Suffolk Journal of Trial and Appellate Advocacy

Volume 26 | Issue 1 Article 8

1-1-2021

Until Data Does Us Part—The Call for a Federal Analog to the California Consumer Privacy Act: A Litigation Perspective

Brendan Chaisson
Suffolk University Law School

UNTIL DATA DOES US PART—THE CALL FOR A FEDERAL ANALOG TO THE CALIFORNIA CONSUMER PRIVACY ACT: A LITIGATION PERSPECTIVE

"The world's most valuable resource is no longer oil, but data."[1]

I. INTRODUCTION

American consumers often receive emails from companies whom they have transacted with.[2] Among the seemingly endless stream of coupons and brand announcements, consumers may encounter a message that takes on a more serious tone: a company—entrusted with customers' Personally Identifiable Information ("PII")—has failed to adequately protect that information from hackers and cyber-criminals.[3]

On September 7, 2017, this message became an unfortunate reality for roughly 44% of Americans as Equifax, a credit reporting company, suffered a cyberattack so large that the company was compelled to notify citizens of the data breach.[4] The breach—likely orchestrated by high-ranking members of the Chinese military—compromised 145 million Americans' PII.[5] While no evidence existed that the hackers had misused consumers'

---

[1] *See Internet Service Providers: Customer Privacy*, S. JUDICIARY COMM., 2017-18-A.B. 375 2017-18 Sess., Background (Cal. June 25, 2018).

[2] *See* Jordan Elias, *Course Correction—Data Breach as Invasion of Privacy*, 69 BAYLOR L. REV. 574, 574 (2017) (suggesting consumers typically receive notice of data breaches via email).

[3] *See* Clara Kim, Note, *Granting Standing in Data Breach Cases: The Seventh Circuit Paves the Way Towards a Solution to the Increasingly Pervasive Data Breach Problem*, 2016 COLUM. BUS. L. REV. 544, 546 (2016) (describing increasingly prevalent phenomenon of data breaches). A data breach is "the loss, theft, or other unauthorized access . . . to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data." *Id.* (quoting 38 U.S.C. § 5727 (2012)).

[4] *See* Elizabeth Weise, *A Timeline of Events Surrounding the Equifax Data Breach,* USA TODAY (Oct. 3, 2017, 2:46 PM), https://www.usatoday.com/story/tech/2017/09/26/timeline-events-surrounding-equifax-data-breach/703691001/ (providing timeline of Equifax's notice to consumers regarding breach); *Equifax Announces Cybersecurity Incident Involving Consumer Information*, EQUIFAX (Sep. 7, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628 (describing information hacked). Information accessed "primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers." Equifax*, supra* note 4.

[5] *See* Department of Justice Office of Public Affairs, *Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax*, U.S. DEP'T. OF JUSTICE (Feb. 10, 2020), https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking (an-

personal information at the time consumers were notified, many Americans were left with the same question after their private information was compromised: what now?[6] In fact, consumers nationwide have increasingly asked this question as large-scale data breaches continue to infect the consumer marketplace.[7] In Equifax's case, the answer to this question relied on—as it often has in mass data breaches—the statutorily-prescribed enforcement powers of the Federal Trade Commission ("FTC"), a government agency designed to protect consumers nationwide against deceptive and unfair business practices.[8] Using its broad authority under Section 5 of the FTC Act, the FTC filed a complaint in federal district court seeking an injunction against Equifax, which ultimately resulted in the largest settlement for a data breach in United States' history.[9] In total, the parties settled for $650 million, with $300 million reserved for a "Consumer Fund" to settle the multidistrict litigation brought on behalf of the individuals affected by the breach.[10] While this judicial resolution was an ostensible success, consumers were still faced with a different set of challenges, which included increasing credit monitoring to police their exposed PII and finding an

---

nouncing indictments of four members of Chinese military). "[Their actions were] a deliberate and sweeping intrusion into the private information of the American people . . . ." *Id.*

[6] *See* Elias, *supra* note 2, at 575 (acknowledging that news of Equifax breach left many "deeply rattled").

[7] *See id*. (noting that immediate fallout of data breaches results in "anxiety, embarrassment, and distress" for consumers); *see also* Kim, *supra* note 3, at 548-49 (listing recent large-scale data breaches).

[8] *See* QUEMARS S. AHMED, ET. AL., CALIFORNIA ANTITRUST AND UNFAIR COMPETITION LAW: PRIVACY ENFORCEMENT BY THE FTC, 1 CA ANTITRUST AND UNFAIR COMPETITION L. § 26.17(B)(1) (3d ed. 2019) (articulating FTC enforcement powers under FTC Act). In short:

> [T]he FTC has used its Section 5 authority to investigate and file complaints for privacy and data security violations . . . [b]roadly speaking, FTC investigations may lead to one or several of the following outcomes: (1) the agency's decision to close the investigation, (2) a settlement between the FTC and the target of the investigation, (3) the agency's filing of an administrative complaint, or (4) the agency's filing of a complaint in federal district court.

Id.

[9] *See Federal Trade Comm'n v. Equifax Inc.*, No. 1:19-cv-03297-TWT (Thrash, J., Stipulated Order for Permanent Injunction and Monetary Judgment) (N.D. Ga. July 23, 2019) (ordering settlement of FTC claims against Equifax and establishing "Consumer Fund" to pay affected consumers).

[10] *See id.* at 31 ("An amount no less than Three Hundred Million Dollars . . . must be used and administered . . . for the exclusive purpose of providing restitution and redress to Affected Consumers"); Stacy Cowley, *Equifax to Pay at Least $650 Million in Largest-Ever Data Breach Settlement*, N.Y. TIMES (July 22, 2019), https://www.nytimes.com/2019/07/22/business/equifax-settlement.html (indicating final size of settlement may change depending on several conditions applied in order).

effective way to actually collect damages from Equifax.[11] As it turned out, the FTC settlement did not account for such a large number of consumers seeking cash compensation, which meant that the amount set aside in the "Consumer Fund" was grossly underestimated; thus, a deadline was given to consumers to either file more paperwork to receive their payout or opt for a non-cash settlement.[12]

The Equifax settlement is illustrative of a common theme in data breach litigation: while government regulations may cause businesses to enhance their cybersecurity regimes, the consumer-plaintiffs harmed by data breaches face significant impediments in attempting to redress their injuries through judicial process.[13] Enabling consumer access to federal courts has become a weighty concern in the context of data breaches, with no current consensus regarding *how* the courts or legislature should address the issue.[14] The California legislature, however, has adopted a seemingly common-sense method to confer standing to individual consumers affected by data breaches.[15] With the passage of the California Consumer Privacy Act ("CCPA")[16], California residents now have a private right of action against certain businesses if their "nonencrypted and nonredacted information . . . is subject to an unauthorized access and exfiltration, theft, or

---

[11] *See* Megan Leonhardt, *If You Want to Claim $125 from the Equifax Data Breach, You Have More Work To Do*, CNBC (Sep. 9, 2019, 11:11 AM), https://www.cnbc.com/2019/09/09/equifax-settlement-you-need-to-update-your-claim-to-get-125.html (outlining process for individual consumers seeking cash compensation).

[12] *See id.* ("[C]onsumers who filed for the $125 cash payout were sent an email with the subject line: 'Your Equifax Claim: You Need to Act by October 15, 2019 or Your Claim for Alternative Compensation Will Be Denied.'"). The FTC also urged consumers to pick free credit monitoring over the cash payout as it came with identity theft insurance among other benefits. *Id.*

[13] *See* Kim, *supra* note 3, at 547 (noting that consumers' class action lawsuits to redress "increasingly common occurrence of data breaches" generally fail); Elias, *supra* note 2, at 576-77 (asking federal courts to confer standing by applying common-law privacy torts in data breach cases).

[14] *See* Kim, *supra* note 3 ("[T]he current state of the law cannot fully address the complicated issues that arise from data breach incidents. The existing regulations operate in a piecemeal manner and do not adequately address the situation."); *2018 Security Breach Legislation*, NAT'L CONF. OF STATE LEGISLATURES (Feb. 8, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/2018-security-breach-legislation.aspx (noting that all fifty state legislatures have addressed security breaches through some type of legislation); *accord* U.S. GOV'T ACCOUNTABILITY OFF., GAO 19-52, INTERNET PRIVACY: ADDITIONAL FEDERAL AUTHORITY COULD ENHANCE CONSUMER PROTECTION AND PROVIDE FLEXIBILITY 6 (2019). "No comprehensive federal privacy law governs the collection, use, and sale or other disclosure of personal information by private-sector companies in the United States." U.S. Gov't Accountability Off., *supra* note 14.

[15] *See* Mike Quartararo, *Challenges of the California Consumer Privacy Act*, ABOVE THE LAW (Oct. 29, 2019, 5:46 PM), https://abovethelaw.com/2019/10/challenges-of-the-california-consumer-privacy-act/ (noting CCPA creates private right of action to consumers). "Any consumer may bring an action [for statutory damages] under the law." *Id.*

[16] *See* CAL. CIV. CODE §§ 1798.100-199 (2020).

disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices. . . ."[17]

This Note will focus on the implementation of the CCPA and its inevitable effect on data breach class actions nationwide.[18] With California residents' claims being distinguished from the other subclasses in multidistrict litigation, it is likely that those suffering from the same data breaches will be received with stark distinctions in federal courts.[19] A brief analysis of prior data breach class actions across different circuits will further illustrate the burden that class action plaintiffs outside of California must overcome to recover damages.[20] Throughout this Note, this author will analyze the current state of data breach class actions involving both class plaintiffs and the government (FTC).[21] This Note will then forecast the outcome of conflicts arising out of favored CCPA class treatment, ultimately leading to the conclusion that a comprehensive, federal scheme of privacy legislation

---

[17] CAL. CIV. CODE § 1798.150(a)(1) (2020); *see also* Dominique Shelton Leipzig et al., *The California Consumer Privacy Act*, 5 PRATT'S PRIV. AND CYBERSEC. L. REP. 39, 39 (2019) (noting that CCPA "goes well beyond" most comprehensive data privacy regulations).

[18] *See In re* Anthem, Inc. Data Breach Litig., 327 F.R.D. 299, 311 (N.D. Cal. 2018), *appeal dismissed sub nom.* No. 18-16866, 2018 WL 7890391 (9th Cir. 2018) (finding differences in state law central to class certification under Federal Rules of Civil Procedure). According to the Federal Rules of Civil Procedure, "plaintiffs must show 'that the questions of law or fact common to class members predominate over any questions affecting only individual class members.'" *Id.* (quoting FED. R. CIV. P. 23(b)(3)). "Courts should examine differences in underlying state law as part of the predominance analysis because 'in a multistate class action, variations in state law may swamp any common issues and defeat predominance.'" *Id.* at 313 (internal quotations omitted).

[19] *See In re* Hyundai & Kia Fuel Econ. Litig., 881 F.3d 679, 702-03 (9th Cir. 2018), *reh'g en banc granted sub nom.* 897 F.3d 1003 (9th Cir. 2018), and on *reh'g en banc*, 926 F.3d 539 (9th Cir. 2019) (finding district court erred in certifying nationwide consumer class before conducting choice of law analysis).

[20] *See generally* Kim, *supra* note 3, at 561-73 (acknowledging discrepancies in approaching standing for data breach class actions in district and circuit courts); *see also* Elias, *supra* note 2, at 575 (suggesting no true precedent exists on federal level to analyze standing in data breach actions).

[21] *See In re* Zappos.com, Inc., 888 F.3d 1020, 1023 (9th Cir. 2018), *cert. denied sub nom.* 139 S. Ct. 1373 (2019) (finding plaintiffs in putative data breach action "sufficiently alleged [Article III] standing based on the risk of identity theft"); *accord* Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 696 (7th Cir. 2015) (reaching same finding that plaintiffs' injuries satisfied Article III standing requirement). *Contra* Anderson v. Hannaford Bros. Co., 659 F.3d 151, 154 (1st Cir. 2011) (dismissing class plaintiffs' claims in data breach action where future harm was not foreseeable); Rudolph v. Hudson's Bay Co., No. 18-cv-8472, 2019 U.S. Dist. LEXIS 77665, *4-5 (S.D.N.Y 2019) (finding plaintiff failed to allege "a substantial risk of future injury" but conferring Article III standing on other grounds). "A plaintiff has Article III standing if she plausibly alleges future injury, provided that 'the threatened injury is certainly impending, or there is a substantial risk that the harm will occur.'" *Rudolph*, 2019 U.S. Dist. LEXIS at *11 (quoting Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014)) (internal quotations omitted); *see also* U.S. Gov't Accountability Off., *supra* note 14, at 44-51 (outlining FTC internet privacy enforcement actions).

is necessary to provide all American consumers the same rights to recover monetary damages in data breach class actions.[22]

II. HISTORY

The collection of consumer data has rapidly become one of the most pressing privacy issues in our legal system.[23] The proliferation of the digital world has far outpaced the government's responses to how businesses must handle consumer data, and there is still little to no comprehensive regulatory scheme in place.[24] In 2006, without a federal privacy law, "the FTC created the Division of Privacy and Identity Protection ("DPIP") to protect consumer data."[25] Since adopting this leadership role, the FTC has brought enforcement actions against companies "using its general authority under section 5 of the FTC Act. . . [which] prohibits 'unfair or deceptive acts or practices in or affecting commerce.'"[26] As demonstrated in Equifax's case, this practice may be effective in ensuring corporate compliance, but it fails to adequately redress individual consumer injuries stem-

---

[22] *See* U.S. Gov't Accountability Off., *supra* note 14, at 38 (recommending that Congress develop comprehensive legislation on internet privacy to enhance consumer protection); Kim, *supra* note 3, at 591-93 (calling for overarching federal regulatory framework to solve data breach problem).

[23] *See* Internet Service Providers, *supra* note 1 ("Currently, everything from toasters and baby dolls to televisions are connected to the Internet, gathering and using a wide range of information. This technology has limitless possibilities."); *see also* U.S. Gov't Accountability Off., *supra* note 14, at 5-7 (noting increased prevalence of internet-connected devices).

> A nationwide survey that the U.S. Census Bureau conducted . . . in 2017 found that 78 percent of Americans ages 3 and older used the Internet . . . . [A]s new and more devices become connected, they increase not only the opportunities for security and privacy breaches, but also the scale and scope of any resulting consequences.

U.S. Gov't Accountability Off., *supra* note 14, at 5-7; Matt Burgess, *What is GDPR? The Summary Guide to GDPR Compliance in the UK*, WIRED (Mar. 24, 2020), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018 (noting that "previous data protection rules across Europe" could not keep up with rapid technological changes).

[24] *See* U.S. Gov't Accountability Off., *supra* note 14, at 6 (stating that no "comprehensive federal privacy law governs the . . . disclosure of personal information by private-sector companies in the United States"); *The General Data Protection Regulation ("GDPR")*, 6 COMPUT. LAW §51.04 (2019) (noting that European Union's privacy law only took effect in May 2018).

[25] *See* Kim, *supra* note 3, at 555 (noting FTC is only one of major federal agencies giving guidance regarding data security preparedness). *But see* U.S. Gov't Accountability Off., *supra* note 14, at 9 (stating that FTC "currently has the lead in overseeing Internet privacy at federal level").

[26] *See* U.S. Gov't Accountability Off., *supra* note 14, at 9 (describing FTC's role in federal privacy enforcement); *see also* Kim, *supra* note 3, at 546-47 (noting that existing federal and state laws operate in "piecemeal manner" to inadequately address data breaches).

ming from data breaches.[27] Similarly, consumer class actions involving data breaches have increasingly been thwarted by federal judges at both the motion to dismiss and class certification stages of litigation.[28]

Still, from both a compliance and individual rights standpoint, global privacy law entered a new age in 2018 when the European Union adopted the General Data Protection Regulation ("GDPR") as the first attempt to create a strict, regulatory scheme that enumerates and protects consumers' rights to their personal data shared with companies.[29] The GDPR "declares the 'right to protection of personal data' to be a fundamental right held by all natural persons."[30] In its ninety-nine articles, the GDPR sets out consumers' rights and the corresponding obligations of companies "controlling" their personal information.[31] Under the GDPR, consumers are provided with eight rights, with perhaps the most prominent being the right to be informed—that is, a company must tell individuals "what data is being collected, how it's being used, how long it will be kept and whether it will be shared with any third parties."[32] Further, individuals protected by the GDPR maintain the "right to be forgotten," which allows them to request that companies erase their personal data in certain circum-

---

[27] *See* Leonhardt, *supra* note 11 (describing discordant process for consumers seeking to reap benefits of FTC data breach enforcement actions); *see generally* U.S. Gov't Accountability Off., *supra* note 14, at 10 n. 24 (noting that FTC cannot impose civil penalties unless business has violated FTC order, statute, or rule "that confers civil penalty authority"); Kim, *supra* note 3, at 546-47 (describing different statutes that contribute to piecemeal federal privacy enforcement).

[28] *See* Gerald E. Arth et al., Practice Note, *Non-Statutory Grounds for Challenging Class Actions: Standing and Ascertainability*, THOMSON REUTERS PRAC. LAW (2019) (discussing defendant-friendly shift in class actions).

> For many years, it seemed as though courts considering motions for class certification were issuing "rubber stamp" decisions allowing proposed class actions to proceed. However, various developments in the case law seemingly have made it easier for defendants to deter class actions both before and at the certification stage.

Id.; *see also* Elias, *supra* note 2, at 578-79 (discussing various circuit court approaches to data breach claims). Courts have taken approaches that involve state consumer protection acts, emotional distress, actual misuse of data by hackers, and claims for negligence and breach of implied contract. Elias, *supra* note 2, at 578-79.

[29] *See* Mark Peasley, Note, *It's Time for an American (Data Protection) Revolution*, 52 AKRON L. REV. 911, 917 (2018) (stating that GDPR is "much more inclusive and comprehensive than U.S. law and reaches each and every entity that handles [EU] citizen data whether located in the [EU] or abroad.")

[30] *See id.* (analyzing GDPR).

[31] *See* Burgess, *supra* note 23 (summarizing GDPR articles).

[32] *See* Alice Baker, *The GDPR: Consumer Rights for your Personal Data*, IT GOVERNANCE (Aug. 18, 2020), https://www.itgovernance.eu/blog/en/the-gdpr-consumer-rights-for-your-personal-data (articulating all eight consumer rights granted in GDPR).

stances.[33] The GDPR's enactment put many American companies conducting business in Europe on notice and forced businesses to update their internal cybersecurity regimes to avoid hefty fines for non-compliance.[34]

A. The California Consumer Privacy Act (CCPA)

Proposed as a ballot initiative in 2018, the California Consumer Privacy Act sought to address the problem of the United States' lackluster data privacy policies and drew from our European counterparts in the adoption of a comprehensive set of regulations similar to the GDPR.[35] The national impact of this legislation is noteworthy as California is the most populous state in the nation, which means that California citizens likely comprise a large portion of the plaintiffs suffering from unauthorized disclosure and use of their PII in large-scale breaches.[36] To combat this harm, the CCPA draws from the GDPR by providing "California consumers with eight new privacy rights and [imposing] eight corresponding as well as three independent obligations on businesses processing California consumers' [PII]."[37] The CCPA, however, goes beyond the GDPR in some respects as well.[38]

---

[33] *See id.* (noting circumstances where data is no longer necessary, unlawfully processed, or individual withdraws consent).

[34] *See GDPR Compliance Checklist for US Companies*, GDPR.EU, https://gdpr.eu/compliance-checklist-us-companies/ (last visited Nov. 25, 2019) (describing "extra-territorial" nature of GDPR and consequences for U.S. companies' failure to comply).

[35] *See* Internet Service Providers, *supra* note 1 (advocating for enactment of CCPA).

> This November 2018 ballot measure says: You have the right to tell a business not to share or sell your personal information . . . . You have the right to know where and to whom your data is being sold or disclosed . . . . You have the right to protections against businesses who do not uphold the value of your privacy . . . . It's your personal information. Take back control!

Id.; *see also* Leipzig et al., *supra* note 17 (explaining to companies that "[i]f you've achieved compliance with the GDPR, you are well on your way to achieving CCPA compliance.")

[36] *See* Leipzig et al., *supra* note 17 (noting that CCPA arose out of "growing concern for the volume of data collected about California Consumers").

[37] *See id.* at 40 (explaining California may request from businesses what PII is collected and sent to third parties).

[38] *See* CAL. CIV. CODE § 1798.140 (2020); Leipzig et al., *supra* note 17, at 40 (stating that "the CCPA expands definition of [PII] beyond the GDPR and well beyond that of current U.S. privacy law."). The CCPA defines PII as:

> [I]nformation that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer *or household* (emphasis added). The definition also includes personal identifiers, IP addresses, commercial information, records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or

In addressing the unique, American issue of standing in federal courts for data breach class actions, the CCPA provides California residents with a statutory right to damages if they are subject to "an unauthorized access, exfiltration, theft, or disclosure as a result of the business' failure to implement and maintain reasonable security procedures and practices."[39] Under this right, California consumers may: (1) recover damages not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater; (2) seek injunctive or declaratory relief; and/or (3) any other relief the court deems proper.[40] This fast-track to the courtroom comes with some caveats, however, as "[p]rior to initiating any action, a consumer must give the business 30 days' written notice identifying the specific CCPA provisions that have been or are being violated."[41] Still, this provision adds to a Californian plaintiff's arsenal in federal court because, if a business is notified and does not properly redress the injuries suffered, a plaintiff's future risk of harm will only increase without remedial measures.[42] Thus, the CCPA's private right of action has properly set the stage for a new era of data breach jurisprudence with federal courts at the forefront of the debate over who may join CCPA subclasses in court.[43]

B. Nationwide Data Breach Class Actions

Prior to the CCPA's enactment, the Ninth Circuit, in which California lies, pioneered a new, plaintiff-friendly era of standing in data breach class actions.[44] For standing purposes, the Ninth Circuit, along with the

---

> tendencies; internet or other electronic network activity information, professional or employment-related information; or any consumer profile.

Leipzig et al., *supra* note 17, at 41 (citing CAL. CIV. CODE § 1798.140(o) (2020)) (emphasis in original).

[39] *See* CAL. CIV. CODE § 1798.150(a)(1) (2020); *see also* Elias, *supra* note 2, at 574-76 (acknowledging problems in data breach litigation include failure to address "hierarchy of personal information" and what "injuries" are compensable).

[40] *See* CAL. CIV. CODE § 1798.150(a)(1) (2020) (establishing remedies available to consumers in data breach class actions).

[41] *See* CAL. CIV. CODE § 1798.150(b) (2020); *see also* Leipzig et al., *supra* note 17, at 49 (noting that class wide statutory actions cannot commence if violation is cured within thirty days).

[42] *See* Kim, *supra* note 3, at 590 (noting "Ninth Circuit has historically followed" liberal approach of granting standing based on risk of future harm). By contrast, more conservative circuits grant standing based on current injury-in-fact. *Id.*

[43] *See generally In re* Anthem, Inc. Data Breach Litig., 327 F.R.D. 299, 317 (N.D. Cal. 2018) (stating that "[d]ata-breach litigation is in its infancy with threshold issues still playing out in the courts.")

[44] *See In re* Zappos.com, Inc., 888 F.3d 1020, 1023 (9th Cir. 2018) (embracing prior Ninth Circuit decision that conferred standing based on future risk of identity theft). "We reject Zap-

Seventh Circuit, set the legal standard for "injury in fact" as the increased risk of future harm stemming from consumers' compromised PII—a decidedly low threshold compared to other federal circuit courts, and perhaps even the Supreme Court of the United States.[45] These distinctions among courts are significant as the sheer magnitude of mass data breaches almost guarantees that many class action lawsuits will be brought against the same defendant across varying judicial districts.[46] Accordingly, it is common for the Judicial Panel on Multidistrict Litigation ("JPML")—which acts under its statutory power to determine whether a single federal district court should hear the pretrial proceedings of the case—to consider these actions for consolidation.[47] This forum selection is perhaps the most important phase for both plaintiffs and defendants, as it can be the difference between dismissal and a successful claim, and therefore serves as a proper lens to evaluate data breach class actions in a post-CCPA world.[48]

With a multitude of state and federal claims canvassing plaintiffs' complaints, the JPML, along with federal district courts, must establish a standard for analyzing how the laws should be applied on a case-by-case basis.[49] Substantively, the transferee court must apply the law of each transferor state and circuit.[50] Procedurally, however, the courts are bound to the Federal Rules of Civil Procedure, which include class certification

---

po's argument that *Krottner* is no longer good law after *Clapper* [2013 Supreme Court decision analyzing standing requirements], and hold that, under *Krottner*, [p]laintffs have sufficiently alleged standing based on risk of identity theft." *Id.*

[45] *Compare* sources cited *supra* note 20 (comparing Ninth Circuit rationale to that of other courts), *with* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408-12 (2013) (discussing contemporary Supreme Court view on Article III standing).

[46] *See generally* Caroline Spiezio, *MDL Watch: Consolidation Sought in Financial Services Data Breach Litigation*, REUTERS LEGAL (September 25, 2019, 9:19 PM), https://1.next.westlaw.com/Document/I731f0da0dff411e998a5af8680d02462/View/FullText.html?transitionType=SearchItem&contextData=(sc.Category)&firstPage=true&bhcp=1&CobaltRefresh=44488 (summarizing recent data breach class actions to be heard for consolidation before JPML).

[47] *See* 28 U.S.C. § 1407 (1968) (stating that decisions to transfer should be made for convenience of both parties and witnesses to "promote the just and efficient conduct of such actions").

[48] *See* sources cited *supra* note 20 (noting differences in standing analysis among federal circuits).

[49] *See In re* Equifax, Inc., Customer Data Sec. Breach Litig., 289 F. Supp. 3d 1322, 1325 (J.P.M.L. 2017) (rejecting plaintiffs' argument that circuit split regarding Article III standing for data breaches precludes consolidation); *see also In re* Air Crash Disaster at Boston, Massachusetts on July 31, 1973, 399 F. Supp. 1106, 1108 (D. Mass. 1975) (comparing § 1407 transfer to *Eerie* Doctrine as applied to § 1404(a)); *accord In re* Four Seasons Sec. Laws Litig., 370 F. Supp. 219, 228 (W.D. Okla. 1974) (same); Phila. Hous. Auth. v. Am. Radiator & Standard Sanitary Corp., 309 F. Supp. 1053, 1055 (E.D. Pa. 1969) (same).

[50] *See In re Air Crash Disaster*, 399 F. Supp. at 1108. ("A United States District Court to which an action is transferred pursuant to 28 U.S.C.A. § 1407 must apply the substantive law of the transferor state and circuit.")

considerations and the choice-of-law analyses that accompany motions to dismiss common law claims in diversity cases.[51] In data breach class actions, the CCPA will throw a wrench in these analyses, which could spell disaster for similarly situated plaintiffs as they may watch CCPA plaintiffs enjoy what will appear to be unequal treatment under the law.[52]

Similarly, with many plaintiffs and defendants advocating for why the JPML should or should not choose a given transferee court, there is hardly a guarantee that non-CCPA classes will have their pretrial matters consolidated and heard within a favorable jurisdiction, such as the Ninth Circuit.[53] Historically, the JPML has given credence to several factors justifying consolidation, but has placed a special emphasis on consistency regarding district courts' pretrial proceedings.[54] Transferee courts typically are those with ample resources to handle these complex matters, which can concurrently decide on any non-common issues and are also convenient to the parties and witnesses.[55] These courts typically appoint plaintiffs' coun-

---

[51] *See* Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co., 559 U.S. 393, 397-99 (2010) (finding state law did not preclude FED. R. CIV. P. 23 from certifying class action); *see also In re Equifax, Inc.*, 362 F. Supp. 3d 1295,1311-12 (2019) (applying transferee court choice-of-law rules to determine that transferee court law will apply).

[52] *See generally* Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 350-52 (2011) (describing contemporary standards for class certification under FED. R. CIV. P. 23); *see also In re Equifax*, 362 F. Supp. 3d at 1333 (analyzing state statutory claims apart from common-law negligence or breach-of-contract claims); Kim, *supra* note 3, at 564 (stating that "data breach cases can be boiled down to state tort law questions.")

[53] *See In re* Anthem, Inc. Data Breach Litig., 327 F.R.D. 299, 317 (N.D. Cal. 2018) (explaining novel issue of data-breach actions across country). "Data-breach litigation is in its infancy with threshold issues still playing out in the courts. In the past three months alone, both the Seventh and Ninth Circuits have issued opinions addressing basic issues of standing in data-breach cases." *Id.* (internal citations omitted).

[54] *See In re* Nat'l Student Mktg. Litig., 368 F. Supp. 1311, 1317 (J.P.M.L. 1973) (quoting *In re* Library Editions of Children's Books, 297 F. Supp. 385, 386 (J.P.M.L. 1973)) (explaining that JPML "must 'weigh the interests of all plaintiffs and all defendants'" while considering litigation in light of purposes of law); *see also In re* Advanced Inv. Mgmt., L.P., Pension Fund Mgmt. Litig., 254 F. Supp. 2d 1377, 1379 (J.P.M.L. 2003) (centralizing actions to prevent inconsistent pretrial rulings).

> We also point out that transfer of all related actions to a single judge has the streamlining effect of fostering a pretrial program that: 1) allows pretrial proceedings with respect to any non-common issues to proceed concurrently with pretrial proceedings on common issues, and 2) ensures that pretrial proceedings will be conducted in a manner leading to the just and expeditious resolution of all actions to the overall benefit of the parties.

Id. (internal citation omitted); *In re* Gen. Adjustment Bureau Antitrust Litig., 375 F. Supp. 1405, 1407 (J.P.M.L. 1973) (consolidating cases where common factual issues present to prevent needless duplication of discovery).

[55] *See In re Advanced Inv. Mgmt.*, 254 F. Supp. 2d at 1379 (explaining characteristics of transferee courts).

sel to file a Consolidated Class Action Allegation Complaint for pretrial purposes, making plaintiffs' claims amenable to motions to dismiss and denial of class certification.[56] Without the oracular power to address all class action parties' interests in choosing a pretrial forum—and because some courts have found the circuit split regarding data breach standing to be immaterial for consolidation purposes—one can only hope to predict the results of class action lawsuits involving CCPA plaintiffs using the most current Supreme Court standards for nationwide class certification, with recent data breach cases serving as the backdrop.[57]

III. ANALYSIS

A. Nationwide Class Certification In The Dukes-Amchem Framework

In *Wal-Mart Stores, Inc. v. Dukes*,[58] the Supreme Court refined the traditional prerequisites to class certification under Fed. R. Civ. P. 23(a).[59] Under Rule 23(a), class action plaintiffs must demonstrate four requirements: (1) numerosity, (2) commonality, (3) typicality, and (4) adequacy of representation.[60] *Dukes* honed in on the commonality requirement, ac-

---

[56] *See In re* Premera Blue Cross Customer Data Sec. Breach Litig., No. 3:15-md-2633-SI, 2019 U.S. Dist. LEXIS 127093, at *2-3 (D. Or. 2019) (describing consolidation process with accompanying pre-trial motions).

[57] *See id.* (describing consolidation process in data breach class action); *see also In re* Equifax, Inc., Customer Data Sec. Breach Litig., 289 F. Supp. 3d 1322, 1325 (J.P.M.L. 2017) (rejecting argument that circuit split regarding data-breach standing precludes consolidation); *Wal-Mart Stores*, 564 U.S. at 349 (discussing nationwide class certification requirements under Rule 23); Amchem Prods. Inc. v. Windsor, 521 U.S. 591, 625 (1997) (discussing certification issues in mass tort litigation). *Compare In re Premera Blue Cross*, 2019 U.S. Dist. LEXIS 127093, at *2-3 (describing consolidation process with accompanying pre-trial motions), *with In re* Target Corp. Customer Data Sec. Breach Litig., 892 F.3d 968, 973 (8th Cir. 2018) (applying abuse of discretion standard to challenge regarding certification of settlement class), *and In re Anthem, Inc.*, 327 F.R.D. at 307 (discussing nationwide class prerequisites).

[58] 564 U.S. 338, 345 (2011) (discussing contemporary standards for class certification).

[59] *See generally In re Anthem, Inc.*, 327 F.R.D. at 314 (discussing nationwide class prerequisites).

[60] *See id.* (discussing Rule 23(a) requirements).

> Rule 23(a) provides that a district court may certify a class only if: "(1) the class is so numerous that joinder of all members is impracticable; (2) there are questions of law or fact common to the class; (3) the claims or defenses of the representative parties are typical of the claims or defenses of the class; and (4) the representative parties will fairly and adequately protect the interests of the class."

Id. (quoting FED. R. CIV. P. 23(a)).

knowledging that the language of Rule 23(a)(2) is easy to misread.[61] The *Dukes* Court found that it is not proper to focus on the myriad of questions common to all plaintiffs; rather, a court considering whether to certify a class of plaintiffs should focus its analysis on the ability of the potential class-wide proceeding to generate common *answers* "to drive the resolution of the litigation."[62] Admittedly, this is still a low threshold to meet for class action plaintiffs as "even a single common question [of law or fact] will do."[63]

In data breach class actions, courts have found the occurrence of a data breach satisfies Rule 23(a)(2), and have reasoned that a defendant's failure to "adequately store" plaintiffs' PII is a common injury suffered by all class members (at least in jurisdictions that recognize such injuries for standing purposes).[64] In a post-CCPA world, however, this analysis will almost certainly look different because CCPA compliance requires heightened data security and storage measures.[65] Indeed, by raising the bar of what companies must do to "adequately" protect consumer PII, the CCPA

---

[61] *See Dukes*, 564 U.S. at 349 (finding that any "competently crafted complaint" raises common questions but "reciting these questions is not sufficient to obtain class certification.") (quoting Richard A. Nagareda, *Class Certification in the Age of Aggregate Proof*, 84 N.Y.U. L. REV. 97, 131-32 (2009)).

[62] *See id.* at 350 (quoting Richard A. Nagareda, *Class Certification in the Age of Aggregate Proof*, 84 N.Y.U. L. REV. 97, 132 (2009)) (discussing commonality requirement).

[63] *See id.* at 359 (discussing commonality requirement of Rule 23(a)); *see also In re Anthem, Inc.*, 327 F.R.D. at 308 (citing JPML decision to consolidate as evidence of commonality).

[64] *See In re Anthem, Inc.*, 327 F.R.D. at 308 (finding that nationwide class met commonality requirement); *see also id.* at 317 (acknowledging strength of plaintiffs' case turns on "[l]egal uncertainties"); *In re* Premera Blue Cross Customer Data Sec. Breach Litig., No. 3:15-md-2633-SI, 2019 U.S. Dist. LEXIS 127093, at *30-31 (D. Or. 2019) (discussing commonality requirement for data breaches within *Dukes* framework).

> [The common issues of law or fact that can be resolved in one stroke] include whether Premera's data security practices were sufficient, whether the contracts issued by Premera included enforceable data security promises, whether Premera engaged in unfair or deceptive business practices with its data security practices or response to the Data Breach, whether the Data Breach compromised class members' Sensitive Information, and whether class members are entitled to damages as a result of Premera's conduct. The Court finds that the commonality requirement is satisfied.

In re Premera Blue Cross, 2019 U.S. Dist. LEXIS 127093, at *31; Elias, *supra* note 2, at 578-79 (discussing various circuit court approaches to data breach claims that involve state consumer protection acts, "emotional distress," "actual misuse of data by hackers," and claims for negligence and breach of implied contract).

[65] *See* Stuart L. Pardau, *The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States?*, 23 J. TECH. L. & POL'Y 68, 88-101 (2018) (discussing violations unique to CCPA regarding handling of consumer PII); *see also* CAL. CIV. CODE § 1798.150 (2020) (stating that private right of action stems from failing to implement "reasonable security procedures and practices appropriate . . . to protect the personal information . . . .").

distinguishes itself from other states' data security laws.[66] This discrepancy raises the novel issue under Rule 23(a)(2) concerning whether a defendant can "adequately store" some plaintiffs' PII under existing state laws, while simultaneously failing to meet the requirements specific to California plaintiffs.[67] In essence, if a private action is brought under the CCPA, a violation of one of the statute's many provisions would constitute negligence per se, with readily available and ascertainable statutory damages; whereas, plaintiffs in many other states must resort to pleading common law negligence claims.[68] Thus, Californian consumers will have no need to join nationwide classes with regard to these common law negligence or breach of contract claims that are subject to scrutiny under a forum state's choice of law analysis, or even negligence per se claims under Section 5 of the FTC Act.[69] This alternative process creates a degree of uncertainty for plaintiffs residing in states without strong, consumer-friendly data breach statutes because, for commonality purposes, the legal duties owed to different plaintiffs could be construed by courts as independent questions of law.[70] This factor alone may be sufficient to swamp class certification as each question of law will require a different answer as to "the extensiveness and

---

[66] *See State Laws Related to Internet Privacy*, NAT'L CONF. OF STATE LEGIS. (Jan. 27, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-Internet-privacy.aspx (summarizing differences among state laws regulating internet privacy); *see also 2019 Security Breach Legislation*, NAT'L CONF. OF STATE LEGIS. (Dec. 31, 2019), https://www.ncsl.org/research/telecommunications-and-information-technology/2019-security-breach-legislation.aspx (noting that all fifty states have enacted "security breach notification laws" but have not afforded private right of action to citizens for breaches).

[67] *See* sources cited *supra* note 66 (noting differences in state data security laws). "California and Utah laws . . . require all nonfinancial businesses . . . the types of personal information the business shares with or sells to a third party for direct marketing purposes or for compensation." *State Laws Related to Internet Privacy*, *supra* note 66; *see also* UTAH CODE § 13-37-203 (2003) (precluding consumers from bringing class actions stemming from unauthorized disclosure of PII).

[68] *See* CAL. CIV. CODE at § 1798.150(a)(1)(A) (2020) (providing statutory damages to consumers for violations of CCPA); RESTATEMENT (THIRD) OF TORTS § 14 (AM. LAW INST. 2010) (discussing standard for negligence per se as violation of statutorily imposed duty). "An actor is negligent if, without excuse, the actor violates a statute that is designed to protect against the type of accident the actor's conduct causes, and if the accident victim is within the class of persons the statute is designed to protect." RESTATEMENT (THIRD) OF TORTS § 14.

[69] *See In re* Equifax, Inc. Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1321-33 (N.D. Ga. 2019) (discussing merits of each claim at motion to dismiss stage after consolidation by JPML). "The application of another jurisdiction's laws is limited to statutes and decisions construing those statutes. When no statute is involved, Georgia courts apply the common law as developed in Georgia rather than foreign case law." *Id.* at 1311-12.

[70] *See id.* at 1340-42 (dismissing Georgia and New York plaintiffs' statutory claims because neither provided private right of action). The court in *Equifax* looked to transferor states' judicial interpretations and legislative intent to determine whether a private right of action for data breaches would be "inconsistent with [those states'] legislative scheme[s]." *Id.* at 1340.

adequacy of . . . security measures [which] lie at the heart of every claim."[71]

Further, the class certification stage is perhaps the most important phase in data-breach litigation for settlement purposes.[72] Courts have distinguished the criteria for class action certification along settlement lines due to the separate goals of going to trial versus settling all claims.[73] There is currently a widely adopted policy among federal courts to favor settlements in complex class action lawsuits and, following the Supreme Court's decision in *Amchem Prod. Inc. v. Windsor*[74], courts have simply been tasked with determining whether class certification for settlement agreements are "fair, reasonable, and adequate" pursuant to Rule 23(e)(2)—with Rule 23(a)(4)'s adequacy of representation requirement spearheading the analysis.[75] In data breach actions, like many other class suits, courts have approved settlement agreements negotiated between named plaintiffs' counsel and defendants even if certain class members receive higher com-

---

[71] *See id.* at 1340 (explaining significance of defendant's data security measures in data breach actions); *see also In re* Anthem, Inc. Data Breach Litig., 327 F.R.D. 299, 308 (N.D. Cal. 2018) ("The extensiveness and adequacy of Anthem's security measures lie at the heart of every claim. Moreover, the answer to those questions does not vary from Settlement Class Member to Settlement Class Member."). "Although Plaintiffs' theories withstood motions to dismiss, they have not been tested beyond the pleading stage . . . [a] finding that Anthem's security measures are inadequate is not a forgone conclusion . . . ." *In re Anthem, Inc.,* 327 F.R.D. at 317.

[72] *See In re Anthem Inc.*, 327 F.R.D. at 318 (noting that, as of date of district court's decision, "only one non-settlement data-breach class [had] been certified in federal court"); *In re* Hyundai & Kia Fuel Econ. Litig., 926 F.3d 539, 556-57 (9th Cir. 2019) ("In deciding whether to certify a litigation class, a district court must be concerned with manageability at trial. However, such manageability is not a concern in certifying a settlement class where, by definition, there will be no trial."); *In re* Premera Blue Cross Customer Data Sec. Breach Litig., No. 3:15-md-2633-SI, 2019 U.S. Dist. LEXIS 127093, at *6-7 (D. Or. 2019) (noting that different criteria apply for class certification in "litigation classes" as opposed to "settlement classes").

[73] *See In re Hyundai*, 926 F.3d at 556 (discussing Ninth Circuit judicial policy that favors settlements in complex class action litigation). "Parties seeking to overturn the [district court's] settlement approval must make a 'strong showing' that the district court clearly abused its discretion." *Id.* (citations omitted); *accord In re* Target Corp. Customer Data Sec. Breach Litig., 892 F.3d 968, 973-74 (8th Cir. 2018) (applying abuse of discretion standard to challenge regarding certification of settlement class).

[74] 521 U.S. 591, 625 (1997).

[75] *See In re Target Corp.*, 892 F.3d at 977 (discussing criteria for judicial approval of class action settlement agreement). "In determining whether a settlement agreement is fair, a district court should consider (1) the merits of the plaintiff's case[] weighed against the terms of the settlement, (2) the defendant's financial condition, (3) the complexity and expense of further litigation, and (4) the amount of opposition to the settlement." *Id.* at 978 (internal citations omitted) (quotations omitted); *see also Amchem Prod. Inc.*, 521 U.S. at 625 ("The adequacy inquiry under Rule 23(a)(4) serves to uncover conflicts of interest between named parties and the class they seek to represent.")

pensation for similarly alleged injuries.[76] This process has often resulted in "subgroup" conflicts and lengthy appeals in cases where some class members feel that the named plaintiffs of a nationwide class do not "possess the same interest[s] and suffer the same injur[ies] as [them]," which results in an unfair settlement.[77] Because of these occurrences, the *Amchem* Court sought to address "fundamental intraclass conflicts" by dividing the class and requiring separate attorneys to represent the interests of each "homogeneous subclass" in accordance with both Rule 23(e)(2) and 23(a)(4).[78] The Supreme Court indicated that, as a practical matter, this can cure any Rule 23(a)(4) adequacy concerns for settlement class certification purposes.[79] Still, when coupled with the deferential "abuse of discretion" standard

---

[76] *See In re Target Corp.*, 892 F.3d at 972 (outlining district court's approval of parties' settlement agreement). In the Target data breach:

> Target agreed to pay $10 million to settle the claims of all class members and waived its right to appeal an award of attorney's fees less than or equal to $6.75 million. For those class members *with documented proof of loss*, the agreement called for full compensation of their actual losses up to $10,000 per claimant. For those class members *with undocumented losses*, the agreement directed a pro rata distribution of *the amounts remaining after payments to documented-loss claimants* and class representatives.

Id. (emphasis added); *see also* Literary Works in Elec. Databases Copyright Litig. v. Thomson Corp., 654 F.3d 242, 251 (2d. Cir. 2011) (analyzing class action settlement agreement of federal copyright claims).

> The Settlement before us "confine[s] compensation and . . . limit[s] defendants' liability" by setting an $18 million recovery and cost ceiling, and distributes that recovery by making "essential allocation decisions" among categories of claims . . . . In addition, individual Category A and B claims are "more valuable" than Category C claims, producing "disparate interests" within the class.

Literary Works in Elec. Databases Copyright Litig, 654 F.3d 242 at 251. (internal citations omitted).

[77] *See generally Amchem Prods. Inc.*, 521 U.S. at 625-26 (observing how plaintiffs in nationwide class actions will not have identical interests in settlement negotiations). In *Amchem*, class members fell into one of two mutually exclusive camps, those injured by asbestos and those with only potential future claims. *See id.*; *see also In re Target Corp.*, 892 F.3d at 973 (discussing data breach class member's appeal regarding "intraclass conflict between class members who suffered verifiable losses from the data breach and those . . . who have not").

[78] *See Amchem Prod. Inc.*, 521 U.S. at 627 (finding that there is "no structural assurance of fair and adequate representation [under Rule 23(a)(4)] for the diverse groups and individuals affected" unless each subclass is represented by counsel).

[79] *See id.* at 625-28 (finding that it remains within district court's discretion to certify settlement agreements so long as class interests are "fairly and adequately protected"); *see also In re* Premera Blue Cross Customer Data Sec. Breach Litig., No. 3:15-md-2633-SI, 2019 U.S. Dist. LEXIS 127093, at *34-35 (D. Or. 2019) (summarizing district court's rationale for certifying settlement class). "The Court also finds that the Representative Plaintiffs and class counsel will prosecute this action vigorously on behalf of the class. The Court specifically selected class

applied to Rule 23(e)(2) judicial settlement approvals, it appears that courts find little trouble in upholding arms-length settlement agreements that may provide disparate compensation to different class members—whether divided into subclasses or not.[80]

When CCPA plaintiffs become class members in nationwide data breach actions, the incentive to settle with that subclass—if allowed by the court—will likely be a beneficial strategy for defendants.[81] With a strong push for CCPA plaintiffs to be separately certified as a subclass for settlement purposes, defendants could theoretically settle each individual CCPA class member's claim for an amount somewhere in the $100-$750 statutory damages range, as opposed to past data breach settlement agreements that have provided for a maximum individual recovery of $10,000.[82] At first glance, it may appear that CCPA plaintiffs will be disadvantaged by this practice, but in reality, the more lucrative settlement agreements typically come with provisions requiring plaintiffs to demonstrate documented proof of loss or "out-of-pocket damages . . . that are plausibly traceable to" the breach, which would only reach $10,000 under extraordinary circumstances.[83] Clearly, Californian plaintiffs now carry a lesser burden of proof by

---

counsel for their extensive experience in prosecuting complex class actions." *In re Premera Blue Cross*, 2019 U.S. Dist. LEXIS 127093, at *35.

[80] *See In re Target Corp.*, 892 F.3d at 976 (affirming district court's settlement class certification because interests of subclasses were "more congruent than disparate[,]" which meant differences in harm suffered were not "fundamental conflict[s] requiring separate representation"); *accord In re Premera Blue Cross*, 2019 U.S. Dist. LEXIS at *34-35 (certifying settlement class because court-selected class counsel had adequately represented interests of all class members).

[81] *See In re Premera Blue Cross*, 2019 U.S. Dist. LEXIS at *34 (noting that "Plaintiffs' expert opined that the average cost for medical identify theft is approximately $13,453" as opposed to $10,000 proposed settlement amount); *see also In re* Anthem, Inc. Data Breach Litig., 327 F.R.D. 299, 310 (N.D. Cal. 2018) (noting that differences in state laws are factor in subclass creation). While the court in *Anthem* found that "there [was] no structural conflict of interest based on variations in state law . . . and the differences in state remedies are not sufficiently substantial so as to warrant the creation of subclasses," this consideration of differing state laws in settlement class certification is instrumental in CCPA analysis. *In re Anthem, Inc.*, 327 F.R.D. at 310 (quoting Hanlon v. Chrysler Corp., 150 F.3d 1011, 1021 (9th Cir. 1998)).

[82] *See* CAL. CIV. CODE § 1798.150(a)(1)(A) (2020) (outlining statutory damages under CCPA); *see also In re Premera Blue Cross*, 2019 U.S. Dist. LEXIS at *34 (noting that parties' settlement agreement called for maximum recovery of $10,000 per consumer); *In re Target Corp.*, 892 F.3d at 972 (stating that parties' settlement agreement consisted of settlement fund of $10 million with "full compensation up to $10,000 per claimant").

[83] *See In re Anthem Inc.*, 327 F.R.D. at 319 (analyzing damages theories for individual plaintiffs).

> Plaintiffs' expert indicated that damages could be valued at $10 per individual, while Defendants' expert put damages at $4 per individual. Employing Plaintiffs' figure, damages total approximately $792 million. Thus, the $115 million Settlement Fund represents approximately 14.5% of the projected recovery that Settlement Class Members would be entitled to if they prevailed on their claims. The Court finds that this

certifying as a "CCPA subclass" and settling for statutory damages; whereas, the attendant risks of litigation will cause headaches for the millions of other class members as they negotiate compensation schemes for harm done to them.[84] Likewise, Congress has suggested that the class action bar has garnered a reputation for untrustworthiness as "many believe the only interests served by [class action] settlements are those of the class counsel."[85] This is partly the issue that the Supreme Court's ruling in *Amchem* tried to correct, but the Court's ruling also opened up more spots at the negotiation table for class action attorneys.[86] This practice may become a particular concern in future data breach actions where CCPA plaintiffs will have a strong argument in favor of subclass certification.[87]

B. Predominance Requirement

To make matters more complicated, commonality and adequacy of representation under Rule 23(a) are not the end of the analysis for class cer-

---

> percentage is within the range of reasonableness after taking into account the costs and risks of litigation.

Id. (internal citations omitted).

[84] *See In re Target Corp.*, 892 F.3d at 972-73 (discussing appeal theory that settlement would not adequately redress injuries or future risk of harm); *In re Anthem Inc.*, 327 F.R.D. at 325 (discussing class members' concerns over limited time period to claim out-of-pocket losses). "Several other objectors believe that the one-year limitation on the period to submit a claim for out-of-pocket costs will cut off recovery for unforeseen future losses." *In re Anthem Inc.*, 327 F.R.D. at 325.

[85] *See* Howard M. Erichson, *CAFA's Impact on Class Action Lawyers*, 156 U. PA. L. REV. 1593, 1599 (2008) (introducing motives behind Class Action Fairness Act of 2005 and distrust among class action lawyers). "Politicians and other CAFA [Class Action Fairness Act] proponents called class action lawyers self-interested, unscrupulous, unprincipled, and unaccountable." *Id.* at 1593-94 (internal citations omitted).

[86] *See id.*, at 1594 (noting class action lawyers' common mistrust of *Amchem*, *Ortiz*, and Rule 23 amendments).

> Each sought to tighten controls on class action lawyers to reduce abuse in light of problems of agency, autonomy, and leverage. Add to this picture the criminal prosecution of [a] firm and several of its leading partners for payments to class representatives in securities class actions, the criminal prosecution of [a] plaintiffs' attorney . . . for misappropriation of settlement funds, a similar prosecution of several . . . mass tort lawyers, and a spate of civil lawsuits against mass litigators claiming that they breached their duties to their clients, and the environment of mistrust of mass litigators becomes even clearer.

Id. at 1594-95.

[87] *See In re Anthem, Inc.*, 327 F.R.D. at 310 (noting that "substantial" differences in state remedies can warrant creation of subclasses).

tification.[88] If plaintiffs meet all four prerequisites under Rule 23(a), they then have the burden of proving that the class meets one of the three requirements under Rule 23(b).[89] As is often the case, data breach classes will seek certification pursuant to Rule 23(b)(3).[90] Under this requirement, plaintiffs must satisfy a two-part test: (1) "that the questions of law or fact common to class members predominate over any questions affecting only individual members;" and (2) "that a class action is superior to other methods of adjudication."[91] Further, plaintiffs must be wary of this test because the Supreme Court repeatedly observed that "Rule 23(b)(3)'s predominance criterion is even more demanding than Rule 23(a)."[92] For instance, in *Comcast Corp. v. Behrend*,[93] the Supreme Court found that the issue of damages was sufficiently individualized to preclude Rule 23(b)(3) predominance and deny class certification.[94] Likewise, in *Amchem*, the Supreme Court suggested that "[d]ifferences in state law may compound" already existing disparities among nationwide class members.[95] Thus, the guarantee of statutory damages for the CCPA subgroup of plaintiffs—and the statute being the first of its kind in the United States—may "swamp any common issues and defeat predominance" required to certify a nationwide class.[96]

---

[88] *See* Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 345 (2011) (stating that once 23(a) requirements are met, plaintiffs have burden to "satisfy at least one of the three requirements listed in 23(b)"); *see also In re Anthem Inc.*, 327 F.R.D. at 307 (noting that data breach classes seek certification under 23(b)(3)).

[89] *See Dukes*, 546 U.S. at 345 (describing class certification process).

[90] *See In re* Premera Blue Cross Customer Data Sec. Breach Litig., No. 3:15-md-2633-SI, 2019 U.S. Dist. LEXIS 127093 at *29 (D. Or. 2019) (stating that plaintiffs seek certification under Rule 23(b)(3)); *In re Anthem Inc.*, 327 F.R.D. at 311 (same); *accord Dukes*, 546 U.S. at 363 (noting "we think it clear that individual monetary claims belong in Rule 23(b)(3).")

[91] *See* FED. R. CIV. P. 23(b)(3).

[92] *See* Comcast Corp. v. Behrend, 569 U.S. 27, 34 (2013) (discussing predominance requirement); *see also Dukes*, 546 U.S. at 362 (discussing predominance criterion).

[93] 569 U.S. 27 (2013).

[94] *See id.* at 34 ("Questions of individual damage calculations will inevitably overwhelm questions common to the class."); *see also In re Anthem Inc.*, 327 F.R.D. at 317 (acknowledging data-breach plaintiffs raise novel issues of damages).

[95] *See* Amchem Prod. Inc. v. Windsor, 521 U.S. 591, 624 (1997) (analyzing class action through Rule 23(b)(3)'s predominance requirement); *In re Anthem, Inc.*, 327 F.R.D. at 313 (stating courts should examine differences in underlying state law as part of predominance analysis); *In re* Hyundai & Kia Fuel Econ. Litig., 881 F.3d 679, 691 (9th Cir. 2019) ("[I]n a multistate class action, variations in state law may swamp any common issues and defeat predominance.") (quoting Castano v. Am. Tobacco Co., 84 F.3d 734, 741 (5th Cir. 1996)).

[96] *See* CAL. CIV. CODE § 1798.150(a) (2020) (outlining private right of action under CCPA); *see also In re Hyundai*, 881 F.3d at 691 (suggesting that "where the consumer-protection laws of the affected [s]tates vary in material ways, no common legal issues favor a class-action approach to resolving [a] dispute.") (internal citation omitted).

On the other hand, the Supreme Court has also found that, "[t]o determine whether common questions predominate, the Court begins with 'the elements of the underlying cause of action.'"[97] If this "elements analysis" was applied to CCPA claims, a federal court will likely break § 1798.150's private right of action into its component parts to ask: (1) did the defendant possess the consumer's nonencrypted and nonredacted consumer information; (2) was that information subject to an unauthorized access and exfiltration, theft, or disclosure; and (3) was that exfiltration, theft, and/or disclosure the result of the defendant's violation of the duty to implement and maintain reasonable security procedures and practices *appropriate to the nature of the information*?[98] It will not be a stretch for a court to find that elements (1) and (2) are issues common to all class members for predominance purposes.[99] However, the more pressing question presented is whether the CCPA creates a heightened legal duty under element (3) as opposed to, for example, the legal duty owed under a common law negligence claim, because the CCPA contains other provisions, which indicate that "the nature of personal information" can vary in different contexts.[100] For instance, in breaches that implicate the CCPA's specific provision regarding businesses' execution of third party vendor contracts—that include an attendant prohibition on vendors' sale, retention, use, or disclosure of PII outside of the vendors' "direct business relationship with

---

[97] *See In re* Premera Blue Cross Customer Data Sec. Breach Litig., No. 3:15-md-2633-SI, 2019 U.S. Dist. LEXIS 127093 at *37 (D. Or. 2019) (quoting Erica P. John Fun, Inc. v. Halliburton Co., 563 U.S. 804, 809 (2011)) (discussing predominance analysis in data breach class action).

[98] CAL. CIV. CODE § 1798.150(a) (2020) (stating elements of private right of action under CCPA).

[99] *See In re Premera Blue Cross*, 2019 U.S. Dist. LEXIS at *56-58 (comparing California statutory claim with common law negligence claim for predominance purposes).

> The question of whether Premera had Sensitive Information is not disputed. The question of whether Premera negligently maintained, preserved, or stored the information would be resolved on a classwide basis. The question of whether a third party (the alleged hackers) accessed the data is also a common question, because it involves common evidence regarding whether data was exported or exfiltrated from Premera's servers.

Id. at *57-58.

[100] *See In re Anthem, Inc.*, 327 F.R.D. at 314 (noting common factual and legal issues relevant to negligence claims outweigh any individualized differences). In this pre-CCPA class action, the court found that the case did not "implicate any of the state-specific issues that can sometimes creep into the negligence analysis." *Id.* In the same decision, the court rejects an argument that the "predominance requirement cannot be met because the affected state consumer-protection statutes vary in their coverage," because "the core of the [p]laintiffs' case relie[d] on the uniform aspects" of these laws. *Id.* at 315.

the business"—courts will have to decipher whether businesses employed certain, context-specific procedures to safeguard consumer PII.[101]

Subsequently, under the private right of action provision of the CCPA, courts will then have to determine whether those procedures constitute "appropriate" and "reasonable" practices given the nature of the information.[102] Courts, however, may still be inclined to rely on past data breach actions, which found that predominance was established since each individual action stemmed from a single course of conduct by a single defendant.[103] Nonetheless, the CCPA certainly invigorates the debate over predominance, and at the very least, may cause courts to err on the side of caution by certifying CCPA plaintiffs as their own subclass during pre-trial proceedings, given that lengthy appeals interpreting this landmark statute are likely foreseeable.[104]

IV. CONCLUSION

The California Consumer Privacy Act is the first law of its kind in the United States. Its global reach in protecting Californian citizen's rights to their Personally Identifiable Information has already had a profound effect on the consumer marketplace as businesses become CCPA-compliant. Some may argue that its mere enactment is the final push needed for comprehensive federal data privacy legislation. If such a result does not come to fruition, however, an overarching federal data privacy regime will be necessary after a post-CCPA data breach's tangled and unpleasant journey through the federal court system. This journey is perhaps already being put to the test after California plaintiffs brought a class suit against Ring, LLC, whose in-home video surveillance systems have continuously been hacked.[105] Although the alleged injuries suffered in this case—hackers physically viewing consumers' private lives inside their homes—are far more concrete than the exposure of consumers' PII, the class action com-

---

[101] *See* CAL. CIV. CODE § 1798.140(w)(2)(A) (2020) (describing compliance requirements for third party contracts related to consumer PII).

[102] *See* Leipzig et al., *supra* note 17, at 37 (discussing guidelines for businesses' contracts with third party vendors).

[103] *See In re Anthem, Inc.*, 327 F.R.D. at 315 (finding predominance was met because vast majority of common issues regarding data breach stemmed from defendant's "common course of conduct").

[104] *See In re* Target Corp. Customer Data Sec. Breach Litig., 892 F.3d 968, 976 (discussing data breach as "one accident" that caused series of events leading to *all* plaintiffs' injuries) (emphasis added).

[105] *See In re* Ring LLC Privacy Litig., Docket No. 2:19cv10899 (C. D. Cal. Apr. 13, 2020) (Fitzgerald, J., Order Consolidating the Related Cases) (district court order allowing data breach class action to proceed with CCPA claims).

plaint brings both common-law negligence and CCPA claims on behalf of a nationwide class.[106] As this Note points out, this interplay between nationwide class members and California class members will surely be an interesting issue worth close observation.

With the FTC's confounded Equifax settlement still in sight, it is unsurprising that individual consumers continue to file data breach class actions in federal courts. The CCPA will likely muddle these pre-trial proceedings in multidistrict litigation, which could result in greatly disparate—and far more attainable—outcomes for Californian consumer-plaintiffs. The CCPA compounds the existing differences in state laws (or the lack thereof) regarding data breaches, and could be interpreted by federal courts to swamp either the commonality or predominance requirements for nationwide class certification under FED. R. CIV. P. 23(a) and (b). Likewise, the readily ascertainable damages for a CCPA subclass will have an indelible impact on data breach settlement negotiations, which will surely invigorate any adequacy of representation analyses by courts.

If such diversified treatment between citizens of different states becomes the norm for data breach class actions in federal courts, the federal government will seemingly have only two options. First, Congress could leave data breach legislation to the states, making it each state's prerogative to adopt CCPA-esque protections for its citizens, which includes a private right of action. However, such a course is symptomatic of why the CCPA was adopted in the first place: the piecemeal nature of data breach legislation on both the federal and state level is simply not an adequate means of protecting consumers' data. Alternatively, Congress could adopt its own CCPA-esque statutory scheme, granting more power and resources to the FTC to work as the sole organ of data breach litigation. In practice, such a scheme will theoretically provide uniform recovery for citizens of all fifty states, prevent needless multidistrict litigation that expends federal courts' resources, and create uniform standards for business practices related to the collection and protection of consumers' PII.

Until then, circuit splits over standing in data breach class actions and debates concerning what evidence needs to be shown to recover damages will perpetually rule the day in data breach litigation, as hackers and cybercriminals continue to infiltrate consumer data from businesses such as Microsoft, Estée Lauder, and MGM Resorts to the tune of 730.6 million consumer records.[107]

---

[106] *See id.* (permitting data breach class action to proceed with CCPA claims).

[107] *See* Eugene Bekker, *2020 Data Breaches | The Worst So Far*, IDENTITYFORCE (Jan. 3, 2020), https://www.identityforce.com/blog/2020-data-breaches (providing up-to-date list of all reported data breaches by year).