Harvard Journal of Law & Technology
Volume 37, Number 3 Symposium 2023

CERTIFYING PRIVACY CLASS ACTIONS

Ignacio Cofone[*]

ABSTRACT

Privacy class actions are undertheorized. Courts are increasingly called upon to adjudicate them when they arise from corporate business practices and data security events. But, even when they overcome problems of standing and compensation, courts lack frameworks for constituting and certifying a class in view of shared intangible losses and harms. Consequently, despite the importance of class actions for access to justice and corporate compliance, their success in these two aims is hindered. This Essay provides a tool for identifying which losses and harms to people's privacy can and should be grouped in a class. It proposes using opacity loss, which is inversely related to the probabilistic knowledge gained by a third party, for assessing class commonality. It aims to provide courts with a framework for assessing these claims following data practices that better achieves the aims of civil procedure and privacy law.

[*] Canada Research Chair in AI Law & Data Governance, McGill University Faculty of Law. ignacio.cofone@mcgill.ca. This paper benefited from comments received at the *Harvard JOLT*-UIowa IBL Symposium: Beyond the FTC. Many thanks to Jérémy Boulanger-Bonnelly, Mihailis Diamantis, Kirsten Martin, Helen Nissenbaum, Geneviève Saumier, Konstanze von Schütz, Katherine Strandburg, Daniel Weinstock, and Jonathan Zittrain for their helpful comments. I am also grateful to Rachel McKenzie for her outstanding research assistance, the SSHRC Canada Research Chairs program for providing research funding, and the editors of the *Harvard Journal of Law & Technology* for superb editing.

TABLE OF CONTENTS

I. INTRODUCTION

Privacy class actions are paradigm-shifting. They stand to become a key legal vehicle to hold corporations accountable for privacy violations given their rapid development and the surging number of lawsuits filed in recent years. Privacy class actions are set to shift the corporate liability landscape for companies that handle personal information and change how people seek redress for privacy violations.[1]

Developments in privacy class actions, which allow a representative to bring a claim against a defendant on behalf of a group of people in a single action, raise issues of substantive and procedural law. They test the boundaries of tort law and consumer law, as well as the traditional procedures governing class action litigation. Their impact exceeds privacy, and the outcomes of ongoing and future cases stand to be integral to the evolution of these fields of law.

The main uncertainty with privacy class actions, as identified by courts, exists at the intersection of substantive and procedural law. When considering claims that implicate privacy, courts are unsure how to determine intangible privacy harm. Courts' difficulty with defining and identifying intangible privacy harm is problematic considering that

[1] A class action is a legal proceeding in which a group of individuals with claims against a defendant can bring those claims to court in a single action. While I refer to class actions in this Essay, most of the considerations in this Essay apply to the bringing of any collective claim following a wrongful act that has similarly harmed numerous victims.

the harm plays a key role in granting class certification.[2] This leads to inconsistent results at the district and appellate levels as to which class actions proceed and which do not.

There is little insight into how courts may determine which privacy class actions to certify — an issue closely related to tracing the line between concrete and particularized harm and risk of future harm for the purposes of standing and compensation.[3] Scholarship on the topic, similarly, has provided little guidance on how courts should approach certification in privacy class actions. This exists in contrast to a growing trend towards class certification in favor of plaintiffs for some types of privacy class actions, particularly after a data breach.[4] In such legal and economic contexts, courts will be increasingly called on to grapple with evolving notions of privacy harm at trial and will require a tool to evaluate intangible privacy harm.

There are two ways to unify plaintiffs, depending on the basis for their lawsuit. When plaintiffs sue on the basis of tort law or a statute without an explicit harm requirement, the class can be ascertained on the basis of a shared loss built on a nondichotomous, or continuous, notion of privacy.[5] Federal statutes that require harm are more complicated — plaintiffs may not share downstream harms in a class action, but they almost always share intangible privacy harm, which should satisfy the commonality requirement.[6]

The Essay proceeds as follows. Part II explains why class actions are fundamental for the effectiveness of privacy law, yet they consistently fall short of the task under their current framing. Part III proposes how to overcome their limitations with a framework for unifying classes of plaintiffs. Part IV explores the implications for two questions at the intersection of policy and doctrine — subclasses of plaintiffs and risks of frivolous litigation.

[2] *See* Matthew S. DeLuca, Note, *The Hunt for Privacy Harms After* Spokeo, 86 FORDHAM L. REV. 2439, 2466–67 (2018).

[3] *See* Molly Reynolds, *Class Actions in Canada Part 4: A Cross-Border Perspective on Privacy Class Actions*, TORYS (July 19, 2018), https://www.torys.com/insights/publications/2018/07/class-actions-in-canada-part-4-a-cross-border-perspective-on-privacy-class-actions [https://perma.cc/R53W-Q7RX].

[4] *See* Travis LeBlanc & Jon R. Knight, *A Wake-Up Call: Data Breach Standing is Getting Easier*, 4 CYBERSECURITY L. REP. 1, 1 (2018); *see also* William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1152 (2019).

[5] *See infra* Section III.B.

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

II. Crucial for Privacy Redress and Consistently Falling Short

A. The Importance of Class Actions for People's Privacy

Private rights of action are key to privacy and data protection, as they are for consumer protection more generally.[7] As Mark Rotenberg and David Jacobs write, "[t]he enforcement of rights is a critical requirement of privacy law. Absent actual enforcement, there is little meaningful incentive for companies to comply with privacy requirements. Enforcement helps to ensure that the individuals whose privacy is placed at risk are fairly compensated."[8]

In practice, overcoming the information and power asymmetries that exist in data collection, processing, and sharing requires combining public and private enforcement.[9] Lawsuits allow individuals to influence which cases are brought, draw attention to facts about blameworthy security practices, and provide redress to victims while acting as a deterrent against rule breaches.[10] Lawsuits can be a bigger deterrent than administrative fines if compensation is estimated adequately, particularly in jurisdictions without large fines.[11] Private rights of action alleviate the regulatory burden on administrative agencies, reduce the risk of agency capture, and pressure companies to comply with the law.[12]

However, relying on private rights of action for enforcement has a key weakness. Often, claims are too numerous and too small to be

[7] *See* Janet Walker, Douez v Facebook *and Privacy Class Actions*, *in* CLASS ACTIONS IN PRIVACY LAW 56, 67–72 (Ignacio Cofone ed., 2020); *see also* Jackson Erpenbach, Note, *A Post*-Spokeo *Taxonomy of Intangible Harms*, 118 MICH. L. REV. 471, 473, 484–90 (2019) (applying the *Spokeo* standard to plaintiffs raising a statutory violation under a private right of action).

[8] Marc Rotenberg & David Jacobs, *Enforcing Privacy Rights: Class Action Litigation and the Challenge of* cy pres, *in* ENFORCING PRIVACY: REGULATORY, LEGAL AND TECHNOLOGICAL APPROACHES 307, 307 (David Wright & Paul De Hert eds., 2016).

[9] Lauren Henry Scholz, *Private Rights of Action in Privacy Law*, 63 WM. & MARY L. REV. 1639, 1646–48 (2022); *see also* BECKY CHAO, ERIC NULL & CLAIRE PARK, A PRIVATE RIGHT OF ACTION IS KEY TO ENSURING THAT CONSUMERS HAVE THEIR OWN AVENUE FOR REDRESS, *available at* https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/a-private-right-of-action-is-key-to-ensuring-that-consumers-have-their-own-avenue-for-redress [https://perma.cc/UTP6-453M] (explaining how states could play a vital role in public and private enforcement).

[10] *See generally* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 781 (2018) (recognizing the importance of having a private right of action for data breach harms).

[11] *See* JAMES X. DEMPSEY, CHRIS JAY HOOFNAGLE, IRA S. RUBINSTEIN & KATHERINE J. STRANDBURG, BREAKING THE PRIVACY GRIDLOCK: A BROADER LOOK AT REMEDIES 28–32 (2021), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839711 [https://perma.cc/KB72-H4BF]; Walker, *supra* note 7, at 68–69.

[12] *See* Solove et al., *supra* note 10, at 781–82; Scholz, *supra* note 9, at 1655–63.

litigated individually.[13] It is common for the cost for individual plaintiffs to litigate their violated rights to be expected to exceed the compensation they can receive.[14] Privacy statutes, accordingly, are designed to protect the public as a whole and not simply resolve private disputes.[15] Due to the frequency of harm producing numerous and small claims, the lack of widely recognized collective privacy proceedings undermines their effectiveness.

The claims raised in privacy class actions are often worth little on an individual basis. For example, many privacy violations are litigated under the Fair Credit Reporting Act ("FCRA")[16] and the Fair and Accurate Credit Transactions Act ("FACTA").[17] Yet, even willful noncompliance with the FCRA or FACTA entitles plaintiffs only to meager statutory damages — $100 to $1,000 per violation.[18] Most other individual privacy claims either involve similarly low compensation or go unrecognized.[19]

Class actions are key to privacy for the same reason that they are to consumer protection. Privacy actions suffer in greater ways from this cost-ineffectiveness problem because of how data harms materialize.[20] Data harms are often spread among a larger group and harder to identify than typical consumer harms.[21] Together, this leads to low individual amounts of compensable harm, decreasing already low incentives to sue. In most cases, plaintiffs would obtain awards that are so low that most people are unlikely to commence these claims.[22]

The lack of cost-effective options to bring individual privacy claims disadvantages victims.[23] Only severe data harms provide

[13] IGNACIO COFONE, THE PRIVACY FALLACY: HARM AND POWER IN THE INFORMATION ECONOMY 139 (2023).

[14] *See* Lauren Henry Scholz, *Privacy Remedies,* 94 IND. L.J. 653, 685–87 (2019); *see also* Dalia Ramirez, *If You Get a Class Action Settlement Notice, Here's What to Consider When Deciding to Join or Opt Out*, L.A. TIMES (May 13, 2023, 5:00 AM), https://www.latimes.com/business/story/2023-05-13/if-you-get-a-class-action-settlement-notice-heres-what-to-consider-when-deciding-to-join-or-opt-out [https://perma.cc/JZ79-3CNC] (outlining incentives and disincentives to joining a class action settlement).

[15] Erpenbach, *supra* note 7, at 473–74.

[16] 15 U.S.C. § 1681 (West).

[17] 15 U.S.C. §§ 1681, 9701–08; *see* Calli Schroeder, *Intangible Privacy Harms Post-*Spokeo, INT'L ASS'N OF PRIV. PROS. (Dec. 15, 2016), https://iapp.org/news/a/intangible-privacy-harms-post-spokeo/ [perma.cc/8PD7-LH68]; Peter C. Ormerod, *Privacy Injuries and Article III Concreteness,* 48 FLA. STATE UNIV. L. REV. 133, 136, 183 (2020).

[18] Ormerod, *supra* note 17, at 149; *see also* 15 U.S.C. § 1681n(a)(1)(A). Note that FCRA and FACTA rely on the same damages provision.

[19] Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. Rev. 793, 810–15 (2022).

[20] Thomas E. Kadri & Ignacio Cofone, Cy Près *Settlements in Privacy Class Actions*, *in* CLASS ACTIONS IN PRIVACY LAW 99, 105 (Ignacio Cofone ed., 2020).

[21] *Id.*

[22] *Id.* at 100.

[23] Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 831 (2020).

enough reason to individually go through a costly and lengthy judicial process. As a result, few people can afford to litigate harms that are not debilitating. Individual private actions do not adequately address data that uniquely affects the most disadvantaged, such as unfair insurance premium increases or algorithmic discrimination in securing new employment.[24]

The lack of cost-effective options to bring privacy claims presents a systemic problem, too. Corporations are not deterred from harmful data practices if liability is hypothetical.[25] Insufficient private enforcement is also ineffective at ensuring deterrence. Because of their low compensation coupled with the costs of litigation, private rights of action in privacy law work best as part of a mechanism of collective redress, such as class actions.

Even if commenced, most of these individual claims would be litigated in small claims courts. In most states, small claims courts hear civil cases for amounts up to about $15,000.[26] But small claims courts do not set precedent.[27] Because individual privacy awards are often small,[28] the lack of collective redress that would move these cases to regular courts impedes the formation of precedent and thus development of case law. Consequently, the development of privacy law is impeded by both under-litigation and litigation in small claims courts that do not set precedent.

That issue makes class actions crucial for privacy law. Class actions are a means by which rights that would be too costly to litigate individually can be vindicated. By coalescing claims from people whose rights have all been similarly violated to obtain a judgment against a defendant, class actions enable courts to adjudicate behaviors that cause serious and widespread harm in the aggregate. Class actions,

[24] *See* Andrés Páez, *Negligent Algorithmic Discrimination*, 84 L. & CONTEMP. PROBS. 19 (2021).

[25] *See* Wayne Unger, *Reclaiming Our Right to Privacy by Holding Tech. Companies Accountable*, 27 RICH. J.L. & TECH. 1, 16–21 (2020).

[26] Ann O'Connell, *50-State Chart of Small Claims Court Dollar Limits*, NOLO, https://www.nolo.com/legal-encyclopedia/small-claims-suits-how-much-30031.html [https://perma.cc/EQ5P-E6ZQ]. States with higher limits are Delaware ($25,000), Tennessee ($25,000), and Texas ($20,000). *Id.* Some states, such as Kentucky, have a limit as low as $2,500. *Id.*

[27] *See* Eric Steele, *The Historical Context of Small Claims Courts*, 6 AM. BAR FOUND. RSCH. J. 293, 299, 346–47 (1981); Victoria Haneman, *Bridging the Justice Gap with a (Purposeful) Restructuring of Small Claims Courts*, 39 W. NEW ENG. L. REV. 457, 465 n.36 (2017); *see also* Megan Leonhardt, *Consumers Can't Sue Some of the Biggest Companies in the US— Here's What That Means for You*, CNBC (July 12, 2019, 10:49 AM), https://www.cnbc.com/2019/07/12/why-you-cant-sue-fortune-100-companies.html [https://perma.cc/9WP4-R2XA] (exposing corporations for circumventing consumers' rights in their user agreements).

[28] *See* Ormerod, *supra* note 17, at 149; DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT 56 (2022).

in other words, seek to address the problem of a lack of incentive to sue, which arises when there are numerous plaintiffs with small claims.

By aggregating similar individual actions, class actions increase the number and types of claims that can be litigated.[29] They improve access to justice by reducing the legal cost for each individual, which improves affordability and therefore the number of meritorious victims who can bring claims. Collective mechanisms provide redress that would otherwise be unavailable to people who are harmed but cannot afford litigation, either due to the cost of litigation or low potential rewards.[30] In most cases, lawyers are paid on a contingency fee basis with no upfront cost for class members.[31] Affordability is of particular importance in privacy claims, where success is uncertain and damages are likely to be low on a per-person basis.[32]

Similarly, class actions reduce informational costs at the individual level and avoid duplication of information acquisition costs at the social level.[33] Individuals who are harmed may not have the resources or knowledge required to seek legal recourse in privacy suits. Beyond pecuniary costs and lack of knowledge, class actions moderate other barriers that can prevent people from putting forth meritorious individual claims: limited language skills, age of the plaintiffs, psychological barriers to engaging with the claim, fear of retaliation by the defendant, and alienation from the law and courts.[34]

In sum, data harms are uniquely dispersed, usually impacting many people in small amounts. Therefore, few plaintiffs litigate privacy cases outside of a class. Because of their small expected awards, coupled with the costs of litigation, private rights of action in privacy law are of limited use individually. To have effective private enforcement, privacy law needs class actions.

B. Why Privacy Class Actions Fail

Class actions need commonality to be certified. To satisfy this requirement, there must be common issues of fact or law that affect all members of the class.[35] Privacy harms affect many people at the same

[29] Michael A. Eizenga & Emrys Davis, *A History of Class Actions: Modern Lessons from Deep Roots*, 7 CANADIAN CLASS ACTION REV. 3, 22 (2011).

[30] COFONE, *supra* note 13, at 160–61.

[31] Brian T. Fitzpatrick, *An Empirical Study of Class Action Settlements and Their Fee Awards*, 7 J. EMPIRICAL LEGAL STUD. 811, 837 (2010); Tyler Hill, Note, *Financing the Class: Strengthening the Class Action Through Third-Party Investment*, 125 YALE L.J. 484, 487 (2015).

[32] Citron et al., *supra* note 19, at 810–15.

[33] Jérémy Boulanger-Bonnelly, *Actions Collectives et Tribunaux Administratifs : Un Vide Juridictionnel à Combler*, 67 MCGILL L.J. 453, 460–61 (2022).

[34] *Id.*

[35] *See* Joseph A. Seiner, *Commonality and the Constitution: A Framework for Federal and State Court Class Actions*, 91 IND. L.J. 455, 485–86 (2016).

time from the same misconduct. This makes them good candidates for class actions, but it is also their downfall.

The harms caused by corporations in the information economy often impact a large number of people. They often affect larger groups than the economic harms that the law commonly addresses do.[36] In the information economy, harm comes from the fact that corporations collect, process, and hold personal information from many individuals to reveal profitable inferences and patterns.[37]

A persistent privacy law problem thus extends to class certification. U.S. federal courts often deny standing to privacy class actions for lack of an injury in fact.[38] They require the privacy violation to have led to a downstream injury that courts are used to identifying and measuring (such as a financial one).[39] As a consequence, people who suffered a privacy injury are systematically denied standing — before even starting a conversation about class certification.[40] Litigants who reach class certification face a new problem — lack of recognition as a class — with the same origin: lack of privacy harm recognition.

To increase access to justice, privacy class actions must overcome two intertwined obstacles. They must overcome the difficulty of proving compensable harm (a difficulty from privacy law), and they must overcome the difficulty of obtaining class certification (a difficulty from civil procedure).

Class actions are often undermined because individuals in the class suffer different downstream harms that prevent courts from unifying their claims. For example, some could have been subjected to identity theft as a result of unjust sharing of user data, but not all. These downstream harms do not impede the intangible privacy harm they have in common, as I argue below.[41]

To address the standing challenge that extends to certification, courts have undertaken different approaches. Three judicial approaches are worth noting. The first is relying on future harm. Some courts have granted class certification for threats of a future injury, such as an

[36] Kadri, *supra* note 20.

[37] *See* Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357, 411–14 (2022).

[38] *See* Citron, *supra* note 19, at 798.

[39] Ryan Calo, *Privacy Harm Exceptionalism,* 12 COLO. TECH. L.J. 361, 361–63 (2014) (describing courts' limited recognition of privacy harm outside established, material bounds); Ryan Calo, *Privacy Law's Indeterminacy*, 20 THEORETICAL INQUIRIES L. 33, 48 (2019); *see also* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2214 (2021) (inferring lack of standing from the lack of a consistent, concrete harm shared among all class members, as well as from a lack of a downstream injury).

[40] Ignacio Cofone, *Privacy Standing*, 2022 U. ILL. L. REV. 1367, 1371–76 (2022).

[41] *See infra* Section III.C.

increased risk of identity theft.[42] The second is looking into plaintiffs' post-misconduct behavior to find common harm, such as loss of time or economic expenses to prevent identity theft.[43] The third is examining the defendant's subsequent actions after the breach in their effort to identify a common behavior toward all plaintiffs.[44] Some courts, for example, have considered that a defendant's post-breach mitigating actions, such as providing free credit monitoring services, may constitute an admission of common injury.[45]

These positive developments are of some, but limited, usefulness. First, they face a doctrinal limitation. The Supreme Court severely limited federal courts' ability to rely on these considerations in a triad of cases: *Clapper v. Amnesty International USA*,[46] *Spokeo v. Robins*,[47] and *TransUnion LLC v. Ramirez*.[48] This does not invalidate the approaches described above, as state courts can use them and some federal courts, notably the Ninth Circuit, have resisted the Supreme Court's limitation.[49] Second, they have a policy limitation. The three trends replicate the challenge of finding common harm, as plaintiffs may have different risks of downstream harm, post-violation behaviors, or mitigating treatments from the defendant. Because these judicial approaches leave many plaintiffs out and they are inconsistently helpful across fact patterns, none of them have consistently helped courts certify classes of plaintiffs.

[42] *See, e.g.*, Remijas v. Neiman Marcus Grp., LLC., 794 F.3d 688, 696 (7th Cir. 2015); *In re* Adobe Sys., Inc. Priv. Litig., 66 F. Supp. 3d 1197, 1215 (N.D. Cal. 2014); Krottner v. Starbucks Corp., 628 F.3d 1139, 1142–43 (9th Cir. 2010); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632–34 (7th Cir. 2007); Galaria v. Nationwide Mut. Ins. Co., 663 Fed. Appx. 384, 388–89 (6th Cir. 2016).

[43] Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016); *cf.* Han cock v. Urb. Outfitters, Inc., 830 F.3d 511, 514 (D.C. Cir. 2015) (noting that a "pecuniary or emotional injury" would suffice for standing but finding none alleged).

[44] *See, e.g.*, *Remijas*, 794 F.3d at 694; *Lewert*, 819 F.3d at 967–68; *Galaria*, 663 Fed. Appx. at 389; *see also* Jordan Z. Dillon, *Standing on the Wrong Foot: The Seventh Circuit's Eccentric Attempt to Rescue Risk-Based Standing in Data Breach Litigation*, 56 WASHBURN L. J. 123, 138, 142–43 (2017).

[45] *See, e.g.*, *Remijas*, 794 F.3d at 694; *Lewert*, 819 F.3d at 967–68; *Galaria*, 663 Fed. Appx. at 389.

[46] 568 U.S. 398, 410–11 (2013).

[47] 136 S. Ct. 1540, 1549–50 (2016).

[48] 141 S. Ct. 2190, 2210–14 (2021).

[49] Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DEPAUL L. REV. 439, 451–52 (2017); Nathan Freed Wessler, *A Federal Court Sounds the Alarm on the Privacy Harms of Face Recognition Technology*, ACLU NEWS & COMMENTARY (Aug. 9, 2019), https://www.aclu.org/news/privacy-technology/federal-court-sounds-alarm-privacy-harms-face [https://perma.cc/UH7L-Q66U]. *See, e.g.*, Patel v. Facebook, 932 F.3d 1264 (9th Cir. 2019).

III. A PROPOSAL FOR CERTIFICATION

A. Legal Pathways for Privacy Class Actions

Privacy class actions can emerge from two legal pathways: through a privacy statute and privacy torts. These are not mutually exclusive.

The first pathway involves data practices that infringe upon a privacy statute. As opposed to data security events, these happen when the wrongdoing is part of a corporate practice or is authorized by management. Examples include collecting personal information illegally or using personal information for a purpose different than the one for which it was collected, breaching the purpose limitation principle.

Many federal and state privacy statutes give rise to this pathway by creating private rights of action.[50] Recent examples of their application are class action lawsuits against Clearview AI for building one of the largest facial recognition databases in history;[51] against Zoom for allegedly sharing data with Facebook;[52] against Six Flags for unauthorized collection of fingerprints;[53] and against Facebook for tracking its users' locations without their consent when they turned off their location history.[54]

The second legal pathway is privacy torts. There are four privacy torts: (1) appropriation of one's name, image, or likeness; (2) false light; (3) intrusion upon seclusion; and (4) public disclosure of private facts.[55] The first, appropriation, allows an individual to prevent the use of her name and picture for commercial purposes without her consent.[56] False light is implicated when someone uses true facts to create a false impression about someone else.[57] Intrusion upon seclusion gives people the right to prevent third parties from obtaining information about them by intrusive means.[58] Public disclosure of private facts allows people to prevent the publication of intimate facts about them.[59]

[50] *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681; Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506.

[51] Mutnick v. Clearview AI, Inc., No. 20 C 0512, 2020 U.S. Dist. LEXIS 144583, at *2 (N.D. Ill. Aug. 12, 2020).

[52] Isobel Asher Hamilton, *Zoom Is Being Sued for Allegedly Handing Over Data to Facebook*, BUS. INSIDER (Mar. 31, 2020, 6:21 AM), https://businessinsider.com/zoom-sued-allegedly-sharing-data-with-facebook-2020-3 [https://perma.cc/AA2K-B8Z7].

[53] Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1201 (Ill. 2019).

[54] Heeger v. Facebook, Inc., 509 F. Supp. 3d 1182, 1186 (N.D. Cal. 2020).

[55] RESTATEMENT (SECOND) OF TORTS § 652H (Am. L. Inst. 1977); William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

[56] RESTATEMENT (SECOND) OF TORTS § 652C (Am. L. Inst. 1977); *see, e.g.*, Blanch v. Koons 485 F. Supp. 2d 516 (S.D.N.Y. 2007).

[57] RESTATEMENT (SECOND) OF TORTS § 652E (Am. L. Inst. 1977); *see, e.g.*, *Godbehere v. Phoenix Newspapers, Inc.*, 783 P.2d 781, 787 (Ariz. 1989).

[58] *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 89–106 (7th ed. 2021).

[59] *See id.* at 114–48.

Privacy scholarship notes an expansion of these claims since the Second Restatement on Torts's original classification of privacy torts.[60] Privacy torts are more often than not used as support in class actions that also claim a violation of a privacy statute, merging both pathways.[61]

One recent example of a putative class action based on privacy torts took place in 2020 in *Davis v. Facebook, Inc.*[62] Represented by Perrin Davis, a group of users sued Facebook for tracking them illegally and continuing to collect their personal data after they had logged off from the platform.[63] The Ninth Circuit held that the plaintiffs had adequately alleged harm to privacy interests and had therefore established a sufficient claim for relief based on the tort of intrusion upon seclusion.[64]

The way to certify classes of plaintiffs, as the next two sections explore, depends on the legal pathway involved.

B. Opacity Loss for Torts and Statutes Without a Harm Requirement

Privacy analyses require a continuous, rather than a dichotomous, view of privacy.[65] This view asks whether someone formed a better picture of a data subject, avoiding false binaries such as that between "public" and "private" information.[66] One should do this by identifying whether an observer gained probabilistic information about someone.[67] This focus on probabilistic information allows one to capture potentially harmful inferences, which are derived probabilistically from collected personal information. For example, a probabilistic view of personal information can capture the inferences involved in facial recognition algorithms, which go beyond pictures and videos that are obtained directly to train them. I call this "opacity loss" to contrast it with privacy harm, but elsewhere I have called it "privacy loss."[68]

[60] *E.g.*, Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1828–52 (2010) (widening Prosser's taxonomy to allow for expanded notions of harm and a lowered burden of proof); Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 145–56 (2007) (discussing the expansion of the law of confidentiality in the late twentieth century, as well as a shift toward recognizing an American-style "right to privacy"). *But see* Neil M. Richards, *The Limits of Tort Privacy*, 9 J. TELECOMM. HIGH TECH. L. 357, 382–84 (2011).

[61] DeLuca, *supra* note 2, at 2458–64.

[62] Davis v. Facebook, Inc. (*In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 598 (9th Cir. 2020).

[63] *Id.* at 595–97.

[64] *Id.* at 598–600.

[65] NEIL RICHARDS, WHY PRIVACY MATTERS 32–33 (2021).

[66] *See* Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1365 (2015).

[67] Ignacio N. Cofone & Adriana Z. Robertson, *Consumer Privacy in a Behavioral World*, 69 HASTINGS L.J. 1471, 1488–1497 (2018) (outlining a framework for analyzing privacy loss that looks at whether an observer has a "clearer picture" about the observed than they did before, independently of whether that information is collected or inferred).

[68] *E.g.*, Cofone, *supra* note 40, at 1376–90.

A class action case illustrates this concept. In *Brown v. Google LLC*,[69] Chasom Brown sued Google in a class action on behalf of a class of users for tracking them, including outside of Google products, without their knowledge.[70] Google collects information about its users through tools like Google Analytics, Ad Manager, the "Sign in with Google" button, and others.[71] This information includes what people do online, what they are viewing, and what device they are viewing it on, among other details.[72] Google profits from selling targeted advertising spots based on this information, so more tracking allows the company to place those advertisements more effectively.[73]

Imagine a situation in which Google, to price advertising for plane tickets more effectively, would like to know Brown's willingness to pay for flights. Google is unable to collect that information directly: it cannot call Brown and ask how much he would pay. Instead, Google relies on statistical inferences. When Google has few data points about how much Brown is willing to pay for his next vacation flight, there is a wide range of potential prices. However, Google knows the overall distribution of that information in the general population. Some options, such as a willingness to pay $0 or $2,000, are unlikely. Other options, such as a willingness to spend between $200 and $500, are more likely because they are closer to the population average.

If Google were an individual, its ability to infer information would stop there. Assume that Google, instead, already has some information about Brown, such as his age.[74] Aggregating that information allows it to estimate from the more precise distribution of his age group, rather than the general population distribution.[75] This improves Google's probabilistic knowledge.[76] Google can then collect further data about Brown that allows it to form a clearer picture.[77] If Google tracks that Brown browses four-star hotels, this data point suggests that Brown has disposable income, so he is unlikely to pay $0 for flights or for a first-class flight. This data does not give Google complete certainty about

[69] 525 F. Supp. 3d 1049 (N.D. Cal. 2021).

[70] *Id.* at 1055–56.

[71] *Id.*

[72] *Id.*

[73] *See* Ben Popken, *Google Sells the Future, Powered by Your Personal Data*, NBC NEWS (May 10, 2018, 3:30 AM), https://www.nbcnews.com/tech/tech-news/google-sells-future-powered-your-personal-data-n870501 [https://perma.cc/KW67-AK62].

[74] David Nield, All the Ways Google Tracks You—And How to Stop It, Wired (May 27, 2019, 7:00 AM), https://www.wired.com/story/google-tracks-you-privacy/ [https://perma.cc/4JJR-5YK9].

[75] Rainer Mühlhoff, *Predictive Privacy: Collective Data Protection in the Context of Artificial Intelligence and Big Data*, BIG DATA & SOC'Y 1, Jan.–Jun. 2023, at 1.

[76] Katherine J. Strandburg, *Free Fall: The Online Market's Consumer Preference Disconnect*, 430 U. CHI. LEGAL F. 95, 98–130 (2013); Rainer Mühlhoff, *Predictive Privacy: Towards an Applied Ethics of Data Analytics*, 23 ETHICS INFO. TECH. 675 (2023).

[77] Mühlhoff, *supra* note 75.

the target information.[78] But, the more data Google assembles, the narrower that range of plausible numbers is for what Brown would spend.[79] Each time Google collects another data point, it becomes more certain. As Google gets more specific information, such as how much Brown previously paid for flights, it develops a better estimation, focusing on a narrower range of plausible options.[80] Google then forms a clearer picture of the target information by running analytics on this data. Each of these certainty-improving steps constitutes probabilistic inferences.[81]

Each increase in Google's certainty results in an equivalent opacity loss. Google's certainty and Brown's loss correlate because, in every knowledge-increasing step, Brown faces a "loss of obscurity."[82] The more certain Google is about the truth of its probabilistic knowledge about Brown, meaning there is a lower chance of error in its estimations, the higher Brown's opacity loss becomes. One can identify whether Brown had an opacity loss, even if Brown does not know it, by looking at whether Google's probabilistic knowledge about Brown improved.

The idea of probabilistic opacity loss is crucial in a world where actors affect our privacy by making inferences about us. In the information economy, we interact with recidivist privacy invaders who learn about us based on inferences.[83] A single data point rarely meaningfully increases the precision of a corporation's probabilistic knowledge. Instead, the inferences from a large amount of otherwise insignificant data points are revealing.[84]

This framing of losses relates to the importance of viewing privacy as a matter of degree.[85] This view captures situations where the loss is produced by aggregating innocuous data from hundreds of entities. It captures inferences, including in difficult situations where many different entities collected the information that led to those inferences. Binary conceptions of privacy are unhelpful in a social and economic context where pervasive corporate data practices reduce our privacy by different degrees.[86]

[78] Mühlhoff, *supra* note 76.

[79] *See* Daniel J. Solove, *Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, 118 NW. U. L. REV. 1081 (2024).

[80] *See* Strandburg, *supra* note 76, at 98–131.

[81] Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 COLUM. BUS. L. REV. 494 (2019); Solow-Niederman, *supra* note 37.

[82] *See* Hartzog et al., *supra* note 66, at 1363, 1369; Evan Selinger & Woodrow Hartzog, *Obscurity and Privacy*, *in* SPACES FOR THE FUTURE 119 (Joseph C. Pitt & Ashley Shew eds., 2018).

[83] Solow-Niederman, *supra* note 37; COFONE, *supra* note 13, at 19, 120–21.

[84] Strandburg, *supra* note 76, at 98–130.

[85] RICHARDS, *supra* note 65, at 21–34.

[86] Cofone, *supra* note 40, at 1389–90.

While Brown lost opacity through data collection, others lose opacity through third-party data sharing. Another class action against Google illustrates that dynamic.

In *Frank v. Gaos*,[87] Paloma Gaos sued Google on behalf of a class of users for sharing user search term information with other websites.[88] Gaos and other plaintiffs faced an opacity loss because Google provided information about them (i.e., their search terms) to third parties.[89] Google's estimation about them remained unchanged from the disclosure: sharing information to the third parties cannot teach it anything new about the users. By providing facts about its users to websites, instead, Google allowed those websites to improve *their own* probabilistic knowledge about the plaintiffs — they lost opacity toward the third parties, not toward Google. The plaintiffs faced an opacity loss, however, because Google enabled third parties to increase the certainty of their inferences.[90] Although plaintiffs' opacity loss was towards third parties, it would have been warranted for Google, rather than the third parties, to compensate them, as Google caused the loss.

Courts often struggle to determine when shared information remains protected by privacy[91] This struggle follows from a false public versus private information dichotomy. When one shares information with a group of people, and one expects them not to share it further, one loses some control over that information but expects privacy over it nonetheless.[92] That information may be known to those with whom the information was first shared but may remain unknown to others.[93] For the *Gaos* loss analysis, it would be irrelevant that Google already had its users' information (i.e., that the information was already "out there") and that Google acquired the information lawfully (with users' consent).

[87] 139 S. Ct. 1041 (2019) (per curiam).

[88] *Id.* at 1044; *see also In re* Google Referrer Header Priv. Litig., 465 F. Supp. 3d 999, 1007–10 (2020) (confirming users' concrete privacy interests in communications stored with electronic service providers).

[89] *Gaos*, 139 S. Ct. at 1044 ("The complaints alleged that when an Internet user conducted a Google search and clicked on a hyperlink to open one of the webpages listed on the search results page, Google transmitted information including the terms of the search to the server that hosted the selected webpage."); *see also* Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039, 1055, 1059–60 (2018).

[90] *See* Wachter et al., supra note 81.

[91] Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 920–25 (2005); *see also* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1107 (2002).

[92] Kirsten Martin, *Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms*, 30 BUS. ETHICS Q. 65, 87 (2020); *see also* Kirsten Martin & Helen Nissenbaum, *Privacy Interests in Public Records: An Empirical Investigation* 31 HARV. J.L. & TECH. 111, 140 (2017) (outlining empirical evidence on judgments about privacy interests).

[93] Strahilevitz, *supra* note 91, at 939 (2005); *see, e.g.*, Sanders v. ABC, 978 P.2d 67, 70, 74 (Cal. 1999).

The answer to whether information is private is found by assessing how information spreads. Network theory teaches us that information has the potential to spread to everyone.[94] To assess whether information is a "private matter," one should examine a counterfactual: whether the information would have reached the third party without the perpetrator.[95] Someone (probabilistically) reduces someone else's opacity when their data practice causes information that would have otherwise been unknown to become (better) known by someone.[96] Applied to *Frank v. Gaos*, one should ask if the third parties would have had the knowledge they obtained from Google without Google's disclosure of information. The answer is likely no.

Probabilistic losses are also relevant to tort law — even absent statutory breach. Loss by data sharing could fall under the tort of public disclosure of private facts if there is publication.[97] Under a hypothetical tort claim, Gaos' claim would be against Google, not the websites. The key difference between an intrusion upon seclusion tort and a public disclosure of private facts tort, in terms of the victim's loss, is not who the perpetrator is but whose probabilistic knowledge improved.[98] Under intrusion, the perpetrator improves their probabilistic knowledge about the target person.[99] Under disclosure, the perpetrator improves a third party's probabilistic knowledge.[100] The perpetrator is the same, while the type of loss differs.

A common violation sufficient to certify a class, when injury-in-fact requirements are absent, can be found through such shared loss. Shared opacity loss could satisfy the requirement of questions of law or fact common to the class by showing predominance of the common element.[101] This is the part of this Essay's proposal most relevant to state courts, which are not subject to Article III requirements.

[94] Strahilevitz, *supra* note 91, at 953; *see also* Stephen P. Borgatti & Daniel S. Halgin, *On Network Theory*, 22 ORG. SCI. 1168 (2011) (examining and complexifying the potential large-scale flows of information according to a network flow model).

[95] Strahilevitz, *supra* note 91, at 935, 953.

[96] *Id.* at 988.

[97] *See* Prosser, *supra* note 55, at 392–98.

[98] Cofone et al., *supra* note 89, at 1055, 1058–61.

[99] COFONE, *supra* note 13, at 122.

[100] *Id.*

[101] *See* Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 350 (2011) (focusing on what holds together plaintiffs' claims for class certification); *see also* Amgen, Inc. v. Conn. Ret. Plans & Tr. Funds, 568 U.S. 455, 466–67 (2013) (holding that materiality is not a prerequisite to class-action certification); Stockwell v. City & Cnty. of S.F., 749 F.3d 1107, 1111 (9th Cir. 2014) (dealing with the application of Rule 23(a) of the Federal Rules of Civil Procedure concerning certification and commonality); Ellis v. Costco Wholesale Corp., 285 F.R.D. 492, 506–07 (N.D. Cal. 2012) (describing the standard for commonality in class certification); Brown v. Nucor Corp., 785 F.3d 895, 902 (4th Cir. 2015) (describing the requirement of "questions of law or fact common to the class"); Amchem Prods., Inc. v. Windsor, 521 U.S. 591, 623 (1997) (discussing the predominance inquiry, which "tests whether proposed classes are sufficiently

C. Intangible Harm for Statutes That Require It

The common thread running through privacy class actions is that they stem from data practices that produce opacity losses. Not all privacy class actions emerge from the same wrong. Different types of privacy violations give rise to different private rights of action that can lead to class actions. Common examples include unauthorized access to personal information by third parties;[102] lack of notification when there is a statutory notification requirement;[103] unauthorized collection of personal information;[104] unauthorized disclosure of personal information;[105] and misuse of personal information.[106] Privacy law protects the collection, use, and dissemination of personal information,[107] and wrongs at any of these three stages can give rise to class actions when formal requirements are met.

Data practices in the information economy can harm people in various ways. These include reputational harm (e.g., when employers find inaccurate information about a job candidate), financial harm (e.g., identity theft), physical harm (e.g., doxing, the disclosure of personally identifiable information that leads to bodily harm), and discrimination (e.g., when a member of a nonvisible minority is outed).[108]

cohesive to warrant adjudication by representation"); FED. R. CIV. P. 23(a)(2). In *Dukes*, the Court indicated that certifying the class for its employee-wide discrimination claim required company-wide biased testing procedures or a general policy of discrimination. *Dukes*, 564 U.S. at 353; Cianan M. Lesley, *Making Rule 23 Ideal: Using a Multifactor Test to Evaluate the Admissibility of Evidence at Class Certification*, 118 MICH. L. REV. 149, 153 (2019). Privacy loss passes that level of commonality: for all users to sue a platform, a company-wide practice would be required, as a common mode of exercising discretion in disparate impact cases is analogous to a common mode of enabling data harms in privacy class actions. *Dukes* is one step away from generating an argument about opacity loss. *See Dukes*, 564 U.S. at 361–62. *Dukes* cites earlier caselaw stating that certification assessment involves considerations that are enmeshed in the factual and legal issues comprising the plaintiff's cause of action, suggesting a purposive approach to assessing commonality. *Id.* at 351. The next step to opacity loss as a unifying element can be made with one degree of inference: if the "glue" holding together plaintiffs' claims is *itself* shared opacity loss that can be probabilistically assessed, then this shared factual issue ought to be sufficient for establishing predominance.

[102] *See, e.g.*, In re Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295 (N.D. Ga. 2019); Complaint, Santana v. 23andMe, No. 3:23-cv-05147 (N.D. Cal. Oct. 9, 2023); *see also* Scholz, *supra* note 9, at 1651–55.

[103] *Cf.* Antman v. Uber Techs., Inc., No. 15-CV-01175, 2018 U.S. Dist. LEXIS 79371, at *10 (N.D. Cal. May 10, 2018) (noting that delay in notification alone is not enough for there to be standing but that delay that leads to further harm may be sufficient).

[104] *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018).

[105] *See, e.g.*, Frank v. Gaos*,* 139 S. Ct. 1041, 1044 (2019).

[106] *See, e.g.*, Simpson v. Facebook, Inc., 2021 ONSC 968, aff'd 2022 ONSC 1284 (Can. Ont.); *see also* Carlo Di Carlo, *Invasions of Privacy: Class Proceedings*, *in* DIGITAL PRIVACY: CRIMINAL, CIVIL AND REGULATORY LITIGATION 246 (Gerald Chan & Nader R. Hasan eds., 2018).

[107] *See, e.g.*, CAL. CIV. CODE § 1798.100(b) (West 2018).

[108] Citron et al., *supra* note 19; *see also* Citron, *supra* note 60, at 1811–19.

Such harmful results increasingly occur through inferences.[109] For example, if a neighborhood is classified as one where many people with high blood pressure live, insurance companies may increase rates based on ZIP codes.[110] Platforms such as Facebook often allow advertisers to filter based on inferred demographic and behavioral features.[111] Manipulating people into buying things they do not need, which one might call "behavior modification," is inference-enabled.[112]

Besides these downstream harms, data practices produce a distinct harm: intangible privacy harm. In Ryan Calo's words, "[j]ust as a burn is an injury caused by heat, so is privacy harm a unique injury with specific boundaries and characteristics."[113] This harm derives from opacity losses that tort law recognizes—protecting us from others learning intimate facts about us—exemplified with the opening of letters and professional secrecy. But it does so in a new social and economic context.

The problem of class certification is caused by courts identifying only downstream harms (or the risk thereof), while neglecting intangible privacy harm, which is often a unifying element among class members. Information about groups of people that is (illegally) collected, misused, or sold by the same data practice is poised to have a similar effect on their privacy. It is common that a subset of victims suffers downstream harms;[114] those harms are a consequence of the opacity loss and privacy harm.[115]

[109] *See* Solow-Niederman, *supra* note 37.

[110] Marshall Allen, *Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates*, PROPUBLICA (July 17, 2018, 5:00 AM), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates [https://perma.cc/P5W4-XXLZ]; *see* Solon Barocas & Helen Nissenbaum, *Big Data's End Run Around Anonymity and Consent*, *in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 44, 45–46 (Julia Lane, Victoria Stodden, Stefan Bender & Helen Nissenbaum eds., 2014).

[111] *See, e.g.*, Ariana Tobin, *Facebook Promises to Bar Advertisers from Targeting Ads by Race or Ethnicity. Again.*, PROPUBLICA (July 25, 2018, 2:47 PM), https://www.propublica.org/article/facebook-promises-to-bar-advertisers-from-targeting-ads-by-race-or-ethnicity-again [https://perma.cc/2RLE-3D9F]; Ariana Tobin & Jeremy B. Merrill, *Besieged Facebook Says New Ad Limits Aren't Response to Lawsuits*, PROPUBLICA (Aug. 23, 2018, 12:48 PM), https://www.propublica.org/article/facebook-says-new-ad-limits-arent-response-to-lawsuits [https://perma.cc/2EFS-3D7F]; Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1162, 1169 (9th Cir. 2008); *see also* Tami Kim, Kate Barasz & Leslie K. John, *Why Am I Seeing This Ad? The Effect of Ad Transparency on Ad Effectiveness*, 45 J. CONSUMER RSCH. 906 (2019).

[112] Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 999, 1003–08 (2014); Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRIES LAW 157, 172–74 (2019); Przemysław Pałka, *The World of Fifty (Interoperable) Facebooks*, 51 SETON HALL L. REV. 1193, 1220 (2021).

[113] M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1131 (2011).

[114] Laurent Sacharoff, *The Relational Nature of Privacy*, 16 LEWIS & CLARK L. REV. 1249, 1278–80 (2012).

[115] *See* COFONE, *supra* note 13, at 113–14.

The importance and pervasiveness of inferential harm means that courts should find commonality in intangible harm — not in its tangible consequences. This is of particular relevance to privacy class actions, as privacy harms' tangible consequences cast their net widely and can be evident, inchoate, or downstream. Conceptualizing privacy in a binary fashion, where one's privacy was violated only if one suffered downstream harms and not violated absent such harms, makes privacy claims overwhelmingly difficult to prove. And the information asymmetry between users and third parties necessitates a continuous concept of privacy loss. Accounting for the nuance of privacy harms through a spectrum of prospective losses and gains provides a better conceptual framework to grapple with the continuous, aggregated privacy harms plaguing the information economy.

In cases where standing requires concrete harm under current Supreme Court doctrine, class certification also requires a common concrete harm, rather than just a shared opacity loss that led to disjointed harms.[116] Statutory anchors, doctrine, and precedent define the requirement of commonality through the framework of the "common question."[117] Plaintiffs meeting the threshold of certification must have questions in common that also have the potential to generate common answers. In other words, a common question must be "capable of classwide resolution — which means that determination of its truth or falsity will resolve an issue that is central to the validity of each one of the [class members'] claims in one stroke."[118] Commonality is often put into conversation with the requirement that questions common to the class must predominate over the questions affecting individual members.[119]

A shared opacity loss resulting from the same data practice is still relevant in federal courts with concrete harm requirements. In these courts, opacity loss resulting from the same data practice should be seen as establishing a presumption that the intangible harm among a class is shared. This intangible harm is frequently shared because the loss that caused it was shared. Presuming that this harm is shared, as it commonly is, avoids overly onerous probatory requirements. For example,

[116] *See* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2200 (2021).

[117] Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 359 (2011); A. Benjamin Spencer, *Class Actions, Heightened Commonality, and Declining Access to Justice*, 93 B.U. L. REV. 441, 445, 455–58 (2013); *see also* Judith Resnik, *Fairness in Numbers: A Comment on* AT&T v. Concepcion*,* Wal-Mart v. Dukes*, and* Turner v. Rogers, 125 HARV. L. REV. 78 (2011); Joseph A. Seiner, *Commonality and the Constitution: A Framework for Federal and State Court Class Actions*, 91 IND. L.J. 455 (2016); Suzette M. Malveaux, *Class Actions at the Crossroads: An Answer to Wal-Mart v. Dukes*, 5 HARV. L. & POL'Y REV. 375 (2011).

[118] Theodore J. Boutrous, Jr. & Bradley J. Hamburger, *Three Myths about* Wal-Mart Stores, Inc. v. Dukes, 82 GEO. WASH. L. REV. 47, 59 (2014) (quoting Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 350 (2011)); *see also* Resnik, *supra* note 117.

[119] *See* Mark A. Perry, *Issue Certification under Rule 23(c)(4): A Reappraisal*, 62 DEPAUL L. REV. 733, 739 (2013).

in *Brown* and *Gaos*, the two class actions against Google discussed in Section III.B, all class members suffered intangible privacy harm resulting from the unauthorized disclosure of their information, in addition to being exposed to different downstream harms.[120] In these cases, users' privacy collectively dropped from one level to another as a direct result of Google's single data practice, linking opacity and privacy harm for each of them and among them.

Traditional class actions similarly address equivalent group harms linked by a single misbehavior. In one prominent example, the U.S. National Football League was sued for failing to protect players against head injuries; in another, Volkswagen was sued for misrepresenting its diesel emissions.[121] Identifying shared intangible privacy harm through a recognition of shared opacity losses provides consistency in allowing people to sue as a class that is analogous to precedent in mass torts.

Loss and immaterial harm concepts can similarly distinguish among groups of plaintiffs. It may be difficult to see that people share an intangible privacy harm resulting from the same data practice, rather than having suffered entirely different ones, when people are harmed in different magnitudes. Because shared opacity loss can uncover unifying elements among plaintiffs, lack of shared opacity loss can also point to the absence of those unifying elements. Plaintiffs should have a presumption in favor of commonality when an opacity loss is the cause of the downstream data harms that they claim — but when downstream harms emerge from different opacity losses, the plaintiffs should have the burden to prove commonality. Identifying commonality in such a way applies to both pathways.

Collective action based on intangible privacy harm better responds to the reality of inferences. Because synergies among collected data points from different people lead to harmful inferences, separating claims in individual lawsuits leads to replicated efforts from plaintiffs, defendants, and the court system.[122] Harms produced by probabilistic opacity losses share this concern. Inferential information often produces group harms, and grouping claims that arise from group inferences is more fitting to the reality of such harms — and of the government and business practices that create them — than dividing them into individual actions.

A continuous view of opacity loss and privacy harm can and should be used for all privacy claims.[123] But it is particularly important for class actions. This idea connects with the nature of class actions, which inevitably have varying degrees of loss and harm suffered by members

[120] *See supra* Section III.B.

[121] Elizabeth J. Cabraser & Samuel Issacharoff, *The Participatory Class Action*, 92 N.Y.U. L. REV. 846, 851 nn.23–24 (2017).

[122] *See* Scott Dodson, *Subclassing*, 27 CARDOZO L. REV. 2351, 2354 (2006).

[123] Richards, *supra* note 60, at 32–33.

of a class. When data practices apply to a group, the opacity loss exists along a spectrum: some group members may face a larger loss than others by the same intervention. In a class action, the loss from a privacy violation is never binary because it can vary for each member of the class depending on the amount and type of information acquired.[124] In many class actions, for example, some members of the class had one type of information shared and others had additional or different information shared by the same data practice.[125] Further, opacity losses from information vary also because inferences vary for each member depending on how much other information is available about them. Binary conceptions of privacy are particularly unhelpful in privacy class actions because they prevent one from identifying commonality.

At the intersection of opacity loss and privacy harm is *Davis v. Facebook*.[126] Facebook's breach of the Wiretap Act and the California Invasion of Privacy Act ("CIPA"), combined with a violation of their privacy interest under tort law, was sufficient for the class to sue as such.[127] Once plaintiffs established breach of statute, the court did not require them to prove reputational, financial, or discriminatory harm to sue based on intrusion upon seclusion.[128] This is because reputational, financial, or discriminatory harm are not the interests that privacy torts protect — rather, they are other social values that may be harmed when someone's personal information is wrongfully collected, processed, or shared. The same distinction applies to statutory privacy cases which, like privacy torts, chiefly protect from privacy harm.

This is the part of this Essay's proposal most relevant to federal courts, which must address unfortunate injury-in-fact requirements as established by the Supreme Court.

D. An Example: TransUnion v. Ramirez

In 2021, TransUnion, one of three large U.S. credit bureaus, mislabeled thousands of people as possible terrorists and other national security threats in credit reports made available to employers and creditors.[129] One of the victims, Sergio Ramirez, learned about this mistaken designation when he was prevented from buying a car.[130] He sued TransUnion as part of a class action, arguing that the company did not take reasonable measures to ensure its files were accurate.[131] The

[124] *See* Cofone, *supra* note 13, at 129.

[125] *See id.* at 19, 129.

[126] Davis v. Facebook, Inc. (*In re* Facebook, Inc. Internet Tracking Litig.), 956 F.3d 589, 598–600 (9th Cir. 2020); *see supra* Section II.A.

[127] *Davis*, 956 F.3d at 598–99.

[128] *See id.*

[129] TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2201 (2021).

[130] *Id.*

[131] *Id.* at 2202.

company argued that plaintiffs whose credit reports were not shared could not have suffered concrete harm.[132] The Supreme Court sided with TransUnion.[133]

The Court's focus on tangible consequences with express commonalities among the plaintiffs precluded a finding of concrete privacy harm for the class. TransUnion breached the statute, but the court rejected the plaintiffs' claim, arguing that they lacked concrete harm, a requirement for standing in federal court.[134] The Court expressed concern that there was not enough interference with the reputational and financial interests of all members of the lawsuit to justify grouping them together.[135] The Court indicated that Ramirez and other members of the lawsuit needed a concrete harm to sue; but it failed to identify privacy harm as concrete.[136]

The Court did not provide a clear standard for determining what would be "concrete."[137] It merely provided examples and stated plaintiffs need a "'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts — such as physical harm, monetary harm, or various intangible harms including reputational harm . . . ."[138]

Data harms, such as those the Court was looking for in *TransUnion*, are downstream harms of data practices. Class members in *TransUnion* shared an inferential opacity loss, which forms an independent concrete harm conducive to commonality and certification, based on their loss of control over their information resulting from TransUnion mislabeling them as terrorists.[139] Besides creating financial and reputational losses, TransUnion also interfered with people's privacy.

As a consequence of mistakenly equating concrete with downstream, most privacy class actions fail the moment they arrive in court.[140] As a result, people who suffer privacy harms are systematically denied redress at federal courts.

TransUnion illustrates the importance of intangible harm when class certification requires evidence of a concrete harm. Solely focusing on downstream harms, even if doing so more substantially than the Court did in *TransUnion*, would not have helped address the plaintiffs'

[132] Brief for Petitioner at 37, TransUnion LLC v. Ramirez, 141 S. Ct. 2190 (2021) (No. 20-297).

[133] *TransUnion*, 141 S. Ct. at 2205–10.

[134] *See id.*

[135] *See id.* at 2200.

[136] *Id.* at 2214.

[137] *See id.* at 2203–14.

[138] *Id.* at 2200.

[139] *Id.* at 2221–24 (Thomas, J., dissenting).

[140] *See* Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 1016 (2018); SOLOVE ET AL., *supra* note 28 at 55–59.

claims.[141] Downstream harms had not yet materialized for many members of the class.[142] But in the future, they will; and, once they finally do, causality will become difficult to prove.[143] When these other harms materialize, proving their relationship with TransUnion's actions may be too burdensome for these plaintiffs. Yet before they do, courts cannot accurately anticipate which subsequent harms will happen. Therefore, making certification (and therefore redress) contingent on downstream harms manifesting early for the entirety of the class leads to those very harms being left unaddressed in the long term, too.

Privacy class actions will fail as long as courts perceive privacy interferences solely through the lens of monetary or physical losses. Addressing situations like *TransUnion* requires two things: first, recognizing the tangible harms that many victims, such as Ramirez, suffered, and second, recognizing the intangible privacy harm that all victims suffered.

The Court did recognize that "intangible harms can also be concrete."[144] It just failed to recognize the concreteness of intangible harms.[145] In a world where terrorists and ordinary citizens are treated very differently, it is a harm in itself when an entity in a position of power such as a credit rating agency wrongly labels people as terrorists.[146] Curiously, national security statutes implicitly recognize intangible privacy harm for some types of data collection, making the rejection by the Court of intangible privacy harm for the information economy somewhat ahistorical.[147] Requiring that plaintiffs prove some type of harm is workable only if all harms, including intangible ones, are recognized.

TransUnion combined both forms of probabilistic opacity loss that could be used to constitute a class absent harm requirements. Ramirez and others contended with two kinds of losses. The first was creating an incorrect inference about them (i.e., that they were terrorists).[148] The second was disclosing the inference.[149] Ramirez's opacity loss was produced by both TransUnion's concluding he was a terrorist, which negatively affected TransUnion's estimation about him, and TransUnion's

[141] Cofone, *supra* note 40, at 1411–15.

[142] *See TransUnion*, 141 S. Ct. at 2208–13; *see also* Cofone, *supra* note 40, at 1415; Summer Elliot, *There's No Understanding Standing for Privacy: An Analysis of* TransUnion v. Ramirez, 37 BERKELEY TECH. L. J. 1379 (2022).

[143] *See* Margot E. Kaminski, *Standing After Snowden: Lessons on Privacy Harm from National Security Surveillance Litigation*, 66 DEPAUL L. REV. 413, 416 (2017).

[144] *TransUnion*, 141 S. Ct. at 2204.

[145] *See generally* Citron et al., *supra* note 38, at 828–29 (2022) (exploring the expressive value of judicially recognizing inchoate or intangible privacy harms).

[146] Daniel J. Solove & Danielle Keats Citron, *Standing and Privacy Harms: A Critique of* TransUnion v. Ramirez, 101 B.U. L. REV. ONLINE 62, 69 (2021).

[147] Kaminski, *supra* note 143, at 422–30.

[148] *TransUnion*, 141 S. Ct. at 2209.

[149] *Id.*

disclosing an incorrect terrorist alert, which negatively affected others' estimations about him.[150]

The Supreme Court lacked this continuous notion of loss in *TransUnion*, getting lost in examining reputational and financial losses that varied from plaintiff to plaintiff. What caused downstream harms for some plaintiffs, in the form of reputational and financial harms, was the opacity loss that all plaintiffs shared.[151] The Court failed to see this common element, emphasizing that some, but not all, class members suffered reputational harm equivalent to defamation.[152] Further, in a context of strict actual harm requirements, intangible privacy harm provided identification over commonality needed for plaintiffs to sue as a class. Plaintiffs had in common the privacy harm that TransUnion caused them.[153] That central commonality justifies their grouping in a class action. Because it was the cause of downstream harms, one should consider such privacy harm as predominant.

Courts can and should focus on common losses and intangible harms produced by data practices that breach statutory rules or privacy policies, rather than downstream harms. That is, they can and should take the opposite direction that the Supreme Court took in *TransUnion*.

IV. Overcoming Policy Obstacles

A. Distribution: Subclasses of Plaintiffs

A question that crosses doctrine and policy in certification of privacy class actions is the distribution of the award, as courts can find that harm varied from person to person. This is a relevant issue in privacy class actions when downstream harms vary: where some groups of people faced downstream harms but some did not, or they faced different types.

One way to address distribution of a monetary award is with subclasses of plaintiffs. Within a class, there may be subclasses, which are subgroups or subcategories of plaintiffs with similar claims within the overall class.[154] Subclasses are created when there are different legal or factual issues that apply to certain members of the class, and it is efficient to manage the case by grouping these plaintiffs together for litigation purposes.[155]

Each subclass is treated as a separate group with its own representative. The court may even appoint class counsel for each subclass

[150] *Id.* at 2201.
[151] *See id.* at 2206–14.
[152] *Id.*
[153] Solove et al., *supra* note 146, at 69.
[154] *See* Fed. R. Civ. P. 23(c)(5).
[155] *See* Dodson, *supra* note 122, at 2362–63.

to represent their interests.[156] Subclasses are subject to the same requirements and procedures as the main class in a class action, including certification by the court as a subclass and notice to the class members.[157] They are nevertheless grouped as subconstructs within a single class action, rather than represented as separate class actions, for the same reasons that the Essay advances class actions as a better tool for addressing privacy harms than individual actions: to offset issues of access, efficiency, and remedies.[158]

The purpose of creating subclasses is to ensure that the rights and interests of all class members are adequately represented, and that the case is managed efficiently and fairly.[159] For example, subclasses have been proposed to address opt-in versus opt-out discussions in class actions.[160] Subclasses can also be helpful in light of *Dukes*' requirements.[161] Subclasses can be useful when there are variations in the claims or damages among the class members, or when there are different issues that apply to different groups within the class.[162] For example, in a product liability class action involving a defective product, there may be subclasses for individuals who suffered different types of injuries, who purchased the product in different states, or who used the product for different purposes.

Subclasses of plaintiffs allow for accounting of harm differences, both in terms of intangible and tangible harm, among groups of people who share an opacity loss or privacy harm. Subcategories can help ensure that the interests of different groups within the class are adequately represented, as the claims of various individuals may differ. When local procedural rules allow it, courts should create subcategories within the class when all members suffered privacy harm (or a shared loss in tort law and statutes without a harm requirement) and some also suffered downstream harm, such as financial.

The use of subclasses in class actions is subject to the rules and procedures of the specific court where the class action is filed, and the decision to create subclasses is at the discretion of the court.[163] When subclasses are not allowed by procedural rules, courts could group a

[156] Jay Tidmarsh, *Rethinking Adequacy of Representation*, 87 TEX. L. REV. 1137, 1163 (2009).

[157] Laura J. Hines, *The Unruly Class Action*, 82 GEO. WASH. L. REV. 718, 735 (2014); FED. R. CIV. P. 23.

[158] Dodson, *supra* note 122, at 2362–63.

[159] *See id.* at 2363 n.58, 2371.

[160] Scott Dodson, *An Opt-In Option for Class Actions*, 115 MICH. L. REV. 171, 205–06 (2016).

[161] *See, e.g.*, McReynolds v. Merrill Lynch, Pierce, Fenner & Smith, Inc., 672 F.3d 482, 492 (7th Cir. 2012).

[162] *See In re* Paxil Litig., 212 F.R.D. 539, 543 (C.D. Cal. 2003); *see also* Jenna G. Farleigh, Note, *Splitting the Baby: Standardizing Issue Class Certification*, 64 VAND. L. REV. 1585, 1600–1603 (2011).

[163] Dodson, *supra* note 122, at 2362–63, 2372.

class for shared opacity loss or privacy harm, and separate class actions for each downstream harm. Financial, reputational, discriminatory, psychological (including harassment), and physical harms happen as a consequence of shared opacity losses. Regardless of whether these other harms for each member of the class are discussed in the same lawsuit or different ones, they should be treated as conceptually independent from plaintiffs' shared opacity loss and privacy harm. Not recognizing the unifying privacy harm among members of a group creates obstacles for them to have a class recognized that run contrary to the purpose of class actions. But recognizing the unifying harm does not impede the acknowledgment of shared or separate downstream harms.

Absent subclasses, courts may decide to address distribution in the context of diverging inchoate downstream harms by setting up an individual claims process. In such a process, members of the class would be required to provide evidence of their situation related to downstream harms, not to be a member of the class but rather to determine the compensation for which they are eligible. In privacy matters, without creating subclasses, this could lead, for instance, to a court making determinations such as: "the defendant breached its privacy obligations; it caused opacity loss and common intangible harm to the entire class; and any person wanting to claim downstream harms in addition to that will have to go through an individual claims process set up by the court."

B. The Goldilocks Problem

Privacy class actions have a Goldilocks problem. Some are concerned that there will be too few privacy class actions because people do not have enough incentives to sue, as detailed above.[164] Others are concerned that, if privacy class actions are recognized, there will be too many because people would have too many incentives to sue.[165] There are reasonable safeguards for both concerns.

A first concern is that collective rights of action in privacy fail at the incentives level. They risk doing so on two fronts, as detailed in the data security literature for data security class actions.[166] First, they frequently fail to recognize harm required for people to sue, leaving

[164] Margaret Lemos, *Special Incentives to Sue*, 95 MINN. L. REV. 782, 795–810 (2011) (exploring the failure of aggregating claims to increase rates of claim filing and affordable access to justice, looking particularly at the effect of enhanced damages and one-way fee shifts on litigation incentives for class actions); Jason Jarvis, Note, *A New Approach to Plaintiff Incentive Fees in Class Action Lawsuits,* 115 NW. U. L. REV. 919 (2020).

[165] Lemos, *supra* note 164, at 782–84.

[166] *See generally* SOLOVE ET AL., *supra* note 28, at 55–59.

victims' claims unrecognized.[167] Second, compensation tends to be under-compensatory, making individual litigation not worth pursuing.[168]

The first hurdle class actions need to overcome is compensation. When based on downstream harms alone, class actions provide insufficient incentives to sue. Claims for mass privacy harms are worth little to each member, so the hassle and expense of litigating meritorious cases do not always exceed their expected benefit.[169] Those amounts would be sufficient for a mass harm class action, but may be insufficient to motivate a small- to medium-size group, even in cases where plaintiffs' lawyers may have other incentives to sue.[170] Compensation that includes intangible privacy harm together with compensation for downstream harms would be an improvement for plaintiffs.

A second, opposing concern is the risk of meritless nuisance lawsuits. For example, a report on federal privacy legislation argues that:

> [A p]rivate right of action substantially increases companies' legal risks. Introducing this amount of legal risk inevitably leads to unnecessary lawsuits, some initiated by plaintiffs' lawyers . . . . If companies must spend money on compliance and legal fees, they cannot invest that money in other areas, such as by lowering prices, offering discounts, or creating new products and services.[171]

Some commentators worry that plaintiffs can become "increasingly creative in finding a statute that gives them a cause of action based on a violation of the statute's provisions alone, even absen[t] actual harm."[172] Others are similarly concerned with companies having to pay excessive amounts if they are fined and sued. Some courts, for example, have expressed concern with over-litigation if privacy class actions are recognized, leading to companies paying excessive damages.[173]

While it is unlikely people would individually incur the cost of suing when litigation costs outweigh benefits, class actions introduce an incentives concern. Lawyers may be incentivized to induce

[167] SOLOVE ET AL., *supra* note 140, at 55–56.

[168] *Id.* at 59.

[169] Kadri, *supra* note 20.

[170] *See supra* Section II.A.

[171] ALAN MCQUINN & DANIEL CASTRO, A GRAND BARGAIN ON DATA PRIVACY LEGISLATION FOR AMERICA 61 (2019), https://www2.itif.org/2019-grand-bargain-privacy.pdf [https://perma.cc/6YUS-AJ3Z].

[172] Karin M. McGinnis, Beck v. McDonald — *4th Circuit Weighs in on Standing in Data Breach Case*, MOORE & VAN ALLEN DATA POINTS: PRIV. & DATA SEC. BLOG (Feb. 8, 2017), https://www.mvalaw.com/data-points/beck-v-mcdonald-4th-circuit-weighs-in-on-standing-in-data-breach-case [https://perma.cc/N6MA-YRRA].

[173] *See* Citron et al., *supra* note 10, at 783–86.

unenthusiastic plaintiffs to motivate suits over trivial statutory violations.[174] Plaintiff's counsel may apply pressure in areas where recouping costs is more viable. Similarly, plaintiff's counsel may pursue claims that, even under a class action, have lower expected gain than cost and then strategically pursue settlement to avoid incurring trial costs.[175] Setting aside the conflict of interests between attorneys and their clients that these incentives raise, they could promote meritless lawsuits.[176] The concern is that, by making suing easier, lawyers operating under a contingency fee model could find otherwise unmotivated plaintiffs willing to sue to vindicate a trivial statutory violation. If that were the case, privacy class actions could fabricate a problem of frivolous lawsuits.

Ironically, however, overly broad privacy claims often come from the corporate and government sides, which are unaffected by class certification.[177] Companies and governments use privacy compliance to prevent algorithmic transparency and as a pretext to avoid sharing information in trials.[178] Recognizing and remedying shared privacy harms in class actions does not open floodgates to frivolous claims like these. Instead, it promotes compensating victims for harm.

The risk of meritless lawsuits exists in many areas of law. Courts manage these risks by avoiding overexpansive bases to sue.[179] A statutory private right of action with clear limits on its scope can similarly narrow the range of lawsuits.[180] Concerns can be mitigated by procedural measures, such as requiring plaintiffs to pay businesses' legal fees for frivolous claims, as adopted by the California Consumer Privacy Act.[181] Alternatively, statutes can set a maximum for intangible damages low enough to avoid strategic individuals having incentives to sue, as adopted by the FCRA and FACTA.[182] These maximums work as long as they do not impede compensation for downstream harm if

[174] Jeffrey Hammond & James E. West, *Class Action Extraction?*, 116 PUB. CHOICE 91, 97 (2003).

[175] *See generally* Lewis A. Kornhauser, *Control of Conflicts of Interest in Class-Action Suits*, 41 PUB. CHOICE 145, 161–64 (1983) (examining the role of the attorney in encouraging or deterring settlements).

[176] *See, e.g.*, Unger, *supra* note 25, at 8, 22–27.

[177] *See* Neil M. Richards, *The GDPR as Privacy Pretext and the Problem of Co-Opting Privacy*, 73 HASTINGS L.J. 1511, 1523–37 (2022).

[178] *E.g.*, Ignacio N. Cofone & Katherine J. Strandburg, *Strategic Games and Algorithmic Secrecy*, 64 MCGILL L.J. 623, 632–34 (2019); Rebecca Wexler, *Privacy Asymmetries: Access to Data in Criminal Defense Investigations*, 68 UCLA L. REV. 212, 229–59 (2021); María P. Angel & Ryan Calo, *Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy*, 123 COLUM. L. REV. (forthcoming 2024).

[179] COFONE, *supra* note 13, at 134.

[180] Cameron F. Kerry, John B. Morris, Caitlin Chin-Rothmann & Nicol Turner Lee, *Bridging the Gaps: A Path Forward to Federal Privacy Legislation*, BROOKINGS INST. RSCH. & COMMENT. (June 3, 2020), https://www.brookings.edu/research/bridging-the-gaps-a-path-forward-to-federal-privacy-legislation [https://perma.cc/B387-EHJR].

[181] *See* CAL. CIV. PROC. CODE § 128.5 (West 2017).

[182] *See* 15 U.S.C. § 1681n(a)(1)(A).

proven and bind plaintiffs in a larger class than they would otherwise have. They would work better if paired with compensation for plaintiffs' legal fees for meritorious claims to keep incentives for those cases. Nominal amounts, a well-recognized approach in tort law, may be meaningful for deterrence if aggregated in a class action. Basing certification on shared opacity loss and privacy harm may further allow courts to curtail frivolous claims while simultaneously working to expand judicial notions of privacy.

Appropriate class certification may moderate concerns of under-litigation and over-litigation further — even if they are not eliminated, as they are also not in other areas where class actions are recognized. For under-litigation, more comprehensive and consistent class identification provides better incentives to sue. For over-litigation, the wrongness of a data practice captured in tort or statutory violation, curtailed by shared loss or immaterial harm, mitigates the problem.

V. CONCLUSION

The new, ever-increasing threats to privacy that the information economy presents necessitate novel mechanisms and remedies for adequately addressing privacy harms. Class action suits may prove to be particularly effective in the privacy sphere, compared to other areas of the law, because of the inchoate, continuous, and aggregated nature of these harms. By recognizing the limits of private rights of action and remaining equally cognizant of the procedural shortcomings of class actions, we can work towards a new framework for unifying classes of plaintiffs that engages relevant questions of policy and doctrine.