberlain, *GeoMarketing 101: What Is Geotargeting?*, GEOMARKETING (Mar. 31, 2016), <https://geomarketing.com/geomarketing-101-what-is-geo-targeting>.

ample, if a consumer in New York visited ESPN.com, they may be served with an advertisement for a New York-based Honda dealer, while a consumer who visits the website from Los Angeles will be served with an advertisement for a Los Angeles-based Honda dealer. The geo-targeting is done on the back end of ESPN's webpage in accordance with its advertising partners' preferences.¹⁵⁷ Alternatively, many advertisers can target or "block" certain geographic locations by uploading a list of approved zip codes, regions, counties or countries to their ad server.¹⁵⁸ Similar to the targeting of advertisements, online businesses now have the capability to geo-target specific web pages to consumers based on location.¹⁵⁹

In implementing geo-targeting solutions, it can be deduced that companies will not want to block specific locations that would be detrimental to their brand's international accessibility and appeal.¹⁶⁰ Therefore, companies will likely be forced to target users by IP address. In other words, companies can geo-target one specific landing page to consumers who are shown to be based in California according to those users' IP addresses.¹⁶¹ Another dedicated landing page will be served to consumers whose IP addresses show that they are located within the EU. The two landing pages would be designed to comply with the

157. *See id.*

158. *See generally*, Google Ads Help, *Exclude ads from geographic locations*, GOOGLE, <https://support.google.com/google-ads/answer/1722040>, (last visited December 5, 2019).

159. *See generally* Drew Allen, *Why You Should be Building Location Pages*, BKA CONTENT (July 15, 2020), <https://www.bkacontent.com/building-geo-landing-pages/>.

160. *See* Hui Chu Chen & Robert D. Green, *Marketing Mix and Branding: Competitive Hypermarket Strategies*, INT'L. J. MGM'T. & MKTG. RES., 19 (2009) (explaining that customer-based brand equity is the deferential effect of brand knowledge on consumer response to the marketing of the brand. Brand knowledge includes brand awareness and brand image. "Customer-based brand equity occurs when the customer is aware of the brand and holds some favorable, strong, and unique brand associations in memory.").

161. *See generally* Sean Callahan, *Forget Click-Through Rate: 10 Metrics to Track for Display Advertising*, ADEXCHANGER (Oct. 14, 2013), <https://adexchanger.com/ad-exchange-news/forget-click-through-rate-10-metrics-to-track-for-display-advertising/> (Inherently, two sets of landing pages will lead to two different display advertisement being shown to users (i.e. one in the California and one to users outside of California). Advertisers will want to collect key metrics for both advertisements, and so this will require twice the workload). *Id.*

CCPA's requirements for opting-out and the GDPR's requirements for opting-in, respectively.

In a vacuum, this approach may appear to be straightforward and simplified. Despite its apparent ease, there are a host of issues that come to light when delving into the intricacies of the geo-targeting solution. From an advertising perspective, companies will now have to keep track of online metrics and user preferences for two separate landing pages. For example, ad traffickers within each company will now have to upload two sets of all advertising materials—tracking pixels, creative, layered targeting, etc.—to their advertising server.¹⁶² Further, advertisers may spend less on advertising partnerships with companies who have an international presence and are subject to the CCPA and GDPR because of these inefficiencies.¹⁶³ The number of unique visitors per page will be drastically decreased based on the dual-page approach, and the targeted advertisements to California and the EU may not be the preference of the advertiser.

To combat the potential for losing advertising dollars, websites may decide to employ an even more cumbersome three-page approach; one for the EU, one for California, and one main page for locations unaffected by data regulations. With the potential for more data regulations forthcoming, the picture begins to come into focus as to how much of an albatross geo-targeting webpages and constructing numerous regulation-specific privacy policies will undoubtedly be for international companies.

It is also important to note that while IP addresses are considered protected personal information under both the GDPR and CCPA, businesses may be able to find loopholes in the realm of geo-targeting based on IP addresses.¹⁶⁴ IP addresses

162. See generally, *Ad Trafficking 101*, ADOPSWORLD, <http://www.adopsworld.com/adtraffic.php>, (last visited Nov. 16, 2019).

163. Callahan, *supra* note 161 (key metrics throughout the sales funnel include volume of visitor-specific metrics – i.e. direct website traffic, cost per new website visitor, total leads, etc. A lack of visitors would decrease a website's ability to show a return on investment, thus decreasing the likelihood of retaining valuable advertising partnerships).

164. See David A. Zetoony, *Privacy FAQs: Is an IP Address considered "personal information" under the CCPA?*, BRYANT CAVE LEIGHTON PAISNER (Apr. 19, 2019), <https://www.bclplaw.com/en-US/thought-leadership/privacy-faqs-is-an-ip-address-considered-personal-information.html> (analyzing the various scenarios under which an IP address may be considered personal information).

are not necessarily stored in a website's records, and thus are not "collected" under both the CCPA¹⁶⁵ and the GDPR¹⁶⁶. This ambiguity is certain to lead to litigation down the road,¹⁶⁷ and the necessity for geo-targeted websites due to the contrasting requirements set forth by the GDPR and CCPA only adds to that likelihood.

III. THE IMPLEMENTATION OF AN INTERNATIONAL FRAMEWORK

Turning to a solution for this siloed approach to data privacy regulation, the most prudent course of action resides in the establishment of one consistent international framework. Throughout this section, the recent developments in global patchwork legislation will be discussed, and the precedents for a singular international pact will be analyzed. Finally, the tenets of the International Data Privacy Agreement will be introduced as a viable solution given the multi-jurisdictional and transnational nature of the Internet.

A. Further Developments to the Patchwork Approach

As has been repeated time and again in this Note, the current patchwork approach to data privacy regulation on the Internet is an unworkable, inefficient, and burdensome standard for businesses to comply with. While the CCPA and the GDPR are the two current headline-grabbing regulations, this burden is being compounded as other countries begin to consider and enact their own data privacy regulations since the GDPR was passed into legislation.¹⁶⁸ While there may be commonalities in

under the CCPA and GDPR. "Static" IP addresses, or IP addresses belonging to a specific device, are more capable of linking personal information to a user and therefore are likely to be considered "personal information" under both regulations. In contrast, a "dynamic" IP address is assigned by a network's servers each time a computer or other device connects to it, and thus changes over time. Therefore, dynamic IP addresses are less capable of identifying a user and are less likely to be considered personal information.).

165. CAL. CIV. CODE §1798.130(a)(3)(B), *supra* note 120.

166. GDPR, *supra* note 62, art. 1.

167. See *IP Addresses and the GDPR*, DBS Interactive (Aug. 2, 2018), <https://www.dbswebsite.com/blog/ip-addresses-gdpr/> ("As GDPR discussions continue (and as inevitable future litigation arises), we'll get more details about how IP addresses fit within the context of personally-identifiable information protections.").

168. See *generally Data Protection Laws of the World*, DLA Piper (Jan. 14, 2019), <https://www.dlapiperdataprotection.com/?t=law&c=BR>.

both practice and theory between the regulations, the inefficiencies inherent in complying with a plethora of guidelines is an anchor on the health of international businesses.

Several of the world's largest economies have or will be enacting data privacy regulations of their own in the near future. Brazil, Australia, Japan, Canada, China and India have all either enacted or amended prior data privacy laws to address the threat of the mishandling of their citizens' cyber data.¹⁶⁹ A toxic combination consisting of the prominence of these countries, the attraction for foreign companies to conduct business within their borders, and the open nature of the internet will only add to the inherent nuisance of the data privacy regulation landscape.

Furthermore, in the absence of federal legislation,¹⁷⁰ a handful of American states aside from California have comprised their own frameworks for data privacy regulation for enactment in the near future.¹⁷¹ Nevada joined California as the only other state to pass legislation in 2019, as it enacted SB 220 on October 1st.¹⁷² Additionally, Illinois, Massachusetts, New Jersey and Pennsylvania all have outstanding bills on their legislature's floor, and enactment could be coming by the end of 2020.¹⁷³ Notably, the Massachusetts bill would include a private right of action for any violation of its terms and not just for data breaches, which was the standard set forth by the GDPR and CCPA.¹⁷⁴ To have that threat residing over interna-

169. See generally *GDPR: the emergence of a global standard on privacy?*, WORD FED'N OF ADVERTISERS (Nov. 28, 2018), <https://www.wfanet.org/news-centre/gdpr-the-emergence-of-a-global-standard-on-privacy/>.

170. McCabe, *supra* note 86.

171. See *New State Bills Inspired by the California Consumer Privacy Act May Re-appear Next Year*, Ropes & Gray LLP (Nov. 7, 2019), https://www.ropesgray.com/en/newsroom/alerts/2019/11/New-State-Bills-Inspired-by-the-California-Consumer-Privacy-Act-May-Re-Appear-Next-Year?utm_source=alert&utm_medium=email&utm_campaign=New-State-Bills-Inspired-by-the-California-Consumer-Privacy-Act-May-Re-Appear-Next-Year.

172. See *id.* ("The act requires operators of commercial websites or online services (not all businesses) to allow Nevada resident consumers the opportunity to opt-out of the "sale" of personal information about them. The Nevada statute defines "sale" more narrowly than the CCPA's broad definition. Under SB 220, "sale" only encompasses the exchange of information for "monetary consideration.").

173. See *id.*

174. See *id.*

tional companies who wish to conduct business with a top-ten U.S. media market¹⁷⁵ only adds to the burdens of the patchwork approach. Eleven other states introduced bills in 2019 but were not enacted at the time of this Note; those states include Hawaii, Louisiana, Maryland, New Mexico, New York, Rhode Island and Washington.¹⁷⁶

Suffice to say, the data privacy regulation landscape will soon look vastly different than it did when the GDPR first came into force in 2018. Once that time comes, businesses across the world will be forced to comply with a variety of regulations, unnecessarily burdening both their sweat equity and financial bottom lines. A singular uniform solution is needed.

B. Precedent for an International Agreement

When the WIPO was founded by the UN in 1967, it was seen as a unifying bridge between scattered agreements and jurisdictional divides pertaining to the increasingly transnational nature of intellectual property (IP).¹⁷⁷ Specifically, the WIPO sought to enforce cooperation stemming from agreements between parties to both the Paris & Berne Convention as well as other IP-related treaties between nations.¹⁷⁸ Today, the WIPO continues to adhere to the tenets of its founding, while also serving as a dispute resolution for Internet domain names through its Uniform Domain Name Dispute Resolution Policy (UDRP).¹⁷⁹ While domain names have a closer relation to IP than data privacy does,¹⁸⁰ the implementation of the UDRP by an international body such as the WIPO proves that global oversight of activities native to the Internet can be achieved.

175. *Top 100 Media Markets*, NEWS GENERATION, <https://newsgeneration.com/broadcast-resources/top-100-radio-markets/> (last visited Dec. 15, 2019).

176. Serrato & Ross, *supra* note 136.

177. *World Intellectual Property Organization*, ENCYC. BRITANNICA, <https://www.britannica.com/topic/World-Intellectual-Property-Organization> (last visited Dec. 20, 2019).

178. *Id.*

179. *Domain Names Dispute Resolution*, WORLD INTELL. PROP. ORG., <https://www.wipo.int/amc/en/domains/> (last visited Dec. 20, 2019).

180. See generally WIPO Domain Name Process, *The Management of Internet Names and Addresses: Intellectual Property Issues*, (Apr. 30, 1999), WORLD INTELL. PROP. ORG., <https://www.wipo.int/amc/en/processes/process1/report/finalreport.html>.

C. The International Data Privacy Agreement

The International Data Privacy Agreement (IDPA) would take a similar form, bridging an agreement between all member nations to set forth a uniform guideline to data privacy protection. The agreement's enforcement body would hand down penalties to violating businesses, while any legal recourse against a company for a data breach would take place in the appropriate home forum on the bases of jurisdiction and civil procedure.

The incentive for countries to join the IDPA is two-fold. The first angle is the citizen protection motivation. By joining the IDPA, governments can ensure that their citizens are being afforded the same heightened standard of privacy protection that they enjoy domestically across the world. For example, consider an online European business that processes the information of some California residents but does not fall within the scope of compliance of the CCPA.¹⁸¹ Under the current makeshift regime, it is possible that this business will escape liability for processing household information of California residents. Given the construction of the CCPA,¹⁸² it is doubtful this is the result preferred by the California state legislature, thus rendering their citizens susceptible to data privacy shortcomings.

Second, governments have the added incentive of assisting businesses within their borders in achieving their most optimal economic production, resulting in a boom to the domestic economy. Agreeing to one uniform data privacy regulation will help realize this end, as companies will conserve financial and human resources by not having to multiply their efforts for each country or state-specific regulation that comes to be enacted. Additionally, companies will garner a clear concept of notice, as opposed to attempting to adhere to a mixed-bag of regulatory oversight.

The approach to forming an organization or committee to enforce the agreement would not be without precedent, but even more importantly, the UN has already expanded its initiatives into the digital data arena with its Global Pulse initiative, a

181. See generally *A quick reference guide for CCPA compliance*, DELOITTE <https://www2.deloitte.com/us/en/pages/advisory/articles/ccpa-compliance-readiness.html> (explaining the benchmarks for compliance with the CCPA).

182. CAL. CIV. CODE § 1798.140, *supra* note 88 (the CCPA includes "household information" under personal information, as opposed to the narrower interpretation of personal information in the GDPR).

flagship innovation program of the UN Secretary-General on big data.¹⁸³ The program seeks to utilize big data in order to better understand the changes in human well-being by leveraging data to accelerate sustainable development and humanitarian action.¹⁸⁴ Further, the initiative aims to forge public-private data sharing partnerships or the sharing of a private company's data with the government.¹⁸⁵ Certainly, a transnational data privacy regulation enforced by the UN would not be a wholly unique concept given the governing body's current data-induced focus.

The three key divergent concepts that the IDPA would seek to unite under a comprehensive scheme are: (1) opt-out right as opposed to opt-in; (2) a concise definition of personal information precluding "household information;" and (3) a consumer's private right of action being reserved strictly for occurrences of data breaches.

The opt-in vs. opt-out notification that businesses must display on their webpages is perhaps the greatest operational difference between the GDPR and the CCPA,¹⁸⁶ and one solution must govern the IDPA. The IDPA will set forth a mandate that businesses must provide an opt-out right in a conspicuous link on each separate page that a user visits during his or her time spent on the website. The design must also provide a separate link to the company's IDPA privacy policy. In essence, the decision to implement an opt-out over an opt-in or cookie style banner provides consumers with a clear understanding as to how their data is being processed on the site. It eliminates the grey area inherent in many current cookie banners or opt-in requests. Additionally, it enables consumers to affirmatively disallow their data to be sold, as opposed to passively or mindlessly opting into cookie-sharing. Many consumers will opt-in to cookie sharing as opposed to challenging it or learning more

183. *About UN Global Pulse*, U.N. GLOBAL PULSE, <https://www.unglobalpulse.org/about-new> (last visited Dec. 20, 2019).

184. *Id.*

185. See Paula Forteza & Marianne Billard *Why data from companies should be a common good*, APOLITICAL (Oct. 1, 2019), https://apolitical.co/solution_article/why-companies-should-share-their-data-with-government/ (Discussing the benefits of sharing a private company's data with the government. "The main arguments for opening private data are that it will allow better public decision-making and it could trigger a new way to regulate big tech.")

186. Umhoefer & Shapiro, *supra* note 137.

about cookie sharing activities because of the time consuming process of clicking on a cookie banner, landing on a different page and reading through the subsequent information.¹⁸⁷

Importantly, the definition of “personal information” will have one universal meaning under the IDPA in order to better signal to businesses what information they must data map for and more efficiently protect. Some businesses might even choose to simply bypass the liability of an overly broad data pool and not collect specific pieces of information based on the requirements set forth by one blanket regulation. Specifically, “personal information” will take on the definition set forth in the GDPR. Under the GDPR’s standard, data subjects are identifiable “if they can be directly or indirectly identified, by reference to a name, identification number, location data, an online identifier, or one of several special characteristics which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons.”¹⁸⁸ By implementing the GDPR’s definition of personal information, a business’ focus is kept squarely on the user in question, as opposed to the windfall of information that would be deemed necessary to protect under the CCPA’s household information requirement.¹⁸⁹

Last, the IDPA will set a restriction on the private right of action for consumers to be applicable only in instances of data breaches. As explained above, it is a growing trend in the US for data privacy proposals to include the private right of action to extend to situations beyond redress for data breaches.¹⁹⁰ The sheer volume of liability that the alternative would encumber businesses with would be financially crippling and unjustifiable. A private right of action for a gross mishandling of data holds businesses accountable and provides harmed users with a direct source of recourse. Anything greater than that right for

187. See Rene van Bavel & Nuria Rodriguez-Priego, *Testing the Effect of the Cookie Banners on Behaviour*, E.U., at 11 (2016) <https://publications.jrc.ec.europa.eu/repository/bitstream/JRC103997/jrc103997.pdf> (showing that less than 10% of users in an experiment stated that they knew “a lot” about cookies, while 60% of the same user pool accepted cookie banners).

188. GDPR, *supra* note 62, art. 5.

189. CAL. CIV. CODE §1798.140, *supra* note 88.

190. *New State Bills Inspired by the California Consumer Privacy Act May Re-appear Next Year*, *supra* note 171.

consumers opens up businesses to an unnecessary amount of liability.

CONCLUSION

To conclude, it is imperative that governments avoid a patchwork approach to data privacy regulation. The preference for separate regulations with even the slightest divergent operational effect unduly burdens online businesses. This encumbrance has been showcased through the issues stemming from dual GDPR and CCPA compliance, with even more conflicting regulations on the horizon. Given the transnational nature of the Internet and the ubiquitous cyber presence of businesses worldwide, a singular international agreement to data privacy is the most prudent and economically efficient approach towards combating the lack of transparency in the handling of consumer data.

Scott Resnick *

* B.A., State University of New York at Buffalo (2013); J.D. Brooklyn Law School (Expected 2021); Notes Editor, *Brooklyn Journal of International Law* (2020-2021). Thank you to the Journal staff for all of their diligence and dedication throughout the note writing process. Your efforts made this an incredibly rewarding adventure. I would like to thank my parents, Fern and Richard Resnick, for their unwavering support over the course of the last several years – starting from my decision to change careers and take the LSAT, to the publication of this note, and throughout the entirety of law school. Your backing has always and will always mean the world to me. A very special thank you is owed to my incredible significant other, Kelly Piccirullo, for her patience, understanding, and encouragement throughout all of the late nights and weekend afternoons dedicated to this note. Thank you for putting up with a multitude of obscure acronyms over the last year-plus. I thoroughly enjoyed researching and writing this note, as it became an interplay between my prior career in the advertising technology industry and my legal education. The GDPR was a focal point in my previous work throughout its implementation – I was continually required to educate clients on the resulting impact that the GDPR would have on their businesses from an advertising technology standpoint. This non-legal background has enabled me to cultivate a unique perspective on the data privacy compliance battlefield. To see my experience come full circle from those early days of the GDPR to publishing a legal note on the current landscape of the data privacy regulatory scheme is truly a testament to the expansive scope of the data privacy space. It is a rapidly emerging area of law, and I am exceedingly enthusiastic about sharing my insights and research with the larger academic and legal community. All errors or omissions are my own.