Note

Whose Data Anyway? The Inconsistent and Prejudicial Application of Ascertainability in Data Privacy Class Actions

*Nathan Webster**

INTRODUCTION

In September 2016, Yahoo disclosed that a data breach exposed account information of over 500 million users in a 2014 data breach.[1] Soon thereafter, on December 14, 2016, Yahoo made another disclosure: in a separate attack in 2013, malefactors gained access to the accounts of an estimated one billion users.[2] The compromised information included names, telephone numbers, dates of birth, security questions, and passwords.[3] In addition to the sensitivity of the information accessed, the scope of the breach also gave cause for concern.[4] At the time, less than three billion people used the Internet in the entire world.[5] One breach had affected over a third of global Internet users.

Even worse, the incident was not an isolated one. In 2018, Marriot disclosed that, over the course of four years, breaches

* J.D. Candidate 2021, University of Minnesota Law School. The Author wishes to thank Professor Bradley Clary, without whom this piece would not be possible. Special thanks also to the staff of the *Minnesota Law Review*, particularly Kaitie Eke, Melanie Griffith, and Abby Oakland. Copyright © 2021 by Nathan Webster.

[1] Vindu Goel & Nicole Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked*, N.Y. TIMES (Dec. 14, 2016), https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html [https://perma.cc/CMY2-NQBY].

[2] *See id.*

[3] *Id.* (describing the leaked information as "sensitive").

[4] *See* Jim Finkle & Anya George Tharakan, *Yahoo Says One Billion Accounts Exposed in Newly Discovered Security Breach*, REUTERS (Dec. 14, 2016, 4:12 PM), https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-one-billion-accounts-exposed-in-newly-discovered-security-breach-idUKKBN1432WZ [https://perma.cc/L78B-DH4N] (claiming that the 2013 attack was the largest data breach in history at the time).

[5] INTERNET SOC'Y, GLOBAL INTERNET REPORT 41 (2014), https://www.internetsociety.org/wp-content/uploads/2017/08/Global_Internet_Report_2014_0.pdf [https://perma.cc/4C2S-KMRA].

compromised information for 500 million guests.[6] The compromised information included passport numbers, credit card numbers, addresses, names, phone numbers, and information showing where and when guests were traveling.[7] Other victims of data breaches include: 414 million users of Adult FriendFinder, an adult dating site,[8] 145 million users of eBay,[9] 110 million customers of Target,[10] 83 million accounts at JP Morgan,[11] 57 million users of Uber,[12] 56 million customers of Home Depot,[13] and many others.[14] Reported breaches are increasing in frequency,[15] and some estimate that hackers attack the average

[6] Taylor Telford & Craig Timberg, *Marriot Discloses Massive Data Breach Affecting up to 500 Million Guests*, WASH. POST (Nov. 30, 2018, 12:03 PM), https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests [https://perma.cc/BUT2-XECP] ("The breach of the reservation system for Marriott's Starwood subsidiaries was one of the largest in history, after two record-setting Yahoo hacks.").

[7] *Id.*

[8] Andrea Peterson, *Adult FriendFinder Hit with One of the Biggest Data Breaches Ever, Report Says*, WASH. POST (Nov. 14, 2016, 1:30 PM), https://www.washingtonpost.com/news/the-switch/wp/2016/11/14/adult-friendfinder-hit-with-one-of-the-biggest-data-breaches-ever-report-says [https://perma.cc/6WEG-46FV].

[9] Andrea Peterson, *eBay Asks 145 Million Users To Change Passwords After Data Breach*, WASH. POST (May 21, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach [https://perma.cc/39DZ-PX8W].

[10] Elizabeth A. Harris & Nicole Perlroth, *For Target, the Breach Numbers Grow*, N.Y. TIMES (Jan. 10, 2014), https://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html [https://perma.cc/53FC-V9CJ].

[11] Tanya Agrawal, David Henry & Jim Finkle, *JP Morgan Hack Exposed Data of 83 Million, Among Biggest Breaches in History*, REUTERS (Oct. 2, 2014, 9:32 PM), https://www.reuters.com/article/us-jpmorgan-cybersecurity-idUSKCN0HR23T20141003 [https://perma.cc/J6BH-WM4Q].

[12] Brian Fung, *Uber Reaches $148 Million Settlement over Its 2016 Data Breach, Which Affected 57 Million Globally*, WASH. POST (Sept. 26, 2018, 11:07 AM), https://www.washingtonpost.com/technology/2018/09/26/uber-reaches-million-settlement-over-its-data-breach-which-affected-million-globally [https://perma.cc/U546-2S3H].

[13] Robin Sidel, *Home Depot's 56 Million Card Breach Bigger than Target's; 'Unique, Custom-Built Malware' Eliminated from Retailer's Systems After Five-Month Attack on Terminals*, WALL ST. J. (Sept. 18, 2014, 5:43 PM), https://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571 [https://perma.cc/J6BH-WM4Q].

[14] *See* Daniel Funke, *By the Numbers: How Common Are Data Breaches – and What Can You Do About Them?*, POLITIFACT (Sept. 23, 2019), https://www.politifact.com/article/2019/sep/23/numbers-how-common-are-data-breaches-and-what-can- [https://perma.cc/4GP9-RZRD] (reporting over nine thousand data breaches between 2005 and 2020).

[15] Rob Sobers, *107 Must-Know Data Breach Statistics for 2020*, VARONIS: INSIDE OUT SEC. (Sept. 24, 2020), https://www.varonis.com/blog/data-breach-statistics

Internet-connected computer once every thirty-nine seconds.[16] Perhaps most alarmingly, there are likely many thousands of attacks that go undetected and unreported.[17]

Unsurprisingly, consumers are availing themselves of legal recourse. Yahoo users filed a class action suit following disclosure of the 2013 and 2014 breaches.[18] Other injured consumers followed suit.[19] However, as such lawsuits become more common, obstacles, both judicial and circumstantial, are emerging, threatening the ability of plaintiffs to achieve equitable, efficient outcomes for their claims.[20] This Note focuses on the issue of ascertainability, that is, the requirement that certain class actions be definable by objective criteria and that it be administratively feasible to identify class members prior to certification.[21] As this Note will demonstrate, courts deploy this requirement inconsistently and, in doing so, perseverate on issues that inordinately arise in data privacy class actions.[22] Though courts have traditionally scrutinized other barriers to data privacy class actions,[23] ascertainability has the potential to gain prominence as traditional barriers are surmounted.[24] The limited treatment of ascertainability in data privacy so far paints a worrying picture of inconsistent decisions, penalization of data privacy classes, and no accountability for defendants. Unfortunately, despite the potential impact of

[https://perma.cc/9PUA-RMVD] (claiming that incidents of compromised data are "on the rise").

[16] *Hackers Attack Every 39 Seconds*, NBC NEWS (Feb. 7, 2007, 7:00 PM), https://www.nbcnews.com/id/wbna17034719 [https://perma.cc/6ZE9-F4R5].

[17] Thomas Claburn, *Most Security Breaches Go Unreported*, DARK READING (July 31, 2008, 7:27 PM), https://www.darkreading.com/attacks-and-breaches/most-security-breaches-go-unreported/d/d-id/1070576 [https://perma.cc/X4LP-7SML] ("More than 89% of security incidents went unreported in 2007 . . . .").

[18] *See In re* Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752, 2017 U.S. Dist. LEXIS 140212, at *26 (N.D. Cal. Aug. 30, 2017) (describing the class action).

[19] *See, e.g.*, Leon Stafford, *Suit Filed Against Home Depot in Possible Breach*, ATLANTA J.-CONST. (Sept. 5, 2014), https://www.ajc.com/business/suit-filed-against-home-depot-possible-breach/08rQKUVc9DHTfmdsW9ox1K [https://perma.cc/7ZQG-G4EF] (discussing a class-action lawsuit that was filed against Home Depot in a federal court in Georgia).

[20] *See infra* Part II (analyzing the ascertainability requirement's threat to data privacy class actions).

[21] *See infra* notes 40–45, 60–62 and accompanying text.

[22] *See infra* Part II.A (discussing the inconsistent application of the ascertainability requirement and its effect on data privacy actions).

[23] *See infra* notes 105–16 and accompanying text (discussing the standing issue for data privacy class-actions).

[24] *See infra* note 122 and accompanying text.

ascertainability on data privacy class actions, discussion among courts[25] and legal scholars[26] is scarce.

This Note will argue that the sparse case law that exists indicates that courts are making capricious ascertainability determinations and, in doing so, are perseverating on policy considerations that uniquely penalize data privacy class actions for indolent recordkeeping by defendants.[27] As a solution, this Note will argue that courts can and should permit ascertainability by affidavit without exception when a defendant's records are overinclusive and that new legislation awarding nominal damages would incentivize good behavior by defendants.[28] Part I will examine the history of the ascertainability requirement and the subsequent circuit split.[29] Next, Part I will briefly survey the standing issue and discuss how courts' resolution of that barrier increases ascertainability's potential to confound class certification.[30] Part I will conclude with a brief survey of judicial and scholarly treatment of ascertainability in data privacy class actions.[31] Part II will show that the limited treatment of ascertainability among data privacy class actions has been arbitrary thus far and employs criteria that are particularly hostile to data privacy classes, particularly when defendant records do not precisely identify class members.[32] To conclude, Part III will suggest a two-part solution: (1) that Congress pass legislation providing for nominal damages for data privacy infractions,[33] and (2) that courts can and should permit plaintiffs to ascertain classes using affidavits when a defendant's records are overinclusive.[34] Such action would provide some predictability for parties, promote judicial efficiency, and incentivize good behavior by defendants.

[25] *See infra* notes 64–76 and accompanying text.

[26] *See infra* notes 88–89 and accompanying text.

[27] *See infra* Part II.B (describing how ascertainability is particularly problematic for data breach claims due to the imprecise nature of their damages).

[28] *See infra* Part III.

[29] *See infra* Parts I.A–C.

[30] *See infra* Part I.D.

[31] *See infra* Part I.E.

[32] *See infra* Parts II.A–B.

[33] *See infra* Part III.A.

[34] *See infra* Part III.B.

I. BACKGROUND: ASCERTAINABILITY AS A JUDICIALLY CONSTRUCTED, CONTENTIOUS ELEMENT OF CLASS ACTIONS

A. ASCERTAINABILITY'S RELATIONSHIP TO OTHER CLASS ACTION REQUIREMENTS

Class actions have a celebrated history in American jurisprudence.[35] In a class action, many claims arising out of similar facts are aggregated into a class represented by a representative individual or group of individuals.[36] Emerging in their modern form in the mid-twentieth century, class actions seek to increase judicial efficiency and economy.[37] Plaintiffs benefit inasmuch as class actions afford the opportunity to litigate claims that would not otherwise be economically feasible.[38] Defendants, on the other hand, receive the benefit of repose—the knowledge that the suit resolves all related claims.[39] Rule 23 of the Federal Rules of Civil Procedure authorizes class actions in four different situations, one of which ((b)(3) classes) is particularly relevant to this Note.[40]

The first iteration of a class action arises where separate actions would create a risk of "inconsistent or varying adjudications with respect to individual class members that would establish incompatible standards of conduct for the party opposing the class."[41] Such classes arise where separate resolutions of similar cases might generate different instructions for similarly situated parties.[42] The second type of class arises where individual adjudication of claims "would be

[35] *See* David Marcus, *The History of the Modern Class Action, Part I: Sturm und Drang, 1953-1980*, 90 WASH. U. L. REV. 587, 588 (2013) (describing class actions as "the mechanism that has long stirred passions more than any other procedural rule").

[36] GERALD F. HESS, THERESA M. BEINER & SCOTT R. BARRIES, CIVIL PROCEDURE 397 (2015).

[37] *See* China Agritech, Inc. v. Resh, 138 S. Ct. 1800, 1811 (2018) (describing "efficiency and economy of litigation" as "a principal purpose of Rule 23").

[38] *See* Deposit Guar. Nat'l Bank v. Roper, 445 U.S. 326, 339 (1980) ("Where it is not economically feasible to obtain relief within the traditional framework of a multiplicity of small individual suits for damages, aggrieved persons may be without any effective redress unless they may employ the class-action device.").

[39] HESS ET AL., *supra* note 36.

[40] *See* FED. R. CIV. P. 23. The rule first lays out four prerequisites for class actions. *See id.* 23(a). When these prerequisites are met, the rule provides four scenarios where class actions can be maintained. *See id.* 23(b).

[41] *Id.* 23(b)(1)(A).

[42] For a discussion of a (b)(1)(A) class, see *Corley v. Entergy Corp.*, 222 F.R.D. 316, 320 (E.D. Tex. 2004), which shows how multiple plaintiffs argued that class certification under 23(b)(1)(A) was appropriate because the defendant might have been exposed to divergent court orders and standards of conduct.

dispositive of the interests of the other members."[43] Sometimes known as the "limited fund" class, an archetypal example is where the claims of many plaintiffs exceed the size of a limited fund, thereby ensuring that the only plaintiffs who will be made whole are those who are first in time.[44] The third kind of class action—the injunctive class[45]—arises where the defendant "has acted or refused to act on grounds that apply generally to the class" thereby making injunctive or declaratory relief appropriate.[46] An archetypal example of injunctive classes includes situations where the defendant has a policy that discriminates against a particular group—say women or minorities—and the plaintiffs seek a court-ordered change.[47]

The final (and for this Note's purposes, most relevant) iteration of class action arises when "questions of law or fact common to class members predominate over any questions affecting only individual members, and . . . a class action is superior to other available methods" of adjudicating the claims.[48] Essentially used for mass-damages claims, the purpose of this "(b)(3) class" is to allow plaintiffs to litigate otherwise economically infeasible claims.[49] Given the pecuniary interests involved, Rule 23 requires courts to give notice to (b)(3) class

[43] FED. R. CIV. P. 23(b)(1)(B).

[44] For a discussion of a "limited fund" class action, see *Ortiz v. Fibreboard Corp.*, 527 U.S. 815, 821 (1999), which details the additional requirements plaintiffs must satisfy to obtain this type of class certification.

[45] Typically, these classes exclusively seek injunctive relief, however, some courts have held that damages are permissible provided they are incidental to the injunctive relief sought. *See, e.g.*, *In re* Monumental Life Ins. Co., 365 F.3d 408, 416 (5th Cir. 2004) (defining incidental as "capable of computation by means of objective standards and not dependent in any significant way on the intangible, subjective differences of each class member's circumstances" (quoting Allison v. Citgo Petroleum Corp., 151 F.3d 402, 415 (5th Cir. 1998))).

[46] FED. R. CIV. P. 23(b)(2).

[47] Kathryn A. Honecker & Kevin Hanger, *Class Actions 101: Rule 23(b)(2) or (b)(3)? Does It Matter?*, A.B.A. (Sept. 11, 2011), https://www.americanbar.org/groups/litigation/committees/class-actions/articles/2011/summer2011-class-actions-101-federal-rules-civil-procedure [https://perma.cc/BV4P-Q4P6] (explaining that the purpose of such a class action is usually to obtain injunctive relief that will force the defendant to alter the discriminatory policy).

[48] FED. R. CIV. P. 23(b)(3).

[49] Amchem Prods., Inc. v. Windsor, 521 U.S. 591, 617 (1997) ("The policy . . . of the class action mechanism is to overcome the problem that small recoveries do not provide the incentive for any individual to bring a solo action prosecuting his or her rights." (quoting Mace v. Van Ru Credit Corp., 109 F.3d 338, 344 (1997))).

members, including (if practicable) individual notice mailed to potential plaintiffs.[50]

However, before plaintiffs can avail themselves of Rule 23, the Federal Rules of Civil Procedure identify four preliminary requirements plaintiffs must satisfy as a prerequisite for class certification: (1) numerosity, (2) commonality, (3) typicality, and (4) adequacy.[51] Additionally, courts have subsequently imposed a fifth requirement, namely that the putative class be ascertainable by "objective criteria," characterized by many circuits as "ascertainability."[52] This general objective criteria requirement—also known as "weak" ascertainability[53]—is typically a low bar, only requiring that classes be clearly defined enough such that individuals can determine they are members[54] and not be defined by reference to subjective criteria such as state of mind[55] or in terms of success on the merits of a claim.[56] Though not every circuit articulates this requirement as a *distinct* precondition to certification,[57] all circuits require that members of prospective classes be identifiable by objective criteria.[58]

[50] FED. R. CIV. P. 23(c)(2)(B) ("[T]he court must direct to class members the best notice that is practicable under the circumstances, including individual notice to all members who can be identified through reasonable effort.").

[51] *See id.* 23(a)(1)–(4).

[52] *See, e.g.*, Mullins v. Direct Digit., LLC, 795 F.3d 654, 657 (7th Cir. 2015) (explaining that this requirement has been imposed on all class actions regardless of which subsection of Rule 23 they fell under).

[53] *See* Tom Murphy, Comment, *Implied Class Warfare: Why Rule 23 Needs an Explicit Ascertainability Requirement in the Wake of* Byrd v. Aaron's Inc., 57 B.C. L. REV. E. SUPP. 34, 50 (2016).

[54] *See Mullins*, 795 F.3d at 659–60.

[55] *Id.* at 659.

[56] *Id.* at 657 (discussing "fail-safe" classes).

[57] *See, e.g.*, Sandusky Wellness Ctr., LLC v. Medtox Sci., Inc., 821 F.3d 992, 996 (8th Cir. 2016) (clarifying that, though a class must be ascertainable through objective criteria, this is an implicit requirement of the existing class action rules and does not constitute a separate prerequisite); *Mullins*, 795 F.3d at 657 (noting that "courts have *sometimes* used the term 'ascertainability'" to describe the requirement that (b)(3) classes be definable by objective criteria (emphasis added)).

[58] *See In re* Nexium Antitrust Litig., 777 F.3d 9, 19 (1st Cir. 2015) (explaining that the definitions of classes must be definite and citing cases); *In re* Petrobras Sec., 862 F.3d 250, 257 (2d Cir. 2017) (holding that "a class is ascertainable if it is defined using objective criteria"); Chiang v. Veneman, 385 F.3d 256, 271 (3d Cir. 2004) (agreeing with the argument that defining a class involves an objective evaluation); EQT Prod. Co. v. Adair, 764 F.3d 347, 358 (4th Cir. 2014) (holding that "a class cannot be certified unless a court can readily identify the class members in reference to objective criteria"); Seeligson v. Devon Energy Prod. Co., 761 F. App'x 329, 334 (5th Cir. 2019) (holding that a class must be "adequately defined and clearly ascertainable" (quoting Union Asset Mgmt. Holding A.G. v. Dell, Inc., 669 F.3d 632, 639 (5th Cir. 2012))); Young v.

Though courts are not in universal agreement, many circuits characterize ascertainability as only requiring that classes be definable by "objective criteria" to (b)(3) damages classes, if they articulate a distinct ascertainability requirement at all.[59] Courts justify this limitation by pointing to the notice requirement imposed on (b)(3) classes.[60] Inasmuch as (b)(2) classes need not give notice to their members,[61] multiple circuits hold that "the actual membership of the class need not . . . be precisely delimited."[62] In this spirit, the Third,[63] Fifth,[64] and Tenth Circuits[65] have explicitly rejected ascertainability as a requirement for (b)(2) injunctive classes.

Nationwide Mut. Ins., 693 F.3d 532, 538–39 (6th Cir. 2012) (citing MOORE'S FEDERAL PRACTICE § 23.21[3] (3d ed. 1997)); *Mullins*, 795 F.3d at 657 (holding that "a class must be defined clearly and that membership be defined by objective criteria"); *Sandusky Wellness Ctr.*, 821 F.3d at 997–98 (quoting Byrd v. Aaron's Inc., 784 F.3d 154, 163 (3d Cir. 2015)); Briseno v. ConAgra Foods, Inc., 844 F.3d 1121, 1124 n.4 (9th Cir. 2017) (explicitly rejecting a discrete "ascertainability" requirement but recognizing the need for classes to be defined based on objective criteria); Davoll v. Webb, 194 F.3d 1116, 1146 (10th Cir. 1999) (requiring that a class definition be sufficiently definite so as to indicate who is a member (citing Davoll v. Webb, 160 F.R.D. 142, 144 (D. Colo. 1995))); Karhu v. Vital Pharm., Inc., 621 F. App'x 945, 946 (11th Cir. 2015) ("This court has stated that a class is not ascertainable unless the class definition contains objective criteria that allow for class members to be identified in an administratively feasible way." (citing Bussey v. Macon Cnty. Greyhound Park, Inc., 562 F. App'x 782, 787 (11th Cir. 2014))).

[59] *See, e.g.*, Moore v. Walter Coke, Inc., 294 F.R.D. 620, 627 (N.D. Ala. 2013) ("Ascertainability depends on the class definition, and a successful definition is one that is 'precise, objective, and presently ascertainable . . . by reference to objective criteria.'" (quoting MANUAL FOR COMPLEX LITIGATION (FOURTH) § 21.222 (2004))).

[60] *See* FED. R. CIV. P. 23(c)(2)(B); *Byrd*, 784 F.3d at 165 (noting that "[t]he separate ascertainability requirement ensures that class members can be identified after certification . . . and therefore better prepares a district court to direct to class members the best notice that is practicable under the circumstances" (citation omitted) (citing FED. R. CIV. P. 23(c)(2)(B))); *Moore*, 294 F.R.D. at 627 ("For a 23(b)(3) class, ascertainability is also important because the 'best notice practicable' must be given to all class members, which often requires a list of addresses." (citing Krueger v. Wyeth, Inc., No. 03-CV-2496, 2011 WL 8984448, at *2 (S.D. Cal. July 13, 2011))).

[61] *See* FED. R. CIV. P. 23(b)(2) (choosing not to discuss a notice requirement).

[62] *E.g.*, Shook v. El Paso Cnty., 386 F.3d 963, 972 (10th Cir. 2004) (quoting Yaffe v. Powers, 454 F.2d 1362, 1366 (1st Cir. 1972)).

[63] Shelton v. Bledsoe, 775 F.3d 554, 563 (3d Cir. 2015) ("The nature of Rule 23(b)(2) actions . . . lead[s] us to conclude that ascertainability is not a requirement for certification of a(b)(2) [sic] class seeking only injunctive and declaratory relief.").

[64] *See In re* Monumental Life Ins. Co., 365 F.3d 408, 413 (5th Cir. 2004) (holding that precise class definition is not a requirement when plaintiffs plead a (b)(2) class and opt-out rights are not requested).

[65] *See Shook*, 386 F.3d at 972. However, such a ruling was not strictly necessary inasmuch as the Tenth Circuit has thus far declined to rule conclusively on ascertainability, only mentioning the requirement in one case. *See* Naylor Farms, Inc. v. Chaparral

B. *CARRERA* AND THE HEIGHTENED ASCERTAINABILITY REQUIREMENT

However, despite the courts' uniformity in requiring a general notion of ascertainability—namely objective criteria—for (b)(3) damages classes, the circuits split in their characterization of what exactly "identifiable with respect to objective criteria" ought to entail.[66] The Third Circuit precipitated this split in its 2013 case, *Carrera v. Bayer Corp*.[67] In *Carrera*, plaintiffs attempted to certify a (b)(3) class against defendant Bayer Corporation for "falsely and deceptively" advertising a product as having metabolism-enhancing effects.[68] The essence of the plaintiffs' complaint was that the product did not, in fact, enhance metabolism.[69] In moving to certify the class, plaintiffs attempted to establish ascertainability in two ways: (1) through online retailer records and sales made with store loyalty or reward cards, and (2) through class members' provision of affidavits attesting that they bought the product and detailing the amount purchased.[70] The district court ordered certification over the defendant's objections, defining the class as every person who purchased the product in Florida.[71]

On appeal, the circuit court revisited the issue of ascertainability.[72] The court identified three particularly important justifications for requiring ascertainability in a (b)(3) damages class, namely: (1) to provide plaintiff class members the opportunity to opt out, (2) to ensure a defendant's rights are protected by the class action mechanism, and (3) to ensure class members are identified consistently with "the efficiencies of a class action."[73] For a class to be ascertainable (and further the aforementioned objectives) the court clarified that class members must be identifiable "without extensive and individualized fact-finding or 'mini-trials.'"[74] The court held that, rather than merely

Energy, LLC, 923 F.3d 779, 788 n.9 (10th Cir. 2019) (noting that defendant's attempt to plead ascertainability failed on procedural grounds).

[66] *See infra* Part I.C (providing an analysis of the circuit split).

[67] 727 F.3d 300 (3d Cir. 2013).

[68] *Id.* at 304.

[69] *Id.* (explaining how the plaintiffs alleged that Bayer falsely asserted that its product enhanced metabolism due to its inclusion of a green tea extract).

[70] *Id.*

[71] Carrera v. Bayer Corp., No. 08-4716, 2011 WL 5878376, at *9 (D.N.J. Nov. 22, 2011) (concluding that the plaintiffs had satisfied all of Rule 23's certification requirements).

[72] *Carrera*, 727 F.3d at 303.

[73] *Id.* at 307 ("The sole issue on appeal is whether the class members are ascertainable.").

[74] *Id.* at 304 (quoting Marcus v. BMW of N. Am., LLC, 687 F.3d 583, 593 (3d Cir. 2012)).

identifying "objective criteria," class members must be identifiable in a way that is "administratively feasible," which the court took to mean a "manageable process that does not require much, if any, individual factual inquiry,"[75] and that identification must take place "at the class certification stage."[76] Thus was born the "heightened" ascertainability requirements, which has split courts and scholars alike.[77]

Using this new, heightened standard requiring an administratively feasible mechanism of class identification rather than mere objective criteria, the court proceeded to de-certify the plaintiffs' class.[78] The court found that, because the online records and rewards cards records could not identify individual purchasers of the product, the proposed methods of ascertaining the class were not administratively feasible inasmuch as they would require extensive individual factual inquiries.[79] The court's denial of certification threw down a gauntlet: not only would prospective classes have to satisfy the "objective criteria standard" (also known as "weak" ascertainability,) classes would also have to demonstrate an "administratively feasible" method of identifying members *before* certification, a standard that some classes might never clear where defendant records were deficient.[80]

C. The Ascertainability Circuit Split and Its Implications

Following the decision in *Carrera*, the courts of appeals diverged with some accepting and some rejecting the new administrative feasibility requirement.[81] The Eleventh Circuit Court of Appeals cited *Carrera* in holding that, to establish ascertainability, plaintiffs must demonstrate "an administratively feasible method by which class members can be identified."[82] Similar to the *Carrera* court, the Eleventh Circuit precluded self-identification and perfunctory references

[75] *Id.* at 307 (first quoting *Marcus*, 687 F.3d at 594; and then quoting William B. Rubenstein & Alba Conte, Newberg on Class Actions § 3:3 (5th ed. 2011)).

[76] *Id.*

[77] *See infra* notes 82–90 (identifying the ascertainability circuit split).

[78] *Carrera*, 727 F.3d at 312 (remanding the case to give the plaintiffs another opportunity to satisfy the ascertainability requirement).

[79] *Id.* at 308–09.

[80] *See generally infra* Part I.D (explaining how data privacy class actions are in a position where they are particularly vulnerable to dismissal for lack of ascertainability).

[81] *See infra* notes 82–90.

[82] Karhu v. Vital Pharm., Inc., 621 F. App'x 945, 950 (11th Cir. 2015).

to defendant records as establishing ascertainability.[83] Indeed, the Court quoted *Carrera* in precluding a finding of ascertainability absent plaintiffs' proposing a method with "evidentiary support that the method would be successful."[84] Similarly, in *In re Nexium Antitrust Litigation*, the First Circuit quoted *Carrera* in holding that "[a]t the class certification stage, the court must be satisfied that, prior to judgment, it will be possible to establish a mechanism for distinguishing the injured from the uninjured class members" and that the mechanism must be "administratively feasible."[85]

Conversely, the Seventh Circuit explicitly rejected *Carrera*'s holding, saying that the Third Circuit's reasoning "goes much further than the established meaning of ascertainability and in our view misreads Rule 23" and instead held that more detailed questions about ascertainability could be delayed until later in litigation.[86] The Sixth Circuit followed the Seventh Circuit's example.[87] When a defendant objected to class certification on the grounds of administrative feasibility, the court rejected the argument saying it saw "no reason to follow *Carrera*, particularly given the strong criticism it has attracted from other courts."[88] The Second Circuit joined the others, holding that "a free-standing administrative feasibility requirement is neither compelled by precedent nor consistent with Rule 23."[89] Finally, the Ninth Circuit concurred, saying that "an independent administrative feasibility requirement is unnecessary" and that the policy objectives outlined in *Carrera* are sufficiently addressed in Rule 23.[90] The emerging circuit

[83] *Id.* at 947 ("[T]he plaintiff must also establish that the records are in fact useful for identification purposes, and that identification will be administratively feasible." (citing Stalley v. ADS All. Data Sys., Inc., 296 F.R.D. 670, 679–80 (M.D. Fla. 2013))).

[84] *Id.* at 948 (citing *Carrera*, 727 F.3d at 306–07).

[85] 777 F.3d 9, 19 (1st Cir. 2015) (citing *Carrera*, 727 F.3d at 307).

[86] Mullins v. Direct Digit., LLC, 795 F.3d 654, 662 (7th Cir. 2015).

[87] Rikos v. Procter & Gamble Co., 799 F.3d 497, 525 (6th Cir. 2015).

[88] *Id.*

[89] *In re* Petrobras Sec., 862 F.3d 250, 264 (2d Cir. 2017).

[90] Briseno v. ConAgra Foods, Inc., 844 F.3d 1121, 1127 (9th Cir. 2017).

split notwithstanding, the Fourth,[91] Fifth,[92] Eighth,[93] and Tenth[94] Circuits have not yet weighed in on the heightened ascertainability requirement.

Further, the ascertainability controversy shows continued vitality. The Supreme Court has declined certiorari on at least three separate occasions.[95] As such, the uncertainty around ascertainability is likely to continue at least for the present. Indeed, rather than atrophying, the dispute over ascertainability is trickling down from federal courts into state courts as well.[96] Thus, even if the Supreme Court does resolve the issue, the controversy will likely live on in state jurisprudence.

The heightened ascertainability requirement (and its attendant circuit split) raises the following critical question: if plaintiffs pleading a (b)(3) class are required to demonstrate an "administratively feasible" method of establishing class membership, what approach should plaintiffs take when defendants' records are insufficient to precisely demarcate the class?[97] One popular solution is the submission of affidavits, where plaintiffs fill out a form certifying they are class

[91] *See* Krakauer v. Dish Network, L.L.C., 925 F.3d 643, 655 (4th Cir. 2019) (employing the "objective criteria" standard for establishing ascertainability).

[92] *See In re* Deepwater Horizon, 739 F.3d 790, 821 (5th Cir. 2014) (claiming that class certification is not precluded simply because some members would be unable to succeed on their individual claims).

[93] Sandusky Wellness Ctr., LLC v. Medtox Sci., Inc., 821 F.3d 992, 996 (8th Cir. 2016) (explicitly declining to take a position on the ascertainability split).

[94] Naylor Farms, Inc. v. Chaparral Energy, LLC, 923 F.3d 779, 788 n.9 (10th Cir. 2019) (noting, in the circuit's only mention of ascertainability, that the plaintiff's pleadings were procedurally deficient).

[95] *Briseno*, 844 F.3d at 1127, *cert. denied*, 138 S. Ct. 313 (2017); Rikos v. Procter & Gamble Co., 799 F.3d 497, 525 (6th Cir. 2015), *cert. denied*, 136 S. Ct. 1493 (2016); Mullins v. Direct Digit., LLC, 795 F.3d 654 (7th Cir. 2015), *cert. denied*, 136 S. Ct. 1161–62 (2016).

[96] *See, e.g.*, Stephen Carr, *Appeals Court Re-inflates Kiddie Pool Class Action*, A.B.A. (July 1, 2020), https://www.americanbar.org/groups/litigation/publications/litigation-news/top-stories/2020/appeals-court-re-inflates-kiddie-pool-action [https://perma.cc/B2RP-K2SS] (explaining the importance of a recent decision from the California Supreme Court).

[97] Given the abundance of electronic data in modern life, it might surprise readers to learn that defendant records are not guaranteed to precisely identify which consumers or service subscribers are affected by any given issue. *Id.* (detailing defendant record deficiencies in the context of a consumer class); *see also infra* Part II.A (detailing cases with deficient defendant records specifically in the data privacy context); Juliana de Groot, *The History of Data Breaches*, DIGIT. GUARDIAN: DATA INSIDER (Dec. 1, 2020), https://digitalguardian.com/blog/history-data-breaches [https://perma.cc/M4G4-DX9A] (detailing a 2012 data breach at Experian where the total number of compromised records is, as of this writing, "unknown").

members.[98] The Third Circuit—having the most developed ascertainability caselaw—has spoken favorably of the use of affidavits in establishing ascertainability where defendant records are deficient.[99] Indeed, the circuit has entertained the idea of permitting supplemental evidence as a way to buttress the credibility of such affidavits.[100] However, such flexibility notwithstanding, the circuit gives trial judges broad discretion in determining the circumstances under which affidavits are acceptable to fulfill ascertainability.[101] Such autonomy has resulted in inconsistent application, as this Note later discusses.[102]

D. The Receding Standing Issue and Other Jurisprudence Increases the Threat Posed by Ascertainability

The ongoing judicial dispute over the requirements of ascertainability has potentially profound implications for data privacy class actions.[103] As courts and other parties begin to devise ways around traditional barriers to data breach class actions, ascertainability will potentially become a powerful inhibitor to class certification.[104]

Traditionally, data privacy class actions faltered on issues of standing rather than ascertainability.[105] For the last decade, challenges to data privacy and data breach class actions focused on plaintiffs' abilities to articulate theories of injury in fact that were

[98] Byrd v. Aaron's Inc., 784 F.3d 154, 173 (3d Cir. 2015) (Rendell, J., concurring).

[99] *See, e.g.*, *id.* (holding that "[w]here a defendant's lack of records . . . make it more difficult to ascertain the members of an otherwise objectively verifiable low-value class, the consumers who make up that class should not be made to suffer" (quoting Carrera v. Bayer Corp., No. 12-2621, 2014 WL 3887938, at *3 (3d Cir. May 2, 2014) (Ambro, J., dissenting))).

[100] *See, e.g.*, City Select Auto Sales, Inc. v. BMW Bank of N. Am., Inc., 867 F.3d 434, 441 (3d Cir. 2017) ("Affidavits, in combination with records or other reliable and administratively feasible means, can meet the ascertainability standard." (quoting *Byrd*, 784 F.3d at 170–71)).

[101] *See Byrd*, 784 F.3d at 173–74 (making clear that "[i]t is the trial judge's province to determine what proof may be required at the claims submission and claims administration stage" and "when approving a claim form").

[102] *Infra* Part II.A.

[103] *See infra* Parts II.A–B.

[104] *See supra* Part I.D.

[105] *See* Aaron Benjamin Edelman, Note, *Increasing Lapses in Data Security: The Need for a Common Answer to What Constitutes Standing in a Data Breach Context*, 28 J.L. & POL'Y 150, 161–64 (2019) (discussing the historical reluctance of some courts to recognize standing in data privacy class actions); *see also In re* Google, Inc. Priv. Pol'y Litig., No. C-12-01382, 2013 WL 6248499, at *4 (N.D. Cal. Dec. 3, 2013) ("And so even though injury-in-fact [a component of standing] may not generally be Mount Everest, as then-Judge Alito observed, in data privacy cases . . . the doctrine might still reasonably be described as Kilimanjaro." (footnote omitted)).

persuasive enough for courts to find standing under Article III of the Constitution.[106] Article III extends the power of the federal judiciary to cases and controversies.[107] Courts have held that, to demonstrate standing under Article III, plaintiffs must demonstrate (1) that they have suffered a concrete injury (an injury in fact), (2) that the injury is fairly traceable to the defendant's actions, and (3) that it is likely, and not speculative, that a favorable decision will redress the injury.[108] Academics identify the injury in fact requirement as posing the most difficulty for data breach classes.[109] Specifically, the disclosure of private information often comes (a) without pecuniary consequence, or (b) without evidence of misuse of data, leaving some courts unwilling to find an injury in fact.[110]

However, despite initial judicial obstacles, data privacy plaintiffs have begun devising successful legal strategies for overcoming the standing requirement. For instance, some circuits have recognized increased likelihood of injury as a sufficient basis for finding standing in the context of data privacy class actions.[111] One case has even succeeded on the argument that dissemination of private information decreases its inherent value, thereby causing injury sufficient to establish standing.[112] Still more plaintiffs have successfully argued that failure to adequately protect data constitutes a misrepresentation that

[106] Eric S. Boos, Chandler Givens & Nick Larry, *Damages Theories in Data Breach Litigation*, 16 SEDONA CONF. J. 125, 126 (2015) (noting that "[f]or the most part these cases have failed to progress past the motion to dismiss stage, as defendants have successfully challenged the ability of litigants to demonstrate cognizable injuries sufficient to confer Article III standing").

[107] U.S. CONST. art. III, § 2, cl. 1.

[108] Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992).

[109] *See, e.g.*, Clara Kim, *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, 557. *See generally* Megan Dowty, *Life Is Short: Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683 (2017).

[110] *See, e.g.*, *In re* Michaels Stores Pin Pad Litig., 830 F. Supp. 2d 518, 527 (N.D. Ill. 2011) (finding that credit card reimbursements precluded a finding of injury in fact); Chambliss v. CareFirst, Inc., 189 F. Supp. 3d 564, 572–73 (D. Md. 2016) (finding that, despite defendant's loss of insurance data, plaintiffs' inability to prove misuse of lost data precluded finding of injury in fact).

[111] *See, e.g.*, Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010) (finding that the exposure of names, addresses, and Social Security numbers of defendant employees increased threat of future identity theft sufficient to establish standing under Article III); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (finding that "an act which harms the plaintiff only by increasing the risk of future harm" is sufficient to establish standing provided the other *Lujan* factors are met).

[112] *See* Claridge v. RockYou, Inc., 785 F. Supp. 2d 855, 865 (N.D. Cal. 2011).

deprives class members of a benefit of the bargain.[113] Also, more arguments are developing that, while not yet successful, indicate continued efforts to obviate the standing barrier to class actions.[114] The Supreme Court's placing additional scrutiny on the standing requirement[115] notwithstanding, appellate courts are still successfully finding standing in data breach class actions.[116] Furthermore, even as courts continue to find ways around the standing hurdle, nonjudicial entities such as law reviews are engaged in a careful evaluation of the standing issue, further expounding potential solutions to an already diminished barrier.[117] As such, defendants are likely to increasingly employ other arguments when attempting to kill data privacy class actions.

Further, ongoing legal challenges for data privacy class certification continue to limit common-law avenues of securing relief, thereby heightening reliance on statutory avenues of relief. For instance, in many common-law causes of action like negligence, plaintiffs must also establish causation and damages if they are to survive a 12(b)(6) motion to dismiss.[118] In the data privacy context, several courts have proved unwilling to accept plaintiffs' articulation of causation and damages.[119] The limitations of traditional causes of action in

[113] *See, e.g.*, *In re* LinkedIn User Priv. Litig., 932 F. Supp. 2d 1089, 1093–94 (N.D. Cal. 2013); Svenson v. Google, Inc., No. 13-CV-04080, 2015 WL 1503429, at *4 (N.D. Cal. Apr. 1, 2015).

[114] *See, e.g.*, *Chambliss*, 189 F. Supp. 3d at 571 (dismissing claim where plaintiff sought to establish standing by arguing damages from expenses incurred in mitigating the disclosure of their personal data).

[115] *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545 (2016) (emphasizing the particular elements of the standing requirement).

[116] *See, e.g.*, *In re* Horizon Healthcare Servs. Data Breach Litig., 846 F.3d 625, 639–41 (3d Cir. 2017) (holding that *Spokeo* merely reiterated traditional standing doctrine and finding that plaintiffs whose data had been leaked in contravention of a federal statute had pleaded standing with sufficient concreteness).

[117] *See, e.g.*, Bradford C. Mank, *Data Breaches, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits?*, 92 NOTRE DAME L. REV. 1323, 1365 (2017) (suggesting the Court take a broader view of standing in data breach cases); Cristiana Modesti, *Incentivizing Cybersecurity Compliance in the New Digital Age: Prevalence of Security Breaches Should Prompt Action by Congress and the Supreme Court*, 36 CARDOZO ARTS & ENT. L.J. 213, 216 (2018) (suggesting the Court define *Clapper*'s "certainly impending" standard to national security risks). *See generally* Kim, *supra* note 109.

[118] *See, e.g.*, Greenfield v. Suzuki Motor Co., 776 F. Supp. 698, 700–01 (E.D.N.Y. 1991).

[119] *See, e.g.*, Krottner v. Starbucks Corp., 406 F. App'x 129, 131 (9th Cir. 2010) (finding that plaintiffs' data privacy action failed to plead actual damage sufficient to establish negligence and failed to plead a sufficient meeting of the minds to establish an implied contract); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig.,

adequately sustaining data privacy suits ensure that statutory relief will continue to play an important role.[120] Indeed, in cases where courts dismissed common law claims, they have been known to allow statutory claims to stand.[121] Given its capricious application and courts' propensity to penalize statutory damages where a defendant's records are not exhaustive, ascertainability is ripe for exploitation.[122]

E. Judicial and Scholarly Treatment of Ascertainability in the Context of Data Breach Class Actions

A survey of the case law reveals few cases, at present, where ascertainability has been an issue in data privacy suits. The litigation that *has* happened took place at the district level. In *Opperman v. Kong Technologies Inc.*, a plaintiff class sued Apple and application developers under Federal Rule of Civil Procedure 23(b)(3) for allegedly permitting applications to upload class members' address book information without their knowledge or consent.[123] In light of the fact that it was unclear exactly which users of the address book application were affected, the court noted that "variations among the App Defendants in available information regarding users who had their address book data uploaded by a charged app could create ascertainability issues on class certification."[124] However, in the same case on a subsequent ruling on class certification, the same court dismissed any ascertainability concerns.[125] Citing *Briseno*, the court clarified that, in the Ninth Circuit, such obstacles were properly addressed in a 23(a) analysis.[126]

Similarly, the court mentioned ascertainability in dicta in *In re Yahoo Mail Litigation*.[127] There, the court in the Northern District of California, in an order partially granting certification, held that in the case

996 F. Supp. 2d 942 (S.D. Cal. 2014) (dismissing negligence theories in a data privacy suit for failing to establish causation and actual damage).

[120] *See, e.g.*, *In re* Yahoo Mail Litig., 308 F.R.D. 577, 582 (N.D. Cal. 2015) (pleading relief under the Stored Communications Act and California's Invasion of Privacy Act); *In re* Google, Inc. Priv. Pol'y Litig., No. C-12-01382, 2013 WL 6248499, at *10, *16 (N.D. Cal. Dec. 3, 2013) (dismissing common-law causes of action but countenancing statutory causes of action).

[121] *See, e.g.*, *In re Sony Gaming Networks*, 996 F. Supp. 2d at 953–54.

[122] *See infra* Part III.

[123] Opperman v. Kong Techs., Inc., No. 13-CV-00453, 2017 WL 3149205 (N.D. Cal. July 6, 2017).

[124] *Id.* at *15–16.

[125] Opperman v. Kong Techs., Inc., No. 13-CV-00453, 2017 WL 3149205, at *5 (N.D. Cal. July 25, 2017).

[126] *Id.*

[127] *In re* Yahoo Mail Litig., 308 F.R.D. 577, 596 (N.D. Cal. 2015).

of a 23(b)(2) class for injunctive relief, the plaintiffs did not need to define the class in an ascertainable way inasmuch as ascertainability is not necessary for the issuance of injunctive relief.[128] Similar to *Yahoo*, in *In re Google Inc. Privacy Policy Litigation*, the defendants objected to the plaintiffs' method of ascertaining the class (via affidavit), but the court denied certification for lack of predominance and did not address the ascertainability issue.[129] Again, in *In re Lenovo Adware Litigation* the court reiterated a heightened ascertainability requirement but did not analyze the issue inasmuch as the defendants had not objected to the plaintiff's assertion that the class was ascertainable with reference to defendant's records.[130]

In two other cases, which will be the subject of further discussion in Part II, ascertainability played a more important role. In *Harris v. comScore, Inc.*, plaintiffs in the Northern District of Illinois argued that all but a few class members could be established by referencing the plaintiff's records and that the rest could submit affidavits.[131] The court found that the small proportion of class members missing from the defendant's records made affidavits manageable and found ascertainability satisfied.[132] Conversely, in *In re Hulu Privacy Litigation*, the court denied certification due to an unascertainable class.[133] In doing so, the court found that despite the fact that the entirety of the class was encompassed by defendant's records, the fact that the records were overinclusive necessitated submission of affidavits by the larger part of the class, therefore rendering ascertainability by affidavit unmanageable.[134]

Even more sparse than the judicial treatment of ascertainability in the data breach context is its treatment in the secondary literature. As of this writing, only one scholarly work appears to specifically address ascertainability in the context of data privacy breaches. Without citing to any caselaw or statute, J. Thomas Ritchie reviewed the aforementioned circuit split regarding ascertainability.[135] He continued to hypothesize that cases like *Carrera* and *EQT Production Co. v. Adair*,

[128] *Id.*

[129] *In re* Google Inc. Gmail Litig., No. 13-MD-02430, 2014 U.S. Dist. LEXIS 36957, at *6 (N.D. Cal. Mar. 18, 2014).

[130] *In re* Lenovo Adware Litig., No. 15-MD-02624, 2016 WL 6277245, at *16–17 (N.D. Cal. Oct. 27, 2016).

[131] 292 F.R.D. 579, 587 (N.D. Ill. 2013).

[132] *Id.* at 587–88.

[133] *In re* Hulu Priv. Litig., No. C 11-03764, 2014 WL 2758598, at *13–15 (N.D. Cal. June 16, 2014).

[134] *Id.* at *16.

[135] J. Thomas Richie, *Data Breach Class Actions*, 44 BRIEF 12, 16 (2015).

with their heightened ascertainability requirement, might "make certification less likely" though he cited no statutory or judicial authority.[136] Given the sparse judicial consideration of ascertainability in the data privacy context, the subject is ripe for review.

II. ASCERTAINABILITY IN DATA PRIVACY CLASS ACTIONS LEADS TO ARBITRARY CERTIFICATION DECISIONS, FOCUSES ON FACTORS PARTICULARLY CHALLENGING TO DATA PRIVACY SUITS, AND FAILS TO INCENTIVIZE GOOD BEHAVIOR

This Part will identify how the strict ascertainability requirement is applied inconsistently from case to case in the data privacy context, noting that similar situations receive different outcomes based on judges' individual estimations of what is "manageable." Then, it will focus on how, when defendants' records are not sufficient to identify every class member at the outset, courts use large statutory damages (a hallmark of laws commonly used to bring data privacy suits) as an excuse to preclude the use of affidavits to establish ascertainability. Finally, this Part analyzes how courts' inconsistent, prejudicial application of ascertainability creates different outcomes for similarly situated plaintiffs and undermines the goal of class actions to adjudicate claims efficiently.

A. COURTS ENFORCE ASCERTAINABILITY RULES INCONSISTENTLY FROM CASE TO CASE

The ascertainability requirement, while never universally accepted, suffers from a lack of consistent application.[137] Data privacy class actions, with their vast scope and technical sophistication, are particularly vulnerable to arbitrary judicial determinations of ascertainability and "manageability" that lead to conflicting, unpredictable results for different suits. The two cases that particularly encapsulate this issue are *Harris v. comScore, Inc.*[138] and *In re Hulu Privacy Litigation*,[139] the implications of which become clear in additional data privacy cases such as *In re Google Inc. Gmail Litigation*[140] and *Backhaut v. Apple Inc.*[141]

[136] *Id.* at 17.

[137] *Supra* notes 89–105 and accompanying text.

[138] 292 F.R.D. 579, 581 (N.D. Ill. 2013).

[139] No. C 11-03764, 2014 U.S. Dist. LEXIS 83661, at *3 (N.D. Cal. June 16, 2014).

[140] No. 13-MD-02430, 2014 U.S. Dist. LEXIS 36957 (N.D. Cal. Mar. 18, 2014).

[141] No. 14-CV-02285, 2015 WL 4776427 (N.D. Cal. Aug. 13, 2015).

In *Harris v. comScore Inc.*, plaintiffs asserted a classic data scraping claim, that is, that comScore illegally obtained information from class members' computers, repackaged it, and sold it to purveyors of targeted advertising.[142] Defendant comScore garnered its data through a program called OSSProxy.[143] When users installed OSSProxy on their computers, the program collected data, sending it to comScore's servers.[144] comScore induced consumers to download OSSProxy by partnering with bundlers, who provided free digital products to Internet users who downloaded the bundle.[145] In downloading the bundlers' software, consumers confronted a message informing them that the comScore OSSProxy software was included "[i]n order to provide this free download."[146] Alleging several theories of damages, the plaintiffs sued under the Stored Communications Act, the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and the common-law theory of unjust enrichment.[147]

In arguing for certification, the plaintiffs countered comScore's assertion that the task of identifying class members would "swamp[] any common questions in this case."[148] Plaintiffs argued that, rather than class members needing to be ascertained, the class must merely be ascertainable (defined by objective criteria).[149] Here, plaintiffs argued that the objective criteria were clear: namely, whether the class members downloaded the software.[150] If there were no corroborating records to prove class members' downloading of the software, plaintiffs argued that submission of an affidavit affirming that members had downloaded the software would suffice.[151]

At the time of the *comScore* case, the Northern District of Illinois accepted the Third Circuit's ascertainability requirement that class members be identifiable with reference to objective criteria and that there be an administratively feasible way of determining membership at certification.[152] Both parties agreed that comScore's records would

[142] 292 F.R.D. at 581.

[143] *Id.*

[144] *Id.*

[145] *Id.*

[146] *Id.* at 582.

[147] *Id.* at 581.

[148] Plaintiffs' Reply in Support of Their Supplemental Motion for Class Certification at 9, Harris v. comScore Inc., 292 F.R.D. 579 (N.D. Ill. 2013) (No. 11 C 5807).

[149] *Id.*

[150] *Id.* at 15.

[151] *Id.* at 10.

[152] *Harris*, 292 F.R.D. at 587 (citing Marcus v. BMW of N. Am., LLC, 687 F.3d 583, 593 (3d Cir. 2012)).

identify at least some proportion of the proposed class.[153] comScore, however, noted that permitting submission of affidavits would be unwieldy and entail individualized fact determinations inasmuch as comScore would be entitled to challenge each affidavit.[154] The court, while recognizing that affidavits *could* violate the ascertainability requirement, also noted that courts have permitted class identification by affidavit where the administrative burden was "minimal."[155] The court ultimately found that the proposed class was ascertainable inasmuch as most class members were identifiable through comScore's records, rendering the use of affidavits "manageable."[156]

However, in another case, the court in the Northern District of California treated affidavits completely differently despite similar facts. In *In re Hulu Privacy Litigation*, plaintiffs alleged that Hulu, a video streaming website, had inappropriately taken data from users and distributed it to Facebook and other purveyors of targeted ads.[157] As with *comScore*, the court required that class members be identifiable with reference to objective criteria such that it was "administratively feasible" for the court to determine who was bound by the judgment.[158] Citing *comScore*, the plaintiffs argued in their reply in favor of certification that class members, though not ascertainable through Hulu's records, could self-identify through affidavits.[159] Since both Facebook and Hulu require users to register using email addresses, cross-referencing the records of both Hulu and Facebook would (theoretically) produce a list including all of the class members who had data stolen.[160] However, the court noted that cross-referencing would not satisfy ascertainability inasmuch as the true class members were those who had their personal data actually *transmitted* to Facebook, which depended on a number of factors.[161] Given that cross-referencing would produce an over-inclusive class, the court concluded that

[153] *Id.*

[154] *Id.* at 587–88.

[155] *Id.* at 587 (citing Boundas v. Abercrombie & Fitch Stores, Inc., 280 F.R.D. 408, 417 (N.D. Ill. 2012)).

[156] *Id.* at 588.

[157] *In re* Hulu Priv. Litig., No. C 11-03764, 2014 WL 2758598, at *14 (N.D. Cal. June 16, 2014) (pleading a subclass for those whose data was harvested by comScore and a subclass for those whose data was harvested by Facebook).

[158] *Id.* at *13 (citing Shepard v. Lowe's HIW, Inc., No. C 12-3893, 2013 WL 4488802 (N.D. Cal. Aug. 19, 2013)).

[159] Plaintiffs' Reply in Support of Motion for Class Certification at 26 n.15, *In re* Hulu Priv. Litig, 86 F. Supp. 3d 1090 (2015) (No. 11-CV-03764).

[160] *In re Hulu Priv. Litig.*, 2014 WL 2758598, at *14.

[161] *Id.*

the only way to actually *ascertain* who was in the class (rather than define the class) was through submission of affidavits.[162]

Having theretofore mirrored the reasoning in *comScore*, the *Hulu* court abruptly diverged. Citing *comScore*, the court held that, while affidavits were sometimes an acceptable method of satisfying ascertainability, it can also be improper to satisfy ascertainability "only by assertion of the class-members."[163] The *Hulu* court, citing a treatise,[164] instead decided to weigh the ease of documentation, the difficulty of verifying the claims, and the size of the claims.[165] The court found, with little explanation, that the claims were hard to verify, that documentation would be burdensome, and that the claims were large.[166] Though the claims in the *comScore* case were also difficult to verify and also pleaded large claims, the *Hulu* court nevertheless found that ascertainability was not satisfied.[167] In doing so, it distinguished its decision from *comScore*, noting that in *comScore*, "the 'bulk' of the class membership would be determined by comScore's own records" whereas with the instant case "records here would identify a large pool of users with only a subset . . . suffering any injury."[168] The court essentially decided that ascertainability was not satisfied because a larger proportion of *Hulu* class members required verification than the *comScore* class members. Though some might argue that courts have every right to make determinations based on the proportion of the class that has to submit affidavits, such discretion nevertheless raises an important concern of judicial arbitrariness, particularly where—as was the case in *Hulu*—the court makes no attempt to set forth a rule or guiding principal on which future plaintiffs can rely.[169] In the end, both classes contemplated ascertainability by affidavit. The *Hulu* decision, though ostensibly resting on a distinction in degree, in reality rests on an expectation of unquestioned deference to judicial determinations of what constitutes too many affidavits. Both plaintiffs and defendants should expect, and deserve, more reliable indicia, particularly in the case of data privacy where potential classes are vast and judgments of proportion have outsized effects.

[162] *Id.*

[163] *Id.* (citing Harris v. comScore, Inc., 292 F.R.D. 579, 587–88 (N.D. Ill. 2013)).

[164] NEWBERG ON CLASS ACTIONS § 10.12 (Alba Conte & Herbert B. Newberg eds., 4th ed. 2012).

[165] *In re Hulu Priv. Litig.*, 2014 WL 2758598, at *13–15 (citing NEWBERG ON CLASS ACTIONS, *supra* note 164).

[166] *Id.* at *14–15.

[167] *Id.*

[168] *Id.*

[169] *See generally id.*

Such necessity of affidavits to complement defendant records in data privacy class actions extends to other cases as well. For instance, in a consolidated class action against Google, plaintiffs alleged that Google illegally intercepted (scraped) messages sent through Gmail.[170] The class included users of Gmail, as well as users of other email providers who had exchanged emails with Gmail account owners.[171] Though the case was dismissed for failure to satisfy the predominance requirement of class actions,[172] the pleadings in the case fiercely contested ascertainability.[173] Plaintiffs asserted that the subclasses with Gmail accounts were "easily ascertainable because they have Gmail accounts and contracts with Google" and that the subclass of non-Gmail users could be ascertainable through the submission of an email, essentially an affidavit.[174] Google, in its motion to dismiss, argued that despite plaintiffs' assertion that the class was easily ascertainable from defendant's records, the plaintiffs had not explained "what documents they were referring to and did not cite any supporting evidence" proving the assertion to be true.[175] Had the case not been decided on predominance grounds, and Google's assertions proved correct, plaintiffs might very well have had to take their chances with the submission of affidavits. Given the juxtaposition of *Hulu* and *comScore*, the outcome would have been far from certain.

Similarly, in *Backhaut v. Apple Inc.*, plaintiffs sued Apple, saying that the company had improperly intercepted messages sent through the Apple iPhone iOS operating system, causing them not to reach their intended recipients.[176] The Northern District of California articulated the same ascertainability standard as in other cases, namely that it be defined by objective criteria and that it is administratively

[170] *In re* Google Inc. Gmail Litig., No. 13-MD-02430, 2014 U.S. Dist. LEXIS 36957, at *6 (N.D. Cal. Mar. 18, 2014).

[171] *Id.*

[172] *Id.* at *81–83.

[173] *See* Plaintiffs' Reply in Support of Plaintiffs' Consolidated Motion for Class Certification at 20–24, *In re Google Inc. Gmail Litig.*, 2014 U.S. Dist. LEXIS 36957 (No. 13-MD-02430); Defendant Google Inc.'s Motion To Dismiss Plaintiffs' Consolidated Individual & Class Action Complaint; Memorandum of Point & Authorities in Support Thereof at 50–52, *In re Google Inc. Gmail Litig.*, 2014 U.S. Dist. LEXIS 36957 (No. 13-MD-02430).

[174] Plaintiffs' Reply in Support of Plaintiffs' Consolidated Motion for Class Certification, *supra* note 173, at 20.

[175] Defendant Google Inc.'s Motion To Dismiss Plaintiffs' Consolidated Individual & Class Action Complaint; Memorandum of Point & Authorities in Support Thereof, *supra* note 173.

[176] Backhaut v. Apple Inc., No. 14-CV-02285, 2015 WL 4776427, at *1–2 (N.D. Cal. Aug. 13, 2015).

feasible to determine whether potential members belong to a class.[177] Unsurprisingly, defendants, in opposition to class certification, argued that the only way to ascertain whether a person is in the class is through self-identification through affidavit, a process defendants argued would be unreliable and unfeasible.[178] The court agreed, saying that self-reporting would require each plaintiff class member to determine whether they had failed to receive a message.[179] Permitting this method of class identification required, in the court's view "individualized factual determinations," thereby precluding class certification on ascertainability grounds.[180]

Indeed, the only way to mitigate the threat of ascertainability in the data privacy context might be to avoid pleading damages, or to hope that the defendants lack the wherewithal to plead ascertainability. In *In re Yahoo Mail Litigation*, plaintiffs sued Yahoo for scanning information in ingoing and outgoing messages pertaining to Yahoo email accounts.[181] Though Yahoo obtained consent for the data extraction from those with Yahoo accounts, it made no other effort to obtain consent to scrape data from the messages of non-Yahoo users.[182] Unlike other cases, the plaintiffs only requested injunctive relief.[183] Though the defendants attempted to argue that (b)(2) injunctive relief classes also had to demonstrate administrative feasibility,[184] the court decided that the ascertainability requirement only applied to (b)(3) damages classes.[185] In *Lenovo* as previously iterated, the court declined to analyze ascertainability given that the defendants had not objected to the plaintiffs' prospective use of affidavits.[186]

Simply put, the interplay of *Hulu* and *comScore* established a troubling precedent: where defendant records do not precisely establish the contours of a (b)(3) damages class, courts are at liberty to make arbitrary determinations about the acceptable proportion of a class

[177] *Id.* at *9–10 (citing Wolph v. Acer Am. Corp., No. 09-1314, 2012 WL 993531, at *1–2 (N.D. Cal. Mar. 23, 2012)).

[178] Defendant's Opposition to Plaintiffs' Motion for Class Certification at 10–12, *Backhaut*, 2015 WL 4776427 (No. 14-CV-02285).

[179] *Backhaut*, 2015 WL 477427, at *12.

[180] *Id.* at *11.

[181] *In re* Yahoo Mail Litig., 308 F.R.D. 577, 583 (N.D. Cal. 2015).

[182] *Id.* at 584.

[183] *Id.* at 585.

[184] *Id.* at 596.

[185] *Id.* at 597 (holding that the nature of relief sought for a (b)(2) class meant there was little purpose to an ascertainability requirement).

[186] *In re* Lenovo Adware Litig., No. 15-MD-02624, 2016 WL 6277245, at *15 (N.D. Cal. Oct. 27, 2016).

that can satisfy ascertainability through affidavits.[187] Such precedent gives judicial ammunition to data privacy defendants' established efforts to defeat class certification by invoking ascertainability.[188]

B. THE *HULU* COURT'S RELIANCE ON CLAIM SIZE IS UNIQUELY CHALLENGING FOR DATA PRIVACY PLAINTIFFS

In addition to being arbitrarily applied and disincentivizing damages classes, courts evaluate ascertainability in a way that is uniquely challenging for data privacy class actions. Citing *Newberg on Class Actions*, the *Harris* court stated that ascertainability by affidavit can be appropriate "where claims are small or are not amenable to ready verification."[189] The *Hulu* court adopted this reasoning, citing *Harris*'s reliance on *Newberg* in finding that a statutory penalty of $2,500 was "not small" and therefore militated against the use of affidavits.[190] Such focus on damages is particularly challenging in the data privacy context. Damages in data breach lawsuits are notoriously imprecise.[191] Pleading actual damage from the loss of data often results in dismissal or pitifully small awards.[192]

As such, statutory damages are often the only method by which plaintiffs pleading federal claims can receive meaningful damages, particularly if state legislatures have not provided methods of relief. In what initially seems to be a windfall for plaintiffs, statutory damages can be quite generous. For instance, the Stored Communications Act, cited by the *Harris* and *Yahoo* courts, permits minimum statutory

[187] *Supra* notes 143–45 and accompanying text.

[188] *Supra* notes 171–72 and accompanying text.

[189] Harris v. comScore, Inc., 292 F.R.D. 579, 588 (N.D. Ill. 2013) (quoting ALBA CONTE & HERBERT B. NEWBERG, 3 NEWBERG ON CLASS ACTIONS § 10:12 (4th ed. rev. 2012)).

[190] *In re* Hulu Priv. Litig., No. C 11-03764, 2014 WL 2758598, at *15–16 (N.D. Cal. June 16, 2014) (citing *Harris*, 292 F.R.D. at 587–88).

[191] *See, e.g.*, *In re* Horizon Healthcare Servs. Data Breach Litig., 846 F.3d 625, 639 (3d Cir. 2017) (asserting that "[d]amages for a violation of an individual's privacy are a quintessential example of damages that are uncertain and possibly unmeasurable" (citation omitted)); Patrick J. Lorio, *Access Denied: Data Breach Litigation, Article III Standing, and a Proposed Statutory Solution*, 51 COLUM. J.L. & SOC. PROBS. 79, 87–88 (2017) (discussing difficulties data privacy litigants face in attempting to establish actual damages).

[192] *See generally In re Horizon Healthcare*, 846 F.3d at 639; *In re* Rutter's Data Sec. Breach Litig., No. 20-CV-382, 2021 WL 29054, at *6 (M.D. Pa. Jan. 5, 2021) (dismissing data privacy litigants where plaintiffs had "only possible future injuries and prophylactic measures to avoid those potential injuries"); *In re* Cmty. Health Sys., Inc., No. 15-CV-222, 2016 WL 4732630, at *15–17 (N.D. Ala. Sept. 12, 2016) (finding that patients whose health data was stolen suffered no actual damages).

damages of $1,000 per claim.[193] The Communications Privacy Act, cited by the *Harris* and *Gmail* courts, awards up to $500 per claim for initial offenders, and up to $1,000 for repeat offenders.[194] The Video Privacy Protection Act, cited by the *Hulu* court, awards a minimum of $2,500 per violation.[195] Unfortunately for the plaintiffs in *Hulu*, the court held the generosity of statutory damages as weighing against the use of affidavits, thereby preventing the class from being ascertainable and precluding certification.[196] In deciding whether the plaintiffs had satisfied ascertainability, the court found that the large damage award authorized by the Video Privacy Protection Act made the use of affidavits inappropriate, holding that "when dollar amounts are higher, some form of verification is appropriate beyond just an affidavit."[197] The court reasoned that the large damage amount "creates incentives for claimants" to fabricate claims.[198] Inasmuch as courts have not yet determined whether statutory damages under the other statutes are large enough to militate against affidavits, plaintiffs requesting ascertainability by affidavit must exercise caution in pleading or risk denial of certification.

C. The Ninth Circuit's Obviation of the Ascertainability Requirement Does Not Solve the Challenges Ascertainability Presents to Data Privacy Classes

It is important to acknowledge that the Ninth Circuit rendered moot the problematic cases[199] mentioned in this Note in *Briseno v. ConAgra Foods, Inc*.[200] The *Briseno* court eliminated the ascertainability requirement in the Ninth Circuit, saying that "an independent administrative feasibility requirement is unnecessary."[201] However, data privacy class actions are unique inasmuch as they are particularly widespread and often have victims in every circuit in the United States. For example, the Target data breach cases involved complaints in California, Colorado, Florida, Illinois, Louisiana, Massachusetts, Minnesota, Missouri, New York, Oregon, Rhode Island, Utah, and

[193] 18 U.S.C. § 2707(c).

[194] *Id.* § 2520(c).

[195] *Id.* § 2710(c)(2).

[196] *In re* Hulu Priv. Litig., No. C 11-03764, 2014 WL 2758598, at *15–16 (N.D. Cal. June 16, 2014).

[197] *Id.* at *15.

[198] *Id.* at *16.

[199] *See supra* Part II.A.

[200] 844 F.3d 1121, 1127 (9th Cir. 2017).

[201] *Id.*

Washington.[202] Research uncovered class action complaints in the *Gmail* case in jurisdictions from New Jersey[203] to California.[204] The widespread nature of data privacy suits makes it all but certain that complaints will be filed in jurisdictions that maintain a separate ascertainability requirement. The Supreme Court's aversion to certifying the question of ascertainability makes it likely the circuit split will persist for the time being.[205] Even more troubling, plaintiffs may not always be able to certify nationwide classes in the jurisdiction of their choice. In light of the Supreme Court's decision in *Bristol-Myers Squibb Co. v. Superior Court*, data privacy classes that cannot prove minimum contacts with California may not be able to avail themselves of the Ninth Circuit's favorable ascertainability caselaw.[206] Thus, while the Ninth Circuit no longer permits a heightened ascertainability requirement, there are many circuits that do embrace the requirement, and the victims of data breaches who live in those jurisdictions may not be able to escape the negative rulings in their circuits by virtue of a nationwide class.

D. Courts Should Not Create Different Outcomes for Similarly Situated Plaintiffs

The capacity of the ascertainability requirement to inhibit recovery in data privacy suits should raise concern. Damages have long been accepted as an effective mechanism to incentivize good behavior.[207] Though in a perfect world people would behave well out of a sense of altruism, the world is not perfect—therefore the law is replete with carrots and sticks.[208] Indeed, assigning monetary damages

[202] *See* Transfer Order, *In re* Target Corp. Customer Data Sec. Breach Litig., No. 13-cv-00793 (J.P.M.L. Apr. 3, 2014) (listing the various actions considered for consolidation across states).

[203] *See* Class Action Complaint at 1–2, Villani v. Google, Inc., No. 12-cv-01740 (D.N.J. Mar. 20, 2012).

[204] *See* Consolidated Class Action Complaint at 1, 6–7, *In re* Google, Inc. Priv. Pol'y Litig., No. 12-cv-01382 (N.D. Cal. June 8, 2012).

[205] *See generally* Briseno v. ConAgra Foods, Inc., 844 F.3d 1121 (9th Cir. 2017), *cert. denied*, 138 S. Ct. 313 (2017); Rikos v. Procter & Gamble Co., 799 F.3d 497 (6th Cir. 2015), *cert. denied*, 136 S. Ct. 1493 (2016); Mullins v. Direct Digit., LLC, 795 F.3d 654 (7th Cir. 2015), *cert. denied*, 136 S. Ct. 1161 (2016).

[206] 137 S. Ct. 1773, 1787 (2017) (Sotomayor, J., dissenting).

[207] *See, e.g.*, Beaulieu v. Finglam, Y.B. 2 Hen. 4, f. 18, pl. 6 (1401) (expounding the first articulation of negligence liability in 1401 AD).

[208] *See generally* Kristen Underhill, *When Extrinsic Incentives Displace Intrinsic Motivation: Designing Legal Carrots and Sticks To Confront the Challenge of Motivational Crowding-Out*, 33 YALE J. ON REGUL. 213 (2016) (discussing possible downsides of the many legal "nudges" meant to encourage actions for the common good).

to undesirable acts can incentivize good behavior even where economic forces would not.[209] Injunctions, while preventing future abuses, typically do not have the requisite punitive effect to disincentivize bad behavior.[210] It is not improper to surmise that tech giants will likely be incentivized to safeguard data if every breach in a class encompassing millions carries thousands of dollars in penalties. Given lawmakers' technological ineptitude, plaintiff classes are likely one of the most powerful mechanisms for holding tech companies accountable. Indeed, studies suggest that class action plaintiffs are indeed *motivated* by a desire to hold societal actors accountable.[211]

Additionally, the diverging requirements of the circuits regarding ascertainability create an uneven legal landscape where certain plaintiffs are subjected to more exacting certification requirements than others.[212] A divergence that, as previously discussed, exerts particular influence on data privacy class actions.[213] Despite the widespread presence of federal circuit splits, the Framers of the Constitution expressed a clear preference for uniform application of federal law.[214] Uniform application of the law, however, was not solely the purview of the founders.[215] Indeed, even though the Federal Rules of Civil

[209] *See, e.g.*, Robert D. Cooter, *Economic Theories of Legal Liability*, 5 J. ECON. PERSPS. 11 (1991) (detailing how legal liability can incentivize externality minimization). *But see* Tracey L. Meares, *Rewards for Good Behavior: Influencing Prosecutorial Discretion and Conduct with Financial Incentives*, 64 FORDHAM L. REV. 851 (1995) (arguing that pecuniary penalties actually result in perverse incentives that contravene stated policy goals).

[210] *See, e.g.*, FEDERAL CONTROL OF BUSINESS: INJUNCTION § 175 (2020) ("[T]he purpose [of the injunction] is not punishment but is rather to eliminate and prevent violations of the antitrust laws.").

[211] *See, e.g.*, Stephen Meili, *Collective Justice or Personal Gain? An Empirical Analysis of Consumer Class Action Lawyers and Named Plaintiffs*, 44 AKRON L. REV. 67, 90 (2011).

[212] *Compare* Carrera v. Bayer Corp., 727 F.3d 300, 307 (3d Cir. 2013) (ruling that identification of plaintiffs must take place at the "class certification state"), *with* Mullins v. Direct Digit., L.L.C., 795 F.3d 654, 662 (7th Cir. 2015) (arguing that *Carrera*'s approach to ascertainability "misreads Rule 23" and that such decisions could wait until "later in the litigation").

[213] *See supra* Part I.D.

[214] *See* THE FEDERALIST No. 80, at 401 (Alexander Hamilton) (Ian Shapiro ed., 2009) (citing the existence of the federal judiciary as furthering the "necessity of uniformity in the interpretation of the national laws").

[215] *See* Thucydides, *The Funeral Oration of Pericles*, *in* PLUTARCH'S CIMON AND PERICLES 163, 165 (Bernadotte Perrin ed., 1910) (asserting that before the law "all citizens are on an equality").

Procedure extol the virtues of "speedy" and "inexpensive" resolution of suits, they also ostensibly aim for a resolution that is "just."[216]

At present, rather than ensuring equal protection of the law, ascertainability presents the following conundrum. In cases where perfunctory references to defendant's records are insufficient to establish an "administratively feasible" method of ascertaining the class, plaintiffs likely must either forego damages or take their chances requesting certification by affidavit. On one hand, forgoing damages diminishes the incentive of tech companies to safeguard user data.[217] On the other hand, establishing ascertainability by affidavit subjects plaintiffs to the incoherent judgments of courts as evidenced in *Hulu* and *Harris*.[218] While those lucky enough to live in circuits without ascertainability avoid this bleak situation, millions of others live in jurisdictions where ascertainability *is* a requirement.[219] For them, the only recourse would be transferring to a jurisdiction without the heightened ascertainability requirement, an option that has no guarantee of success and that the Supreme Court could foreclose. All of this is to say that ascertainability can (and already has) resulted in similarly situated parties receiving different outcomes.[220]

E. Courts' Current Approach to Ascertainability Undermines the Objective of Efficient Adjudication of Claims at the Base of Rule 23

Writing in 1967 (a year after the adoption of Rule 23), Benjamin Kaplan emphasized the principal of efficiency underlying the genesis of the rule, saying that the objective of the (b)(3) damages class is to "get at the cases where a class action promises important advantages of economy of effort and uniformity of result without undue dilution of procedural safeguards for members of the class or for the opposing party."[221] These "economies of effort" manifest most powerfully class actions' capacity to permit plaintiffs with small claims an incentive to

[216] Fed. R. Civ. P. 1.

[217] Adam Lamparello, *Online Data Breaches, Standing, and the Third-Party Doctrine*, 2015 Cardozo L. Rev. de novo 119, 128 (arguing that without the ability for plaintiffs to "recover damages," private companies will not have the incentive to "adopt stringent procedures").

[218] *See supra* notes 164–65 and accompanying text.

[219] *See supra* notes 82–85 and accompanying text.

[220] *Compare* Harris v. comScore, Inc., 292 F.R.D. 579, 588 (N.D. Ill. 2013) (finding that use of affidavits was "manageable"), *with In re* Hulu Priv. Litig., No. C 11-03764, 2014 WL 2758598, at *54 (N.D. Cal. June 17, 2014) (finding ascertainability was not satisfied despite similarities in claims and class to *comScore*).

[221] Benjamin Kaplan, *Continuing Work of the Civil Committee: 1966 Amendments of the Federal Rules of Civil Procedure (pt. I)*, 81 Harv. L. Rev. 356, 390 (1967).

bring a suit. The Supreme Court encapsulated this rationale in *Amchem Products, Inc. v. Windsor*, saying that "the policy at the very core of the class action mechanism is to overcome the problem that small recoveries do not provide the incentive for any individual to bring a solo action prosecuting his or her rights."[222]

Courts' approach to ascertainability in the context of data privacy, however, undermines this goal. In prohibiting the use of affidavits to satisfy ascertainability, the *Hulu* court effectively foreclosed monetary relief for the plaintiff class due to defendants' bad recordkeeping.[223] Though this does not necessarily inflict undue hardship on plaintiffs (damages are likely to be small anyway),[224] it does prevent the courts from effectively disposing of the class in a way that incentivizes good behavior on the part of defendants. If the only remedy left for data privacy classes is injunctive relief, society, rather than plaintiffs, will be left poorer, as defendants will have no incentive to behave in a socially responsible way.[225]

A useful point of comparison is the jurisprudence surrounding consumer class actions. Courts' tolerance of ascertainability by affidavit in consumer class actions promotes efficiency through the use of compensatory damages.[226] There, courts embrace the use of affidavits as a way to establish ascertainability when defendants' records are insufficient to identify class members at the certification stage.[227] In doing so, the court creates a system where compensatory damages, though small, aggregate into a large enough penalty to incentivize good behavior without creating the incentive to falsify claims. In the data privacy context, though compensatory damages are less easily calculable,[228] nominal damages could serve a similar function, provided Congress amends legislation to permit them.[229] If courts substitute the use of nominal damages for compensatory damages, but otherwise mimic consumer class jurisprudence (as this Note suggests

[222] 521 U.S. 591, 617 (1997).

[223] *In re Hulu Priv. Litig.*, 2014 WL 2758598, at *13–14.

[224] *See, e.g.*, Lawrence J. Ball, *Damages in Class Actions: Determinations and Allocations*, 10 B.C. L. REV. 615, 623 (1969) ("Usually the individual damages [in a class action] that without the device of a class suit the plaintiff would not be afforded any relief.").

[225] *See supra* Part I.B.

[226] *See infra* Part III.B.

[227] *See, e.g.*, Boundas v. Abercrombie & Fitch Stores, Inc., 280 F.R.D. 408, 417–18 (N.D. Ill. 2012) (permitting plaintiffs to employ affidavits in establishing ascertainability provided damages are small).

[228] *See supra* note 165 and accompanying text.

[229] *See infra* Part III.C.

they should), they will both incentivize good behavior as well as permit the efficient adjudication of claims, in line with the original policy goals of Rule 23. This, of course, requires legislative action to mitigate high statutory damage minimums,[230] as well as court cooperation.

III. CONGRESS SHOULD AMEND FEDERAL DATA PRIVACY STATUTES TO PROVIDE DAMAGES IN A NOMINAL AMOUNT, AND COURTS SHOULD PERMIT ASCERTAINABILITY BY AFFIDAVIT

This Part proposes a two-part solution to the capricious application of ascertainability in data privacy suits. To begin, Congress ought to amend data privacy legislation to permit lower damages awards. This would preclude courts from penalizing plaintiffs for large statutory damage provisions in popular data privacy statutes. Additionally, courts should draw upon existing consumer class action jurisprudence and let plaintiffs satisfy the requirement of ascertainability through affidavit. As some courts have already noted, such action would run little practical risk of fraudulent claims while simultaneously creating an aggregate financial impact sufficient to incentivize responsible behavior.[231]

A. CONGRESS SHOULD AMEND THE STORED COMMUNICATIONS ACT AND OTHER DATA PRIVACY STATUTES TO PERMIT NOMINAL DAMAGES

To prevent courts from using large statutory damages awards as a reason to preclude affidavit use (and therefore, ascertainability), Congress should enact a statute creating a cause of action for data breaches and ensure the legislation awards plaintiffs nominal damages. Such a statute would preclude the reasoning employed by the *Hulu* court in finding a lack of ascertainability.[232] Currently, popular statutes for data privacy class actions impose strict minimums for damages in civil suits. For instance, the Stored Communications Act, while providing a private right of action, imposes a $1,000 required *minimum* of damages for each claim.[233] The Video Privacy Protection Act, cited by the *Hulu* court, awards a minimum of $2,500 per violation.[234] Congress should assiduously avoid minimum civil damages awards approaching these levels. Replicating generous awards might

[230] *See infra* Part III.A.

[231] *See infra* notes 262–68, 272–74 and accompanying text.

[232] *See supra* notes 196–98 and accompanying text.

[233] 18 U.S.C. § 2707(c) (requiring that persons recovering under the statute shall not recover "less than the sum of $1,000").

[234] *Id.* § 2710(c)(2)(A).

make the success of suits contingent upon the diligence with which defendants keep records.[235]

In so legislating, Congress should also endeavor to avoid the mistakes of recently passed state legislation and emulate more sensible legislation. New York, for instance, recently enacted the Stop Hacks and Improve Electronic Data Security (SHIELD) Act.[236] New York's law broadens existing statutory definitions to prohibit any unauthorized access to private or personal information.[237] While the law correctly assigns a $20 fee for each documented breach and avoids the obstacles that plague common-law theories of relief, it also suffers from shortfalls.[238] For instance, it caps damages at $250,000,[239] a sum unlikely to encourage good behavior in the wealthiest defendants.[240] Further, the law permits civil suits but only by the state attorney general, thereby depriving victims of the ability to pursue recourse.[241]

Conversely, California recently enacted the California Consumer Privacy Act (CCPA).[242] Since its passage, "more than a dozen class action[s]" have been filed in California courts.[243] Unlike the New York legislation, the CCPA gives consumers a private right of action.[244] What's more, the law imposes a maximum civil liability of $750 per consumer.[245] Not only is this award far below the $2,500 that the *Hulu* court found to be so objectionable, but the law also sets the minimum at a mere $100,[246] thereby permitting plaintiffs to address the *Hulu* court's concerns and reduce damages.[247]

[235] *See, e.g.*, *supra* note 64.

[236] *See* Dimitri Sirota, *Why U.S. Companies Should Know About the CCPA and New York SHIELD Act*, FORBES (Sept. 16, 2020), https://www.forbes.com/sites/forbestechcouncil/2020/09/16/why-us-companies-should-know-about-the-ccpa-and-new-york-shield-act [https://perma.cc/VAT9-3PYV] (discussing implications of SHIELD Act).

[237] N.Y. GEN. BUS. LAW § 899-AA (Consol. 2020).

[238] *Id.* § 899-AA(6)(a).

[239] *Id.*

[240] *See* Marty Swant, *The World's Most Valuable Brands 2020*, FORBES, https://www.forbes.com/the-worlds-most-valuable-brands [https://perma.cc/YMM6-T4VK] (valuing the mere brands of Apple at $241.2 billion, Google at $207.5 billion, and Microsoft at $162.9 billion).

[241] N.Y. GEN. BUS. LAW § 899-AA(6)(a).

[242] *See* Sirota, *supra* note 236.

[243] *See id.*

[244] CAL. CIV. CODE § 1798.150(a)(1) (2020).

[245] *Id.* § 1798.150(a)(1)(A).

[246] *Id.*

[247] *See supra* note 165.

However, even if the CCPA proves to be a perfect device for California class actions, it would still be insufficient to afford relief to nationwide classes. Data privacy victims are seldom (if ever) confined within particular states,[248] and remaining avenues of relief are troublingly fraught. Other theories of pleading a cause of action in data privacy class actions include the Computer Fraud and Abuse Act (CFAA), state common-law theories of breach of contract and trespass to chattels, and state computer crime laws.[249] However, such alternate theories do not serve the interests of judicial efficiency as effectively as federal provisions awarding statutory damages. To begin, the CFAA requires plaintiffs to prove $5,000 in damages before they can plead a civil cause of action.[250] Further, courts have not uniformly determined whether plaintiffs can aggregate damages under CFAA to meet the $5,000 threshold.[251] Given courts' tendency to award low damages for misplacement of data, it is unclear whether plaintiffs could individually clear the $5,000 requirement to successfully plead a private cause of action.[252] As such, CFAA does not present an efficient alternative to the Stored Communications Act and other laws awarding statutory damages.

Common-law theories of trespass to chattels have differing viability from state to state, thereby undermining their efficacy in sustaining a nationwide class (which maximizes efficiency and gives plaintiffs access to federal court).[253] Breach of contract theories leave out plaintiffs who did not have a contract with the defendant, such as non-Yahoo-using recipients of Yahoo messages in the *Yahoo*

[248] *See supra* Introduction.

[249] Kathleen C. Riley, Note, *Data Scraping as a Cause of Action: Limiting Use of the CFAA and Trespass in Online Copying Cases*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 245, 265 (2018) (detailing various theories of liability for data privacy cases).

[250] 8 U.S.C. § 1030(g).

[251] *See, e.g.*, Harris v. comScore, Inc., 292 F.R.D. 579, 589 n.8 (N.D. Ill. 2013) (leaving unresolved the question of whether plaintiff class members can aggregate damages to meet CFAA's $5,000 damages requirement).

[252] *See, e.g.*, *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14 (D.D.C. 2014) (finding that, without evidence of data misuse, the harm resulting from the loss of data was insufficient to confer standing); Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (finding that mere loss of data, compared to actual misuse, was insufficient to confer standing).

[253] *Compare* Matzan v. Eastman Kodak Co., 134 A.D.2d 863 (N.Y. App. Div. 1987) (refusing to allow a trespass to chattels theory of damages if the intangible property was not merged with something tangible), *with* CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (finding that electronic signals in the transmission of personal data are sufficiently tangible to support a trespass to chattels theory of damages).

litigation.[254] As such, a federal law permitting nominal damages would provide a standard theory of liability that enables nationwide classes while removing incentives for plaintiffs to fabricate claims—the contingency that so preoccupied the *Hulu* court.[255]

Specifically, this Note suggests nominal damages of approximately $100. Apart from the numeric appeal of $100, this amount closely approximates awards that other courts have found acceptable when established exclusively by affidavit. In *Mullins v. Direct Digital, L.L.C.* the court encountered a prospective class where the plaintiffs proposed to establish ascertainability exclusively through the use of affidavits.[256] Noting the complete lack of evidence of any fraudulent claims and the fact that only a tiny proportion of an average class typically submits a claim, the court found that "claims of this magnitude [are unlikely to] have provoked the widespread submission of inaccurate or fraudulent claims."[257] While some courts will still have to adjust their jurisprudence (indeed, adjusting jurisprudence is part of this Note's solution), circuit court caselaw lends support to $100 as an acceptable medium.[258] The rational counterargument that reducing awards will disincentivize participation is somewhat undermined by the fact that many class actions give exceedingly low awards,[259] and participation is low to begin with.[260]

B. Courts Should Adopt Consumer Class Action Jurisprudence Permitting More Liberal Use of Affidavits To Establish Ascertainability

Just as important as permitting statutory damages, courts will also need to play along and permit satisfaction of the ascertainability requirement through affidavits when defendant records are

[254] *In re* Yahoo Mail Litig., 308 F.R.D. 577, 582 (N.D. Cal. 2015) (including plaintiffs who did not have accounts with Yahoo but had lost data when they emailed Yahoo accounts).

[255] *In re* Hulu Priv. Litig., No. C 11-03764, 2014 WL 2758598, at *16 (June 17, 2014).

[256] 795 F.3d 654, 669 (7th Cir. 2015).

[257] *Id.* at 667.

[258] *Id.*

[259] *See, e.g.*, *Open Class Action Lawsuit Settlements You Can Claim!*, TOP CLASS ACTIONS, https://topclassactions.com/category/lawsuit-settlements/open-lawsuit-settlements [https://perma.cc/QJ9N-ZF7A] (listing potential claims of $2.50, $53.33, $33, $19.99, and $10).

[260] *See* Alison Frankel, *FTC's Comprehensive Study Finds Median Consumer Class Action Claims Rate Is 9%*, REUTERS (Sept. 10, 2019), https://www.reuters.com/article/us-otc-claimsrate/ftcs-comprehensive-study-finds-median-consumer-class-action-claims-rate-is-9-idUSKCN1VV2QU [https://perma.cc/E625-GX8B].

insufficient. Luckily, courts have already created an analogous and easily applicable body of caselaw regarding consumer classes. In *In re Dial Complete Marketing & Sales Practices Litigation*, plaintiff sued a soap manufacturer, but the defendant's records did not identify every member of the prospective class.[261] The court permitted the plaintiffs to establish ascertainability by affidavit, reasoning that denying certification due to the defendant's inept recordkeeping would render toothless many consumer class actions.[262] Similarly, in *Lyngaas v. Curaden AG*, the court certified a class even though plaintiffs sought to establish ascertainability through affidavit.[263] In doing so, the court identified ways the court could mitigate the risk of a false claim, holding that the benefit of protecting class viability outweighed the risk.[264] Still more courts—including in the previously mentioned *Mullins* decision[265]—have contributed to this jurisprudence, holding that, whatever the risks of fraudulent claims, establishing affidavits are a legitimate way of establishing ascertainability, thereby preserving the viability of small claims without records.[266]

Indeed, the concurrence in *Byrd v. Aaron's Inc.* concisely encapsulates the philosophy of this line of cases. In that case, a couple leased a laptop from Aaron's, a purveyor of office supplies.[267] When an Aaron's employee came to repossess the laptop for alleged lack of payments, the employee allegedly showed the Byrds a screenshot depicting web activity on the laptop.[268] In finding the class to be ascertainable, the court dismissed the defendants' contention that the plaintiffs were trying to establish ascertainability solely through unverified affidavits.[269] However, in doing so, the court indicated that unverifiable affidavits were an inappropriate method of establishing ascertainability, implying that to permit such affidavits would violate the

[261] *In re* Dial Complete Mktg. & Sales Pracs. Litig., 312 F.R.D. 36, 49 (D.N.H. 2015).

[262] *Id.* at 51 (arguing that preclusion of affidavits would thwart "[t]he policy at the very core of the class action mechanism," i.e., "to overcome the problem that small recoveries do not provide the incentive for any individual to bring a solo action prosecuting his or her rights" (citation omitted)).

[263] Lyngaas v. Curaden AG, 436 F. Supp. 3d 1019, 1024 (E.D. Mich. 2020).

[264] *Id.* at 1027.

[265] Mullins v. Direct Digit., L.L.C., 795 F.3d 654, 672 (7th Cir. 2015).

[266] *See, e.g.*, Rikos v. Proctor & Gamble Co., No. 11-cv-226, 2014 WL 11370455, at *6 (S.D. Ohio June 19, 2014); Boundas v. Abercrombie & Fitch Stores, Inc., 280 F.R.D. 408, 417–18 (N.D. Ill. 2012).

[267] 784 F.3d 154, 159 (3d Cir. 2015).

[268] *Id.*

[269] *Id.* at 170.

defendants' due process rights.[270] In a concurrence, Judge Rendell pointed out the absurdity of the concern about false affidavits.[271] He wrote that "chances that someone would, under penalty of perjury, sign a false affidavit . . . for the sake of receiving a [small] windfall . . . are far-fetched at best."[272] Far-fetched indeed. Just as importantly, Judge Rendell pointed out the deterrent effect of small claims in large suits saying that "[o]n the other hand . . . in the aggregate, this sum is significant enough to deter corporate misconduct" when the class is large.[273] With claims as large as those in data privacy suits, his is a point well-taken.

C. New Legislation and a More Permissive Attitude by Courts Would Address the Issues Currently Afflicting Data Privacy Litigation

Finally, this solution—in addition to being fair—addresses challenges currently confronting data privacy classes. Foremost among the challenges inherent in ascertainability's role in data privacy is inconsistent determinations despite similar facts.[274] Enacting legislation providing for $100 in nominal damages would empower courts to permit plaintiffs' establishment of ascertainability through affidavit by minimizing judicial fears of perjury. Having removed the enticement of a windfall award, *Hulu*'s concern for fraudulent claims becomes less credulous and permits a uniform embrace of affidavits. Such legislation and court cooperation would also address the fact that *Hulu*'s focus on the size of awards is uniquely problematic for data privacy classes, which employ statutes that grant generous awards.[275] Further, by enacting national legislation, Congress would ensure that recourse for data breaches is not contingent upon a plaintiff's state of residence or the state of the defendant's records. Currently courts' inconsistent application of ascertainability and the fragmented legislative landscape surrounding data privacy prevent the assurance of equal justice for similarly situated plaintiffs,[276] an ill that would be remedied with a national cause of action. Finally, nationwide legislation and court cooperation would further Rule 23's objectives, efficient disposition of otherwise economically unviable claims. As the

[270] *Id.*

[271] *Id.* at 172–77 (Rendell, J., concurring).

[272] *Id.* at 175.

[273] *Id.*

[274] *See supra* Part II.A.

[275] *See supra* Part II.B.

[276] *See supra* Part II.D.

discussion of standing indicated, courts rarely characterize injuries from data breaches in large, concrete terms.[277] The uncertainty, or small size, of individual awards ensures that the vast majority of claims would not be sustainable on an individual basis.[278] As a result, without the incentives provided by the prospect of substantial damages, defendants have very little incentive to behave responsibly.[279] Providing an acceptably low statutory award of damages, and the cooperation of courts, would obviate the glaring deficiencies in the current system.

CONCLUSION

Data breaches are not going anywhere.[280] As such, data privacy class actions likely are not going anywhere either. As long as the Supreme Court refuses to settle the ascertainability circuit split, district and circuit courts' unsupervised and inconsistent approaches to ascertainability will also persist. This conundrum puts data privacy litigants in an awkward position. If defendants' records do not conclusively establish class membership, plaintiffs face an uncomfortable catch-22. To avoid the issue of ascertainability, plaintiffs must limit themselves to an injunctive class.[281] If plaintiffs seek damages (with all their deterrent and compensatory advantages) and defendant's records are insufficient to identify every class member, plaintiffs risk denial of certification based on ascertainability.[282] What is more, if they seek to correct gaps in defendants' records with affidavits, they risk the possibility of courts holding a facet of their best theories for relief (the generous statutory damages in federal statutes) against them.[283] Even if courts do not perseverate on the issue of large damage awards, plaintiffs still have to navigate courts' conflicting views on "manageability."[284] The existing situation provides neither clarity nor relief, and it fails to incentivize good behavior.

However, if Congress amends statutes like the Stored Communications Act to provide for nominal damages and courts cooperate, the situation might improve. To begin, pleading nominal claims in large

[277] *See supra* Part I.D.

[278] *See supra* Part II.E.

[279] *See supra* Part II.D.

[280] *See supra* notes 5–16 and accompanying text.

[281] *See, e.g.*, *In re* Yahoo Mail Litig., 308 F.R.D. 577, 596–97 (N.D. Cal. 2015) (finding that (b)(2) injunctive classes did not have an ascertainability requirement).

[282] *See supra* Part III.B.

[283] *See supra* Part II.B.

[284] *See supra* Part II.A.

quantities—many data privacy classes include vast numbers of members—would likely impose a deterrent effect on data privacy defendants. As for compensation, though plaintiffs would certainly not receive the windfall the Stored Communications Act and other statutes currently provide,[285] nominal damages are better than nothing. Finally, if courts cooperate and accept affidavits as a matter of course under laws like the Stored Communications Act, parties will achieve a modicum of predictability they currently lack. In doing so, the legislature and courts will minimize the ascertainability circuit split's capacity to inflict inequitable outcomes.

[285] *See, e.g.*, Stored Communications Act, 18 U.S.C. § 2707(c) (awarding at least $1,000 per claim).