DePaul Law Review

Volume 66
Issue 2 *Winter 2017: Twenty-Second Annual Clifford Symposium on Tort Law and Social Policy*

Article 9

Information Privacy Litigation as Bellwether for Institutional Change

Julie E. Cohen

INFORMATION PRIVACY LITIGATION AS BELLWETHER FOR INSTITUTIONAL CHANGE

*Julie E. Cohen**

ABSTRACT

Information privacy litigation is controversial and headline-grabbing. New class complaints are filed seemingly every few weeks. Legal scholars vie with one another to articulate more comprehensive theories of harm that such lawsuits might vindicate. Large information businesses and defense counsel bemoan the threats that information privacy litigation poses to corporate bottom lines and to "innovation" more generally. For all that, though, the track record of litigation achievements on the information privacy front is stunningly poor. This Article examines emerging conventions for disposing of information privacy claims, including denial of standing, enforcement of boilerplate waivers, denial of class certification, disposal via opaque multidistrict litigation proceedings, and cy pres *settlements. It argues that, in an era of complex, informationally-mediated harms, the information privacy lawsuit is a marker of both institutional stress and institutional opportunity. The inability of most information privacy claims to gain meaningful traction reflects the influence of powerful repeat players interested in minimizing their exposure to claims of informational injury. But it also raises important questions about how judicial processes can be adapted to deal with the predominantly informational and infrastructural harms that increasingly characterize our networked, information-based political economy.*

I. INTRODUCTION

Information privacy litigation is controversial and headline-grabbing. New class complaints are filed seemingly every few weeks. Typically, such complaints assert claims under sector-specific statutes and also assert generalized tort, contract, and unfair competition claims aimed at filling the gaps between those statutes. Legal scholars vie

* Mark Claster Mamolen Professor of Law and Technology, Georgetown Law. Thanks to Danielle Citron, Heidi Li Feldman, Maria Glover, Chris Hoofnagle, Paul Ohm, Joel Reidenberg, Marc Rotenberg, Andrew Selbst, David Vladeck, Robin West, and participants in the *22nd Annual Clifford Symposium on Tort Law and Social Policy* for their comments, and to Kelley Chittenden, Ben Hain, Patrick Reid, Apeksha Vora, and Alex Zajac for research assistance.

with one another to articulate more comprehensive theories of harm that such lawsuits might vindicate.[1] Large information businesses and defense counsel bemoan the threats that information privacy litigation poses to corporate bottom lines and to "innovation" more generally.[2] For all that, though, the track record of litigation achievements on the information privacy front is stunningly poor. Some claims are dismissed for lack of cognizable injury and others on grounds of waiver, while still others fail at the hurdle of class certification. The few lawsuits that survive threshold challenges disappear into a complex procedural labyrinth, often under the aegis of the Judicial Panel on Multidistrict Litigation. Occasionally a settlement emerges, but such settlements rarely seem to translate into meaningful substantive changes in practices of mass data harvesting and processing that have become the commercial norm in the United States. What (if anything) does it all mean?

This Article situates the strange tale of information privacy litigation within broader shifts in the landscape of remedial litigation over the past several decades. Among legal scholars, there is broad consensus that the judicial system has reached, and perhaps already passed, an inflection point. Liberalized institutional features dating from an earlier, more reformist era—including the pleading standards inaugurated by the Federal Rules of Civil Procedure, federal class ac-

1. *See generally, e.g.*, M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011); Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1805 (2010); Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241 (2007); Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125 (2015); Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877 (2003); Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. (forthcoming 2017).

2. *See, e.g.*, Brief of the Coal. for Sensible Pub. Records Access et al. as Amici Curiae in Support of Petitioner at 1–2, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) (No. 13-1339) ("As a result, amici's members—some of whom supply lending, insurance or transactional information, or facilitate residential real estate purchases—face increased costs of doing business and are significantly less willing to bear risk and to innovate, to the ultimate detriment of all consumers and the economy."); Brief for Amici Curiae Ebay, Inc. et al. in Support of Petitioner at 23–24, *Spokeo*, 136 S. Ct. at 1540 (No. 13-1339) ("Perversely, the primary consequences of the expensive litigation and resulting *in terrorem* settlements of these no-injury controversies are the diversion of resources away from technology companies' efforts to develop and provide increasingly innovative services and products to the users who often comprise the putative classes in these cases."); Brief of Trans Union LLC as Amicus Curiae in Support of Petitioner at 2, *Spokeo*, 136 S. Ct. at 1540 (No. 13-1339) ("If this Court does not grant the petition for certiorari and correct the Ninth Circuit's error, then the immediate result will be more 'bet the company' litigation filed under the [Fair Credit Reporting] Act," inevitably reducing innovation in new data services and diminishing "the scope of predictive information available to credit grantors to manage risk."); *see also* LARRY DOWNES, CATO INST., A RATIONAL RESPONSE TO THE PRIVACY "CRISIS" 1–2, 16 (2013), https://www.cato.org/publications/policy-analysis/rational-response-privacy-crisis.

tion procedures, standards of tort liability capable of reaching the manufacture of complex consumer products, and statutory regimes intended to help courts reach and remedy a variety of other, information-based harms—are being systematically ratcheted back.[3] Meanwhile, due in part to the volume of case filings and in part to the increasing complexity of some types of litigation, the court system now seems to function principally to funnel disputes toward settlement.[4] Those stories are by now familiar ones. This Article argues that emerging conventions for disposing of information privacy claims are poised both to become capstone achievements of the ongoing process of litigation retrenchment and to supply advocates of retrenchment with powerful new narratives for justifying judicial avoidance of information-economy mass justice claims. Yet information privacy litigation also might become a catalyst for transformative institutional change.

The tale unfolds in three acts. Part II considers the contention that privacy harms are inherently nonjusticiable and concludes that, at least as a conceptual matter, objections to justiciability are overblown. When the claims now being raised about harm and injury in modern privacy litigation are viewed in light of the arcs of product liability and intellectual property law over the last century or so, they are not as remarkable as opponents have worked to make them seem. What has changed is the political will to hold private enterprise accountable for its role in configuring the built and mass-marketed environment to generate particular types of collateral damage. As the judicial system has encountered the demands of evolving political economy, it sometimes has found ways to accommodate the issues of concreteness, imminence, and causation that new types of claims about injury have

3. On pleading standards, see Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009); Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007). On class actions, see, for example, Comcast Corp. v. Behrend, 133 S. Ct. 1426, 1433 (2013) (rejecting certification of a Rule 23(b)(3) class action because plaintiffs failed to provide a sufficiently precise mechanism to calculate damages), and Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 350 (2011) ("Rule 23 does not set forth a mere pleading standard. A party seeking class certification must affirmatively demonstrate his compliance with the Rule—that is, he must be prepared to prove that there are *in fact* sufficiently numerous parties, common questions of law or fact, etc."). On standards for tort liability, see, for example, Brown v. Superior Court, 751 P.2d 470, 476 (Cal. 1988) (excepting prescription drugs from strict products liability); Deborah R. Hensler, *Has the Fat Lady Sung? The Future of Mass Toxic Torts*, 26 REV. LITIG. 883, 892 (2007). On statutory regimes, see, for example, FAA v. Cooper, 566 U.S. 284, 299 (2012) (holding that actual damages under the Privacy Act of 1974 are "limited to proven pecuniary or economic harm" and thus rejecting claim for statutory damages where plaintiff proved only emotional damages); and Fein v. Permanente Med. Grp., 695 P.2d 665, 683 (Cal. 1985) (upholding statutory limit on noneconomic damages in medical malpractice suits).

4. *See, e.g.*, J. Maria Glover, *The Federal Rules of Civil Settlement*, 87 N.Y.U. L. REV. 1713, 1721–25 (2012); Judith Resnik, *Managerial Judges*, 96 HARV. L. REV. 374, 421–22 (1982).

been thought to raise, and it might begin to do so again in the information privacy context.

Part III explores the ways that procedural barriers to remedial litigation, including waiver, class certification thresholds, and the filing-to-settlement pipeline, have unfolded in the information privacy context. It argues that, in part because of widespread acquiescence in the framing of information privacy interests predominantly as contractually-mediated, inherently individualized processes of self-management, information privacy lawsuits present the perfect confluence of opportunities for litigants and courts seeking to accelerate institutional resistance to information-economy mass justice claims.

Finally, Part IV turns to the broader, interlinked questions of redressability and institutional competence, considering whether other legal institutions—for example, administrative agencies—simply are better equipped to grapple with the systemic questions that surround mass data harvesting and processing. The argument from institutional competence has the comforting ring of tradition, but ignores the fact that our legal institutions, including both courts and administrative agencies, are already changing as they struggle to respond to the conceptual and logistical problems posed by information-economy disputes. Some questions undoubtedly will prove to be more appropriately directed to other branches of government, but the courts also have an important role to play in determining the shape of legal institutions and the conditions of access to justice in the networked information society. For that to happen, though, they must reconsider some of the procedural barriers they have put in place to deflect responsibility for resolving aggregate claims in general and information privacy claims in particular.

The moral of the story is that information privacy litigation should be controversial, but for somewhat different reasons than most people appear to think. In an era of complex, informationally mediated harms, the information privacy lawsuit is a marker of both institutional stress and institutional opportunity. The inability of most information privacy claims to gain meaningful traction reflects the influence of powerful repeat players interested in minimizing their exposure to claims of informational injury. But it also raises important questions about how judicial processes can be adapted to deal with the predominantly informational and infrastructural harms that increasingly characterize our networked, information-based political economy.

II. Conceptualizing Privacy Injuries and Harms

An initial set of obstacles to information privacy litigation concerns justiciability. To establish standing to litigate in federal court, a plaintiff must establish injury in fact, which requires a showing of harm that is concrete and particularized, actual or imminent rather than conjectural or hypothetical, and fairly traceable to the defendant's activity.[5] The harm also must be likely to be redressed by a favorable decision, an issue that I consider more closely in Part IV.[6] Although state courts don't impose identical injury-in-fact requirements, would-be privacy plaintiffs still must allege cognizable injury. In either court system, litigants who succeed in establishing standing must then substantiate allegations of injury by showing harm if they want to recover.

As Seth Kreimer explains, the injury-in-fact doctrine is a mid-twentieth-century invention, created by the Court in response to cases in which the claimed injuries were predominantly informational and seemed too general and intangible to count as redressable wrongs.[7] Put differently, the injury-in-fact doctrine is a generally reactionary (i.e., noninterventionist) institutional response to the advent of the information economy. Faced with a variety of situations involving complex, informationally mediated activities and correspondingly complex harms, courts have erected jurisdictional bulwarks against certain kinds of claims. Information privacy litigation offers an especially stark example of this process of institutional retrenchment in action. Yet the noninterventionist stance toward information-economy problems is also nonuniform: Courts have been considerably more receptive to claims involving intellectual property and computer trespass-based harms. Both stances reflect carefully constructed narratives about the appropriate institutional role for courts at a moment of economic transformation.

A. Concreteness and the Problem of Intangibility

The first set of standing-related objections to information privacy claims concerns their asserted lack of concreteness and particularization. The information industries and their advocates argue that the ordinary acts of information collection and use that have become routine background conditions in the information environment create no cognizable injury, both because tiny bits of personal information have

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

6. *Id*. at 561 (quoting Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 38 (1976)).

7. Seth F. Kreimer, *Spooky Action at a Distance: Intangible Injury in Fact in the Information Age*, 18 U. Pa. J. Const. L. 745, 747–50 (2016).

no inherent value and because the asserted consequences of personal data processing and profiling are too vague and speculative.[8] This is so, they argue, even when Congress has reached a different conclusion and has defined certain acts by data processors as working legally distinct injuries. Information privacy claims, they conclude, are really no more than generalized claims about the perceived unfairness of economic and technological processes that people have not yet learned to accept.

Whether that assessment is right, of course, depends importantly on baselines. As Danielle Citron has noted, privacy claims seem especially vague by comparison to more traditional tort claims for bodily injury.[9] It's not clear, though, that bodily injury cases should be the touchstone when so many other kinds of tort claims are cognizable.[10] Kreimer points out numerous other contexts in which intangibility is no particular bar to standing, and Ryan Calo concludes that privacy naysayers who ignore those and similar exceptions are indulging in a specious privacy exceptionalism.[11]

I agree with all of those arguments but want to make a point that is slightly different: Over the years we have come to think of the theories of recovery commonly employed in more traditional tort contexts as concrete and precise, and in the process we have learned to overlook the fact that they are neither. Both bodily injury and the seemingly more nebulous categories of "pain and suffering" and "mental anguish" serve as proxies for other types of harms that are inherently

8. *See, e.g.*, Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1356 (Ill. App. Ct. 1995) ("[A] single, random cardholder's name has little or no intrinsic value to defendants (or a merchant). Rather, an individual name has value only when it is associated with one of defendants' lists. Defendants create value by categorizing and aggregating these names."); Shibley v. Time Inc., 341 N.E.2d 337, 339 (Ohio Ct. App. 1975); Brief for Experian Info. Sols., Inc. as Amicus Curiae Supporting Petitioners at 1–2, First Am. Fin. Corp. v. Edwards, 132 S. Ct. 2536 (2012) (No. 10-708) ("Such suits are possible because the [Fair Credit Reporting] Act permits plaintiffs to sue for . . . what may be a wholly technical violation. Indeed, it is not uncommon in these cases for significant numbers of class members to have actually *benefited* from the alleged violations."); Brief of Trans Union LLC, *supra* note 2, at 19 ("It is rare for a single item, inaccurate in a small detail, to actually result in a denial of credit."); James C. Cooper, *Opinion: Why the Supreme Court Should Side with Data Brokers*, CHRISTIAN SCI. MONITOR (Nov. 2, 2015), http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/1102/Opinion-Why-the-Supreme-Court-should-side-with-data-brokers; Kashmir Hill, *Supreme Court Disappoints Facebook, LinkedIn, Zynga and Yahoo*, FORBES (Jun. 28, 2012, 11:36 AM), http://www.forbes.com/sites/kashmirhill/2012/06/28/supreme-court-disappoints-facebook-linkedin-zynga-and-yahoo/.

9. Citron, *Reservoirs of Danger*, *supra* note 1, at 289–96.

10. *See, e.g.*, Restatement (Third) of Torts: Liability for Physical and Emotional Injury §§ 46–47 (2010) (defining causes of action for intentional or reckless infliction of emotional harm and negligent conduct directly inflicting emotional harm).

11. Ryan Calo, *Privacy Harm Exceptionalism*, 12 U. COLO. J. TELECOMM'N & TECH. L. 361 (2014); Kreimer, *supra* note 7, at 754–57.

anticipatory: lost wages, loss of consortium, lost future happiness, and so on. Focusing on impairment and suffering in the here and now functions conceptually as a way of black-boxing the complex processes by which an unknowable future is translated into a calculable present.[12] At the same time, courts have rejected numerous attempts to formalize injury valuation more precisely—for example, by following the British model that draws on actuarial computation—on the ground that those more definite methods would unacceptably truncate a process that is, and should be, more holistic.[13]

One certainly could do at least as well (if not better) at valuing and compensating privacy injury. For example, data mining offers employers tools designed to predict which prospective employees will be difficult to retain for personal reasons and which current employees may be looking for work elsewhere. Armed with that information, employers can decline to hire candidates characterized as high turnover risks and can use the pool of money available for raises to retain those employees most at risk of leaving.[14] In a suit for employment discrimination, breach of contract, or violation of other applicable labor and employment laws, a court could instruct the jury to consider what an individual's services would be worth if the factors suggesting turnover risk had not been considered or if raises were distributed solely based on performance. In other contexts, profiling and data mining enable merchants and lenders to target particular consumer populations and tailor pricing for goods and services to different kinds of attributes.[15] In a suit for violation of the consumer protection or

12. On the sociological processes by which forms of economic knowledge are constructed, see generally Karin Knorr Cetina & Alex Preda, *The Epistemization of Economic Transactions*, 49 CURRENT SOC. 27 (2001); Peter Miller, *Governing by Numbers: Why Calculative Practices Matter*, 68 SOC. RES. 379 (2001).

13. *See, e.g.*, Randall R. Bovbjerg et al., *Valuing Life and Limb in Tort: Scheduling "Pain and Suffering,"* 83 Nw. U. L. REV. 908 (1989); Philip L. Merkel, *Pain and Suffering Damages at Mid-Twentieth Century: A Retrospective View of the Problem and the Legal Academy's First Responses*, 34 CAP. U. L. REV. 545 (2006); *see also* Heidi Li Feldman, *Loss*, 35 N.M. L. REV. 375 (2005) (arguing that a holistic approach best reflects both tort traditions and classical understandings of human welfare).

14. *See* Pauline T. Kim, *Data-Driven Discrimination at Work*, 58 WM. & MARY L. REV. (forthcoming 2017).

15. *See*, *e.g.*, *Flexible Figures*, ECONOMIST (Jan. 30, 2016), http://www.economist.com/news/business/21689541-growing-number-companies-are-using-dynamic-pricing-flexible-figures; Olga Kharif, *Supermarkets Offer Personalized Pricing*, BLOOMBERG (Nov. 15, 2013, 3:37 PM), https://www.bloomberg.com/news/articles/2013-11-14/2014-outlook-supermarkets-offer-personalized-pricing; Dana Mattioli, *On Orbitz, Mac Users Steered to Pricier Hotels*, WALL ST. J. (Aug. 23, 2012, 6:07 PM), https://www.wsj.com/articles/SB10001424052702304458604577488822667325882; Greg Petro, *Dynamic Pricing: Which Customers Are Worth the Most? Amazon, Delta Airlines and Staples Weigh In*, FORBES (Apr. 17, 2015, 1:17 PM), https://www.forbes.com/sites/gregpetro/2015/04/17/dynamic-pricing-which-customers-are-worth-the-most-amazon-delta-airlines-and-

fairness-in-lending laws, the jury could consider evidence about the services offered and the prices charged to other, differently situated groups.

Before dismissing these suggestions as far-fetched, consider that courts attempting to quantify damages in copyright and patent infringement cases engage in very similar reasoning. They assign damages based on hypothesized reasonable licensing fees for imagined transactions.[16] They posit menus of licensing rates for nascent or nonexistent markets.[17] They determine the profits attributable to infringing activity by means of arithmetically convenient fictions—for example, awarding one-seventeenth of the profits earned by an entire album as damages for sampling a few bars of the plaintiff's song on one of the album's seventeen tracks.[18]

Some types of asserted intellectual property harm are impossible to quantify with any accuracy, but the copyright system has an answer for that, too. It provides statutory damages as an alternative measure for the rightholder to elect. For ordinary (i.e., nonwillful) infringement, a court may in its discretion award up to $30,000 for "all infringements involved in the action, with respect to any one work"; for willful infringement, the upper bound increases to $150,000.[19] Courts have exercised their discretion broadly, awarding damages that often seem to be based on little more than their intuitive sense of the rightness or wrongness of the challenged conduct.[20] And the courts of appeal have

---

staples-weigh-in/#208e69675f04; Jennifer Valentino-Devries et al., *Websites Vary Prices, Deals Based on Users' Information*, WALL ST. J. (Dec. 24, 2012), https://www.wsj.com/article_email/SB10001424127887323777204578189391813881534-lMyQjAxMTAyMDIwMzEyNDMyWj.html.

16. *See, e.g.*, Oracle Corp. v. SAP AG, 765 F.3d 1081, 1087–93 (9th Cir. 2014); Jarvis v. K2, Inc. 486 F.3d 526, 534–35 (9th Cir. 2007); ON Davis v. Gap, Inc., 246 F.3d 152, 159 (2d Cir. 2001); Jonathan S. Masur, *The Use and Misuse of Patent Licenses*, 110 Nw. U. L. REV. 115, 127–38 (2015).

17. *See* Bridgeport Music, Inc. v. Dimension Films, 410 F.3d 792, 804 (6th Cir. 2005); Princeton Univ. Press v. Mich. Document Servs., Inc., 99 F.3d 1381, 1386–88 (6th Cir. 1996); Am. Geophysical Union v. Texaco Inc., 60 F.3d 913, 929–31 (2d Cir. 1995).

18. *See* Bridgeport Music, Inc. v. Justin Combs Publ'g, 507 F.3d 470, 483 (6th Cir. 2007); Andreas v. Volkswagen of Am., Inc., 336 F.3d 789, 795 (8th Cir. 2003) (awarding plaintiff 10% of profits from sale of Audi TT coupe during the time period that infringing commercial aired); Three Boys Music Corp. v. Bolton, 212 F.3d 477, 487 (9th Cir. 2000) (affirming jury finding that 28% of album's profits derived from infringing song and 66% of the profits attributable to that song derived from the infringement); Cream Records, Inc. v. Jos. Schlitz Brewing Co., 754 F.2d 826, 828–29 (9th Cir. 1985) (upholding award of 0.1% of defendants profits from sale of malt liquor during time period that infringing commercial aired based on trial judge's conclusion that infringement was "minimal").

19. *See* 17 U.S.C. § 504(c)(1)–(2) (2012).

20. *See* Pamela Samuelson & Tara Wheatland, *Statutory Damages in Copyright Law: A Remedy in Need of Reform*, 51 WM. & MARY L. REV. 439, 442–43, 453–63 (2009) (reviewing the case law and the incentives that the statutory structure creates for strategic lawyering to maximize awards).

uniformly rejected the argument that some such awards are so excessive that they violate due process, reasoning that even very large awards simply serve the deterrence function that Congress intended.[21]

By contrast, where information privacy statutes provide for statutory damages, courts have been notably less generous. A pair of Supreme Court decisions interprets the statutory damages provisions of the federal Privacy Act as authorizing awards only to plaintiffs who can prove actual pecuniary or economic harm.[22] More recently, in a lawsuit against data aggregator Spokeo for statutory damages under the Fair Credit Reporting Act (FCRA), the Court vacated and remanded an appellate judgment recognizing standing to sue, ruling that although some privacy injuries may be sufficiently particularized to meet the constitutional threshold for standing, especially when they involve violation of statutorily-defined individual rights, such injuries also must be sufficiently "concrete."[23] The Court acknowledged that an injury need not be "tangible" to meet that standard but declined to state what would suffice. It opined, however, that "not all inaccuracies cause harm or present any material risk of harm."[24]

Again, one certainly could derive an account of concrete information privacy injury that meets the lenient standard set in copyright cases awarding statutory damages to plaintiffs who cannot prove actual damages. Just as the copyright plaintiff whose works are included in a karaoke DVD has lost a licensing opportunity (though the defendant might never have taken the license and it's impossible to say with any certainty how much it would have paid),[25] so the FCRA plaintiff whose profile contained errors has lost appropriate employment opportunities (though he may never have been offered the job and it's impossible to say with any certainty what he would have earned). For Spokeo and similar businesses in the data harvesting economy, though, the remand presents an opportunity to argue that the Court had something different and more definite in mind.

---

21. *See* Capitol Records, Inc. v. Thomas-Rasset, 692 F.3d 899, 907–08 (8th Cir. 2012), *cert. denied*, 133 S. Ct. 1584 (2013); Sony BMG Music Entm't v. Tenenbaum, 660 F.3d 487, 509 (1st Cir. 2011).

22. *See* FAA v. Cooper, 566 U.S. 284, 299 (2012) (rejecting claim for statutory damages under the Privacy Act of 1974 where plaintiff whose HIV status was improperly disclosed by one agency to another proved only emotional damages); Doe v. Chao, 540 U.S. 614, 618 (2004) (rejecting claim for statutory damages under the Privacy Act of 1974 where plaintiff whose social security number was used to caption case documents sent to other benefit claimants did not prove any actual damages).

23. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016).

24. *Id*. at 1550.

25. *See* Zomba Enters., Inc. v. Panorama Records, Inc., 491 F.3d 574, 583–84 (6th Cir. 2007).

As these examples illustrate, both concreteness and particularity are socially constructed attributes. Judgments about the sufficiency of a claim reflect conclusions about both the locus of experienced harm (to a person or to an owner of intangible intellectual property) and about the extent of desirable accountability. Some types of asserted harms to copyright interests are extraordinarily abstract, yet the legal system assigns them concrete and particular value. We can tell both that data processing generates consequences of some sort—if it didn't, nobody would spend the resources to engage in it—and that the market considers collected reservoirs of personal data to be valuable. Why, then, must the process of getting from here to there be placed beyond the judicial system's reach?

B. Imminence and the Problem of Risk

A second set of standing-related objections to information privacy claims concerns whether such claims state a plausible connection to some actual or reasonably imminent harm. Defendants in information privacy cases typically argue that plaintiffs who object to the collection, processing, and sale of their personal information have alleged no more than generalized, inchoate fears about possible future events, and courts have found those arguments persuasive.[26] Such fears, they assert, are insufficient to satisfy the jurisdictional requirement of a "case or controversy" because they relate at most to risk, and risk is not injury.

To evaluate that argument, it is important to begin by acknowledging the extent to which the injury-in-fact doctrine is itself oriented toward the future. Although injury-in-fact is framed as a bar to litigating prospective grievances more appropriately addressed through the political process, the "imminence" formulation implicitly recognizes that there may be categories of harms that are felt before they have finished arriving.[27] In so doing, it opens the door to ad-

26. *See, e.g.*, Cahen v. Toyota Motor Corp., 147 F. Supp. 3d 955, 969 (N.D. Cal. 2015) (accepting defendants' argument that risk of future injury resulting from hacking of insecure automotive software by third parties was too speculative to confer standing); Yunker v. Pandora Media, Inc., No. 11-CV-03113-JSW, 2013 WL 1282980, at *5 (N.D. Cal. Mar. 26, 2013) (ruling that possibility of future identity theft based on access to information collected and sold to third parties was insufficient to create standing); Hernandez v. Path, Inc., No. 12-CV-01515 YGR, 2012 WL 5194120, at *2 (N.D. Cal. Oct. 19, 2012) ("The hypothetical threat of future harm due to a security risk to Plaintiff's personal information is insufficient to confer Article III standing.").

27. *See, e.g.*, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150 n.5 (2013) ("Our cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a 'substantial risk'

dressing at least some claims about nascent harm and at the same time designates such claims as a focal point for judicial anxiety.

The heightened sensitivity to nascent harm that the imminence prong of the injury-in-fact doctrine both expresses and attempts to police is in turn the product of a more general conceptual shift toward risk monitoring and risk management that has occurred over the course of the modern era. In the eighteenth and nineteenth centuries, developments in statistical and actuarial modeling began to give governments and businesses new tools for measuring, defining, and profiting from populations.[28] Those developments both expressed a newly abstract, probabilistic sensibility toward concepts like harm and loss and promised to offer ways of making such concepts more concrete and tractable. As constructs based on probability and risk crystallized, they also began to reshape the law, infusing the operation of both old and new legal institutions. Within administrative processes, regulatory methodologies based on formal risk modeling emerged during the late twentieth century as a response to the advent of new analytical techniques that revealed potential chemical harms from industrial activity to be lurking nearly everywhere.[29] In the courts, risk sensibility gave rise to new categories of damages. We have already seen one small example of this, in the idea of damages for "pain and suffering," discussed in Part II.A, above.

As Kim Lane Scheppele observed nearly two decades ago, however, the promise of probabilistic reasoning about harm and liability has never been fully realized within the judicial system.[30] The problem of heightened risk remains one of the flashpoints. Efforts to infuse risk sensibility into tort law in particular have been hotly contested. As awareness of nascent, systemic harms became more widespread, litigants began to assert new theories of injury predicated on heightened risk of future disease and/or earlier death. In a number of states, courts have now ruled that exposure to a toxic chemical with a known and sufficiently predictable risk profile can create liability for the costs

---

that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm.").

28. *See generally, e.g.*, ULRICH BECK, RISK SOCIETY: TOWARDS A NEW MODERNITY (Mark Ritter trans., 1992); IAN HACKING, THE TAMING OF CHANCE (1990); RISK AND MORALITY (Richard V. Ericson & Aaron Doyle eds., 2003); Francois Ewald, *Insurance and Risk*, *in* THE FOUCAULT EFFECT: STUDIES IN GOVERNMENTALITY 197 (Graham Burtchaell et al. eds., 1991).

29. *See* William Boyd, *Genealogies of Risk: Searching for Safety*, *1930s-1970s*, 39 ECOL. L.Q. 895, 942–45 (2012).

30. Kim Lane Scheppele, *Law Without Accidents*, *in* SOCIAL THEORY FOR A CHANGING SOCIETY 267 (Pierre Bourdieu & James S. Coleman eds., 1991) (mapping the disconnect between tort and sociological conceptions of knowledge, foreseeability, and accident avoidance).

of ongoing medical monitoring.[31] Other courts, however, have declined to follow suit, and the defense bar has assailed the development of risk-based liability for toxic tort exposure as unprincipled and potentially ruinous.[32]

At the same time, though, following the pattern described in Part II.A, courts have been more receptive to risk-based reasoning about injury to digital property interests. In cases about unauthorized access litigated under the federal Computer Fraud and Abuse Act, courts have relied on the statutory definition of "loss" as including "any reasonable cost to any victim, including the cost of responding to an offense [or] conducting a damage assessment" to allow recovery for the cost of evaluating and mitigating the risks created by system intrusions.[33] The test for injunctive relief in intellectual property cases is predicated in part on the threat of continuing harm that cannot be remedied adequately by a monetary award.[34]

The Seventh Circuit's opinion in *Remijas v. Neiman Marcus* marks the first federal appellate endorsement of risk-based reasoning about standing in the information privacy context.[35] The plaintiffs in *Remijas* alleged a variety of injuries resulting from a data breach, including lost time and money resolving fraudulent charges and instituting protective measures against identity theft and also including heightened risk of future fraudulent charges and identity theft. Reasoning that "the Neiman Marcus customers should not have to wait

31. *See, e.g.*, *In re* Paoli R.R. Yard PCB Litig., 916 F.2d 829, 835–36 (3d Cir. 1990) (permitting recovery of medical monitoring costs upon proof of negligent exposure, proximate cause of increased risk, and reasonable necessity); Potter v. Firestone Tire & Rubber Co., 863 P.2d 795, 800–81 (Cal. 1993); Donovan v. Philip Morris USA, Inc., 914 N.E.2d 891, 894–95 (Mass. 2009); Bower v. Westinghouse Elec. Corp., 522 S.E.2d 424, 426 (W. Va. 1999).

32. *See, e.g.*, Metro N. Commuter R.R. Co. v. Buckley, 521 U.S. 424, 425–26, 440–44 (1997) (noting that "the cases authorizing recovery for medical monitoring for asymptomatic plaintiffs in the absence of physical injury do not endorse such a full-blown, traditional tort law cause of action" for lump-sum damages and rejecting argument for such a rule under the Federal Employers' Liability Act); Henry v. Dow Chem. Co., 701 N.W.2d 684, 689 (Mich. 2005) (holding that "Michigan law requires an actual injury to person or property as a precondition to recovery under a negligence theory"); George W.C. McCarter, *Medical Sue-Veillance: A History and Critique of the Medical Monitoring Remedy in Toxic Tort Litigation*, 45 RUTGERS L. REV. 227 (1993); Victor E. Schwartz & Cary Silverman, *The Rise of "Empty Suit" Litigation. Where Should Tort Law Draw the Line?*, 80 BROOK. L. REV. 599 (2015). As another example, some state courts have adopted the "lost chance of survival" theory of medical malpractice, but others have rejected it. For an overview, see Matsuyama v. Birnbaum, 890 N.E.2d 819, 829 n.23 (Mass. 2008).

33. *See* 18 U.S.C. § 1030(e)(11) (2012); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 584–85 (1st Cir. 2001); United States v. Middleton, 231 F.2d 1207, 1213 (9th Cir. 2000) (approving jury instruction to consider "only those costs that would 'resecure' the computer to avoid 'further damage'").

34. *See* eBay Inc. v. MercExchange, L.L.C., 547 U.S. 388, 391 (2006).

35. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015).

until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur," the court held that both kinds of alleged harm were cognizable.[36] *Remijas* is widely recognized as having opened the door to standing in the subset of information privacy cases that involve data breaches. Courts around the country are now attempting to flesh out rules that more precisely distinguish the breach-related harms that are sufficiently imminent from those that are not.[37]

According to the conventional way of thinking about standing in the information privacy context, however, other kinds of asserted information privacy harms—those predicated generally on increased vulnerability to profiling and consequent marketplace and dignitary injury—are too diffuse and general to count as actionable injuries. Ryan Calo concludes, for example, that fears of heightened privacy risk are systemic or structural in character, a classification that he defends largely for reasons of taxonomic rigor.[38] And, as we already know, many hold that allegations about systemic harm are more appropriately directed elsewhere—to the political process, or perhaps to the administrative state.

I will return to the objection about the nonredressability of structural harms in Part IV; for now, I simply want to question the emerging consensus that some privacy risks are different in kind from

36. *Id*. at 693 (quoting Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013)); *see also id*. at 694 ("It is telling in this connection that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all customers for whom it had contact information and who had shopped at their stores between January 2013 and January 2014. It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded."). For a detailed exploration of the ways that heightened risk and anxiety following a data breach translate into real, concrete, and present harms, see Solove & Citron, *supra* note 1.

37. *See, e.g.*, Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 965 (7th Cir. 2016) (reversing and remanding for further proceedings based on facts similar to those in *Remijas*); *In re* Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 WL 3029783, at *14 (N.D. Cal. May 27, 2016) (holding that plaintiffs had sufficiently alleged loss of value of their personal information based largely on heightened future risk); Khan v. Children's Nat'l Health Sys., No. TDC-15-2125, 2015 WL 2946165, at *7–8 (D. Md. May 19, 2016) (distinguishing *Remijas* where plaintiffs did not allege "that some of the stolen data had already been misused, that there was a clear intent to use the plaintiffs' personal data for fraudulent purposes, or both"); *see also In re* Zappos.com, Inc. Customer Data Sec. Breach Litig., 108 F. Supp. 3d 949, 955 (D. Nev. 2015) (listing pre-*Remijas* data breach cases declining to find standing based on increased risk).

38. Calo, *The Boundaries of Privacy Harm*, *supra* note 1, at 1135, 1139–40, 1156–61; *see also* Jane R. Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205, 242 (2012) ("But it is not analytically rigorous to say that a difference in scale is a difference in kind. Without a coherent theory of harm, accretion is merely a description of the information ecosystem we live in today and not, necessarily, a threat."); Adam Thierer, *The Pursuit of Privacy in World Where Information Control Is Failing*, 36 HARV. J.L. & PUB. POL'Y 409, 417–21 (2013) (arguing that many claims of privacy harm reduce to subjective and highly variable feelings of "creepiness").

others.[39] The purported difference between data breach cases and cases about profiling more generally is that a data breach requires immediate, discrete mitigation measures to prevent payment fraud and identity theft. But the sense of emergency that surrounds data breaches has been carefully manufactured in a particular way. Large data breaches now receive widespread media coverage, and entire industries have sprung up to serve the needs of data breach victims, offering services such as credit monitoring and credit repair.[40] At the same time, media coverage of data breaches tends to point fingers at particular culprits—the data custodian, its purportedly ham-fisted employees, and/or the nameless hackers that perpetrated the theft—rather than at the background condition of widespread, "ordinary" data harvesting and processing, and there seem to be fewer concrete measures that consumers can take to mitigate that condition. That is no accident; there are no vested interests in creating a comparable sense of emergency about processes that underlie a multibillion-dollar industry. And yet many instances of payment fraud and identity theft do not stem from mass data breaches.[41] Rather, they are the foreseeable results of design choices that privilege convenience and speed over data integrity and security.

The problem, in other words, is that framing the data breach as the exception warranting emergency response has enabled courts to ignore the extent to which background norms and design practices favoring virtually unconstrained data collection, processing, and exchange harm the subjects of those practices now. Application of the imminence prong of the injury-in-fact doctrine to preclude "ordinary" information privacy claims frames the background sociotechnical landscape—including all of the factors that embed vulnerability systemically—as risk-neutral. That is a mistake, and it ignores the heuristics that have been applied in other contexts to translate risk-mitigation problems into the language of injury and remedy. In the language of the medical monitoring cases, contemporary practices of virtually unconstrained data collection, processing, and exchange gen-

39. The problem is not hypothetical. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550 (2016) (remanding for determination of whether data broker's alleged FCRA violations "entail a degree of risk sufficient to meet the concreteness requirement").

40. *See, e.g.*, HARLAND CLARKE & JAVELIN STRATEGY & RESEARCH, FEE INCOME GROWTH OPPORTUNITIES IN THE IDENTITY PROTECTION MARKET (2011), http://harlandclarke.com/files/user/page841/HC-Javelin-FeeIncome; *see also* James P. Nehf, *A Legislative Framework for Reducing Fraud in the Credit Repair Industry*, 70 N.C. L. REV. 781, 798–803 (1992).

41. *See generally* Sasha Romanosky et al., *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 J. POL'Y ANALYSIS & MGMT. 256 (2011); ERIKA HARRELL, U.S. BUREAU OF JUSTICE STATISTICS, VICTIMS OF IDENTITY THEFT, 2014, at 2 (Sept. 2015), https://www.bjs.gov/content/pub/pdf/vit14.pdf.

erate significant risks to consumers that make ongoing monitoring reasonably necessary.[42] In the language of copyright and patent cases, they also create a continuing threat of injury that cannot be remedied adequately by money damages.[43]

C. Causation and the Problem of Proximity

A third argument sometimes levied against information privacy litigants, as an objection either to standing or to liability, concerns causation. Because webs of data collection, exchange, and processing extend broadly throughout the economy, it can be difficult to trace the injuries asserted by particular plaintiffs to the actions of particular defendants. This seems to stand in stark contrast to the precision of the causal connection that exists when, for example, a defective airbag explodes. Defendants in information privacy litigation therefore argue that plaintiffs cannot link the asserted injuries to the actions of any particular firm, including their own, and courts usually agree.[44]

---

42. *See, e.g.*, *In re* Paoli R.R. Yard PCB Litig., 916 F.2d 829, 851 (3d Cir. 1990); Potter v. Firestone Tire & Rubber Co., 863 P.2d 795, 824 (Cal. 1993) (citing considerations of public health, deterrence, and social justice); Bower v. Westinghouse Elec. Corp., 522 S.E.2d 424, 431 (W. Va. 1999).

43. *See, e.g.*, Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 518 F. Supp. 2d 1197, 1217 (C.D. Cal. 2007).

44. *See, e.g.*, Resnick v. AvMed, Inc., 693 F.3d 1317, 1326 (11th Cir. 2012) ("Generally, to prove that a data breach caused identity theft, the pleadings must include allegations of a nexus between the two instances beyond allegations of time and sequence."); Stollenwerk v. Tri-West Health Care Alliance, No. 05-16990, 2007 WL 4116068, at *3 (9th Cir. Sept. 25, 2007) ("As a matter of twenty-first century common knowledge, just as certain exposures can lead to certain diseases, the theft of a computer hard drive certainly *can* result in an attempt by a thief to access the contents for purposes of identity fraud, and such an attempt *can* succeed."); Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 857 (S.D. Tex. 2015) (ruling that allegation that defendant's security flaws proximately caused theft of plaintiff's identity "fails to account for the sufficient break in causation caused by opportunistic third parties."); Jianjun Fu v. Wells Fargo Home Mortg., No. 13-cv-01271-AKK, 2014 WL 4681543, at *4 (N.D. Ala. Sep. 12, 2014) ("[B]ecause the email at issue contained both Qin and Fu's personal information and yet only Qin has had her identity stolen, it is equally plausible that the thieves obtained Qin's personal information from sources other than the email."); Jones v. Commerce Bank, N.A., No. 06-civ-835(HB), 2007 WL 672091, at *4 (S.D.N.Y. Mar. 6, 2007) ("The thieves might well have stolen Plaintiff's information without any negligence on the part of Commerce. . . . In short, the facts of this case do not establish a viable argument for *res ipsa loquitur* sufficient to overcome the lack of evidence of causation on the part of Commerce."); *cf. In re* Zappos.com, Inc. Customer Data Breach Litig., No. 12-cv-00325-RJC-VPC, 2016 WL 2637810, at *5 (D. Nev. May 6, 2016) (finding allegation of breach followed by injury sufficient for pleading purposes but noting that length of time between breach and eventual injury weighs in favor of defendant). *But see* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 696 (7th Cir. 2015) ("The fact that Target or some other store *might* have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue. It is certainly plausible for pleading purposes that their injuries are 'fairly traceable' to the data breach at Neiman Marcus."); *In re* Anthem Data Breach Litig., No. 15-MD-02617-LHK, 2016 WL 589760, at *20 (N.D. Cal. Feb. 14, 2016) ("[U]nder Defendants' theory, a company affected by a data breach could simply contest causation by pointing to the

This is not, however, the first time that the court system has been asked to recognize and then reify connections that at first appeared either nonexistent or too imprecise. Understanding and responding adequately to the dilemma of probabilistic causation has been one of the defining challenges of the modern era. Here again, courts have been more willing to innovate in some contexts than in others.

In the earliest days of the product liability revolution, the conventional ways of framing causes of action insulated mass-market manufacturers from claims brought by both end-users and unlucky bystanders. Theories of privity foreclosed bystander claims; according to those theories, persons lacking a prior commercial relationship with the manufacturer could not claim that the product had performed in a substandard fashion.[45] More fundamentally, the tort system had little experience thinking through the issues of complex harm raised by industrial processes and mass-manufactured products. To return to the problem of probabilistic reasoning in tort, the problem in such cases was that the traditional tort paradigm demanded an individualized inquiry into cause and effect, but many industrial-era injuries were predictable only in aggregate.[46] In a pair of influential opinions, then-Judge Cardozo constructed a now-familiar doctrinal device—foreseeability—for bridging the gap between statistically predictable harms and particular claimants.[47] Following Cardozo's lead, courts gradually learned to understand industrial processes as themselves amenable to inspection with regard to notions of fault and later also to see those processes as appropriate sites for interventions directed toward risk-spreading.[48]

Later in the twentieth century, the court system began to confront cases in which individuation and aggregation could not be so easily reconciled using legal fictions like foreseeability because the identity

---

fact that data breaches occur all the time, against various private and public entities. This would, in turn, create a perverse incentive for companies: so long as enough data breaches take place, individual companies will never be found liable.").

45. *See* Henningsen v. Bloomfield Motors, Inc., 161 A.2d 69, 80–84 (N.J. 1960) (discussing the privity requirement's unsuitability to the modern economy and the growing momentum to reject it); Vernon Palmer, *Why Privity Entered Tort—An Historical Reexamination of* Winterbottom v. Wright, 27 AM. J. LEGAL HIST. 85 (1983) (discussing Winterbottom v. Wright [1842] 152 ENG. REP. 402 (Exch.), the English contracts case that originated the privity requirement).

46. *See* Scheppele, *supra* note 30, at 269–72.

47. *See* Palsgraf v. Long Island R.R. Co., 162 N.E. 99, 100 (N.Y. 1928); MacPherson v. Buick Motor Co., 111 N.E. 1050, 1051 (N.Y. 1916).

48. *See* Greenman v. Yuba Power Prods., Inc., 377 P.2d 897, 900 (Cal. 1963); Escola v. Coca-Cola Bottling Co., 150 P.2d 436, 440 (Cal. 1944) (Traynor, J., concurring). *See generally* George L. Priest, *The Invention of Enterprise Liability: A Critical History of the Intellectual Foundations of Modern Tort Law*, 14 J. LEGAL STUD. 461 (1985).

of the proper defendant was also unclear. In a series of cases involving asserted manufacturing defects in generic pharmaceutical products that could not be traced with certainty to a particular manufacturer, courts in some states concluded that industry-wide failures could provide a basis for assigning causation based on participation in a well-defined market and for assigning partial liability based on overall market share.[49] Not all courts, however, have proved equally willing to assign liability in such cases. Many refused to adopt the theory of market share liability, citing concerns about fairness, administrability, and institutional competence.[50]

As it turned out, the generic pharmaceutical cases were just a rehearsal for the more complex problems that began to emerge as societal understandings of harm evolved to encompass the long-term, systemic effects of industrial development and the growing informationalization of economic activity. Even courts that had been receptive to market-share approaches balked at applying probabilistic approaches to situations in which the contours of the market were more complex. So, for example, courts have resisted extending enterprise liability theories to toxic tort cases in which different manufacturers' products contain different amounts of the substance challenged as harmful, or in which epidemiological modeling implicates both the challenged substance or practice and other causes.[51] Commentators,

---

49. *See, e.g.*, McCormack v. Abbott Labs., 617 F. Supp. 1521, 1526 (D. Mass. 1985); Sindell v. Abbott Labs., 607 P.2d 924, 937 (Cal. 1980); Hymowitz v. Eli Lilly & Co., 539 N.E.2d 1069, 1078 (N.Y. 1989); Martin v. Abbott Labs., 689 P.2d 368, 382 (Wash. 1984); Collins v. Eli Lilly Co., 342 N.W.2d 37, 48 (Wis. 1984).

50. *See, e.g.*, Smith v. Eli Lilly & Co., 560 N.E.2d 324, 338 (Ill. 1990) (predicting that market share cases would "bog down the judiciary in an almost futile endeavor"); Mulcahy v. Eli Lilly & Co., 386 N.W.2d 67, 76 (Iowa 1986) (reasoning that market share liability "involves social engineering more appropriate within the legislative domain"); Zafft v. Eli Lilly & Co., 676 S.W.2d 241, 246 (Mo. 1984) (en banc) (characterizing theory as "unfair" and "unworkable"); Gorman v. Abbott Labs., 599 A.2d 1364 (R.I. 1991) (reasoning that "the establishment of liability requires the identification of the specific defendant responsible for the injury"). *See generally* George L. Priest, *Market Share Liability in Personal Injury and Public Nuisance Litigation: An Economic Analysis*, 18 SUP. CT. ECON. REV. 109 (2010); Aaron D. Twerski, *Market Share—A Tale of Two Centuries*, 55 BROOK. L. REV. 869 (1989).

51. *See, e.g.*, White v. Celotex Corp., 907 F.2d 104, 106 (9th Cir. 1990) ("Unlike DES, which is fungible, asbestos fibers are of several varieties, used in varying quantities in the various products that contain asbestos, and each is different in its harmful effect."); Setliff v. E. I. Du Pont de Nemours & Co., 38 Cal. Rptr. 2d 763, 769–70 (Cal. Ct. App. 1995) (rejecting toxic exposure claim because "paint, solvents, strippers and glue products" are not fungible even if they possessed "common toxic chemical ingredients"); Case v. Fibreboard Corp., 743 P.2d 1062, 1065 (Okla. 1987) ("It is of major importance that *Sindell* was decided in the context of a product that was truly fungible. . . . Asbestos, on the other hand, is a name applied to a family of minerals, each member of which carries a different degree of risk."); Skipworth v. Lead Inds. Ass'n, Inc., 690 A.2d 169, 172–73 (Pa. 1997) (refusing to apply market share liability to lead paint exposure because "the relevant time period in question is far more extensive than the relevant time period

for their part, have remained both uncertain about how tort understandings of cause-in-fact might better accommodate problems of probabilistic causation and divided as to the wisdom of such accommodation.[52] Similarly, defendants in antitrust litigation and in fraud-on-the-market lawsuits filed under the federal securities laws have challenged sophisticated econometric models developed to identify and isolate price effects, arguing that price fluctuations in consumer and securities markets reflect the influence of so many factors that it is impossible to measure with precision the harm caused by any one factor.[53]

The data processing economy is highly complex, and many of its transactions and affiliations are cloaked in secrecy, which exacerbates the difficulty of tracing causes and effects.[54] In general, however, in-

---

in a DES case" and because "lead paint, as opposed to DES, is not a fungible product"). *See generally* M. Stuart Madden & Jamie Holian, *Defendant Indeterminacy: New Wine into Old Skins*, 67 LA. L. REV. 785 (2007); Allen Rostron, *Beyond Market Share Liability: A Theory of Proportional Share Liability for Nonfungible Products*, 52 UCLA L. REV. 151 (2004).

52. The literatures here are vast. For some noteworthy examples, see Kenneth S. Abraham, *Self-Proving Causation*, 99 VA. L. REV. 1811 (2013) (arguing that in certain kinds of cases a court may legitimately infer causation from negligence once the plaintiff has introduced sufficient proof regarding proper definition of the reference class) (discussing Zuchowicz v. United States, 140 F.3d 381 (2d Cir. 1998) (Calabresi, J.)); Danielle Conway-Jones, *Factual Causation in Toxic Tort Litigation: A Philosophical View of Proof and Certainty in Uncertain Disciplines*, 35 U. RICH. L. REV. 875 (2002) (arguing that causation standards in toxic tort cases should be informed by explicit social justice considerations); Steve C. Gold, *When Certainty Dissolves into Probability: A Legal Vision of Toxic Causation for the Post-Genomic Era*, 70 WASH. & LEE L. REV. 237 (2013) (proposing a "probabilistic causal contribution model" for cause-in-fact); Jane Stapleton, *Legal Cause: Cause-in-Fact and the Scope of Liability for Consequences*, 54 VAND. L. REV. 941 (2001) (mentioning "probabilities" only once (and in a footnote) in a 28-page discussion of cause-in-fact, if one excludes citations to articles with variants of the word "probability" in the title); Alex Stein, *The Domain of Torts*, 117 COLUM. L. REV. (forthcoming 2017) (arguing that tort causation doctrines properly reflect both private and public risk-allocation mechanisms at work); Richard W. Wright, *Causation in Tort Law*, 73 CAL. L. REV. 1735 (1985) (setting forth a "necessary element of a sufficient set" (NESS) test for causation); Richard W. Wright, *Liability for Possible Wrongs: Causation, Statistical Probability, and the Burden of Proof*, 41 LOY. L.A. L. REV. 1295, 1295–96 (2008) (disclaiming support for certain implications of his test after being called to Yale to admit heresy).

53. *See* Halliburton Co. v. Erica P. John Fund, Inc. 134 S. Ct. 2398, 2406–07 (2014); Comcast Corp. v. Behrend, 133 S. Ct. 1426, 1431 (2013); Jill E. Fisch, *Cause for Concern: Causation and Federal Securities Fraud*, 94 IOWA L. REV. 811, 815–29 (2009) (describing the emergence of loss causation as a focal point in fraud-on-the-market litigation). *See generally* A.B.A. SECTION OF ANTITRUST LAW, PROVING ANTITRUST DAMAGES: LEGAL AND ECONOMIC ISSUES (2d ed. 2010).

54. *See generally* U.S. SENATE COMM. ON COMMERCE, SCI., & TRANSP., OFFICE OF OVERSIGHT AND INVESTIGATIONS MAJORITY STAFF, A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES 12–13, 32–35 (2013), https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf; FRANK PASQUALE, BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015).

formation privacy cases involve both probabilistic plaintiffs (i.e., plaintiffs as to whom more discrete privacy injuries, such as loss of job opportunities, are absolutely certain in aggregate but difficult to predict on an individual level) and probabilistic defendants (i.e., defendants whose conduct contributes in an epidemiological sense to those injuries). It therefore might seem to present courts with causal conundrums beyond their capacity to resolve.

Yet resistance to assigning liability in cases involving complex, probabilistic causation is not uniform. Courts deciding tort cases continue to experiment with new models for assigning legal responsibility.[55] Plaintiffs in antitrust and securities cases sometimes manage to convince courts that their econometric models of harm are sufficiently precise to establish loss causation.[56] And here again, the intellectual property system may also to be leading the way toward a more expansive approach to judicially-enforced accountability. In *Columbia Pictures v. Fung*, a copyright case involving allegations of contributory infringement against a defendant who maintained BitTorrent sites, the Ninth Circuit observed that "where other individuals and entities provides services identical to [the defendant's], causation . . . cannot be assumed, even though fault is unquestionably present."[57] That did not end the matter, however. Instead, the court preserved the possibility of contributory infringement liability based on some showing of a "sufficient causal connection" between the defendant's conduct and

55. *See, e.g.*, Zuchowicz v. United States, 140 F.3d 381 (2d Cir. 1998) (Calabresi, J.) (reasoning that "when a negative side effect is demonstrated to be the result of a drug, and the drug was wrongly prescribed in an unapproved and excessive dosage (i.e., a strong causal link has been shown), the plaintiff who is injured has generally shown enough to permit the finder of fact to conclude that the excessive dosage was a substantial factor in producing the harm."); Alder v. Bayer Corp., AGFA Div., 61 P.3d 1068, 1086–90 (Utah 2002) (holding that plaintiffs who became ill after prolonged exposure to toxic substances need not prove precise levels of exposure where toxicity was known).

56. On uses of econometric modeling in securities litigation, see S. Austin King, Note, *Proffering the Right Evidence: Proving Loss Causation and Damages under SEC Rule 10b-5*, 18 N.C. BANKING INST. 431, 432 (2014) (reviewing methodologies and describing cases). For examples from antitrust, see *In re* Ethylene Propylene Diene Monomer (EPDM) Antitrust Litig., 256 F.R.D. 82, 97 (D. Conn. 2009) (upholding use of econometric model where "price results from only a small number of variables that are readily determined using publicly available data"); *In re* Linerboard Antitrust Litig., 497 F. Supp. 2d 666, 678 (E.D. Pa. 2007) ("Merely pointing to economic conditions that may affect the dependent variable is not enough to call into question the reliability of an econometric model.").

57. Columbia Pictures Indus. v. Fung, 710 F.3d 1020, 1038–39 (9th Cir. 2013); *see also* Perfect 10, Inc. v. Google, Inc., 653 F.3d 976 (9th Cir. 2011) (affirming denial of preliminary injunction in infringement action where plaintiif "ha[d] not shown a sufficient causal connection between irreparable harm to [its] business and Google's operation of its search engine"), *cert. denied*, 132 S. Ct. 1713 (2012). *See generally* Mark Bartholomew & Patrick F. McArdle, *Causing Infringement*, 64 VAND. L. REV. 675 (2011) (advocating an epidemiological approach to causation in contributory infringement cases).

infringement of the plaintiffs' copyrights and left open what that showing would need to entail.[58] *Fung* raises the prospect of something akin to enterprise liability for (some types of) information intermediaries. For the court, that prospect flowed logically from other evidence clearly suggesting that the defendant knew of and encouraged the use of his sites for infringement.[59] And, notably, the question of traceability did not arise, and does not appear even to have been contemplated, as an objection to justiciability.

As this progression suggests, a decision that a claimed injury is fairly traceable to the defendant's conduct is only partly about causation in the cause-in-fact sense. More generally, such decisions are about how to interpret and reconcile competing instincts about accountability and fairness. Today, those decisions often must be made in the context of emerging categories of networked, probabilistic harms that cannot be traced to any single cause to the exclusion of all others. Courts have real and legitimate reservations about their ability to do justice in such circumstances but also recognize that refusal to assign accountability may leave serious harms unremedied. They are therefore experimenting—cautiously, and in some contexts more readily than others—with new methods of assigning responsibility for complex, probabilistic harms. The various devices now being offered as tools for assigning such responsibility—epidemiological models, econometric modeling of price functions and distributions, and still-emerging theories about material contribution to copyright infringement—are examples, each with its own advantages and pitfalls. By contrast, a decision to bar information privacy plaintiffs from access to the courts on the ground that no causal link can fairly be said to exist cuts off the prospect of institutional experimentation before it can even begin.

* * *

Under each of these prongs of the standing inquiry, answers to questions about justiciability seem inextricably bound up with judgments about both value and perceived technological inevitability. The process of valuing intellectual property often entails considerable indeterminacy, but we have become accustomed both to thinking of intellectual properties as amenable to valuation and to thinking that the court system plays an important role in correcting for certain kinds of

58. *Fung*, 710 F.3d at 1039.

59. *Id.* at 1037 ("[I]f one provides a service that can be used to infringe copyrights, with the manifested intent that the service actually be used in that manner, that person is liable for the infringement that occurs through the use of the service.").

systemic problems that lead to incomplete internalization of benefits.[60] Unlike intellectual property disputes but like environmental disputes and other recent targets of the injury-in-fact doctrine, information privacy disputes involve incomplete internalization of costs by enterprises that generate undeniable economic value. Disputes about accountability for collateral damage flowing from value-generating activity seem to place the court system in tension with the seemingly inevitable direction of economic and technological progress.

Here it is important to acknowledge the political and institutional considerations that have shaped the judicial response to claims of information privacy injury. Both leniency toward intellectual property claims and strictness toward information privacy claims align with the interests of powerful information businesses that are repeat players in the litigation system. But debates about injury-in-fact in the information economy do not simply reflect a banal story of interest group capture. Rather, they hint at a more complex process involving both deep capture and institutional path-dependence. Deep capture—or capture at the level of ideology—proceeds as well-resourced repeat players work to craft compelling narratives about the contours of legal entitlements and the structure of legal institutions.[61] During times of rapid economic and sociotechnical transformation, the institutional stakes are especially high, and the outcomes described in this Part reflect the predictable results. Both leniency toward intellectual property claims and strictness toward information privacy claims align with narratives about innovation and progress that the content, technology, and information industries have worked hard to foster. Those and other industries also have worked to coopt and reshape foundational narratives about the conditions of access to the courts, entrenching a philosophy of limited judicial competence to address systemic harms.

Even as the demands of the networked information economy press courts for more sustained and thoughtful engagement, repeat-player arguments about standing in information privacy cases reflect and reinforce powerful institutional anxieties. For judges, focusing narrowly

60. *See generally* WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW 37–57, 295–331 (2003).

61. *See generally* Marc Galanter, *Why the "Haves" Come Out Ahead: Speculations on the Limits of Legal Change*, 9 L. & SOC'Y REV. 95 (1974); Jon Hanson & David Yosifon, *The Situation: An Introduction to the Situational Character, Critical Realism, Power Economics, and Deep Capture*, 152 U. PA. L. REV. 129, 222–30 (2003). The legal and regulatory paradigms that emerged during the "age of automobility" provide another example of this process in action. *See generally* Jonathan Simon, *Driving Governmentality: Automobile Accidents, Insurance, and the Challenge to Social Order in the Inter-War Years, 1919 to 1941*, 4 CONN. INS. L.J. 521 (1998); Robin L. West, *Gatsby and Tort*, *in* AMERICAN GUY 86 (Saul Levmore & Martha C. Nussbaum eds., 2014).

on discrete, particularized harms promises both a return to the judicial system's undisputed home turf and a reliable strategy for avoiding the uncertainties that attend intervention in complex, far-flung sociotechnical activities. The arguments about lack of harm, lack of imminence, and lack of causal connection advanced by information privacy defendants rest on tightly constructed syllogisms that verge on circularity—a justiciable "controversy" requires actual, concrete injury; the requirement of actual, concrete injury enables courts to avoid issuing advisory opinions; courts should avoid issuing advisory opinions because their core competence lies in the resolution of actual controversies; and so on. Whether or not that reasoning can stand on its own regarding what actually qualifies as a "controversy" is not really the point, however. The injury-in-fact inquiry underscores the complexity and sociotechnical intractability of economic power. And so judicial consensus about the nonjusticiability of certain kinds of claims begins to harden in ways that appear neutral and inevitable but cannot help being ideologically inflected.

III. Privacy Litigation and Institutional Resistance to Mass Justice Claims

Information privacy lawsuits that are deemed to present justiciable claims for relief next confront another apparent institutional mismatch, which has to do with the nature of the procedures available for achieving mass justice through litigation. The court system has already undergone one process of partial retrofitting as an institutional vehicle for mass justice claims. That process began in the early twentieth century and slowly gathered momentum as new procedures were devised to handle claims of injury stemming from mass-manufactured and mass-marketed consumer goods. As both consumer products and services and related theories of personal and economic harm have become more complex, however, and as the number of complaints has mushroomed, the judicial system has come under acute logistical and political strain. The combination of overload and repeat-player resistance has produced the procedural model that Judith Resnik calls "managerial": a system focused on processing mass claims efficiently through its various stages rather than on pausing over the systemic justice issues that those claims may raise.[62] Information privacy disputes have several features that appear to underscore the case for managerial justice, and those features have made them especially ef-

62. *See* Resnik, *Managerial Judges*, *supra* note 4, at 386–414.

fective vehicles for accelerating institutional resistance to mass justice claims.

A. Fooled Us Once, Fooled Us Twice? Mass Waiver and the Jurisprudence of Resignation

A distinctive and much-remarked feature of the contemporary litigation landscape is increasing use of private dispute resolution mechanisms as substitutes for judicial process.[63] In a wide variety of contexts ranging from employment contracts to service contracts to one-off consumer transactions, the Court has become more and more willing to require enforcement of boilerplate clauses requiring arbitration of disputes and waiver of the right to bring class claims.[64] As a result of that stance, the use of such clauses is becoming increasingly widespread.[65] Information privacy litigation brings something new to the table, however. In networked information interactions that involve collection of personal information, terms of service agreements do not simply seek to enshrine arbitration clauses. They also attempt to require users of information networks to give broad prospective consent to information collection and use, thereby effectively disclaiming any argument that mass data harvesting constitutes injury in the first place.

Debates about the validity of boilerplate arbitration clauses and boilerplate waivers follow a now-predictable path. Advocates argue that transactions mediated by boilerplate are consensual, and should

63. *See generally* Myriam Gilles, *The Day Doctrine Died: Private Arbitration and the End of Law*, 2016 U. ILL. L. REV. 371 (2016); J. Maria Glover, *Disappearing Claims and the Erosion of Substantive Law*, 124 YALE L.J. 3052 (2015); J. Maria Glover, *The Structural Role of Private Enforcement Mechanisms in Public Law*, 53 WM. & MARY L. REV. 1137 (2012); Judith Resnik, *Reinventing Courts as Democratic Institutions*, DAEDALUS, Summer 2014, at 9.

64. *See* DirectTV, Inc. v. Imburgia, 136 S. Ct. 463, 469 (2015) (enforcing class arbitration waiver even though it stated that the entire arbitration clause was "unenforceable" if the waiver was unenforceable in "the law of your state" and the waiver was signed prior to *Concepcion*); Am. Express Co. v. Italian Colors Rest., 133 S. Ct. 2304, 2309 (2013) (enforcing class arbitration waiver that prevented plaintiffs from bringing an antitrust class action against defendant); Nitro-Lift Techs., L.L.C. v. Howard, 133 S. Ct. 500, 503 (2012) (holding that validity of a non-compete clause was subject to arbitration in light of arbitration clause in the same contract); Marmet Health Care Ctr., Inc. v. Brown, 565 U.S. 530, 531–33 (2012) (holding that Federal Arbitration Act preempted West Virginia law characterizing arbitration clauses covering personal injury or wrongful death claims as antithetical to public policy); CompuCredit Corp. v. Greenwood, 565 U.S. 95, 101–02 (2012) (enforcing class arbitration waiver that applied to claims brought under Credit Repair Organizations Act); AT&T Mobility LLC v. Concepcion, 563 U.S. 333, 352 (2011) (holding that Federal Arbitration Act preempted California law characterizing class arbitration waivers as unconscionable).

65. *See* Gilles, *supra* note 63, at 400–09; Jean R. Sternlight, *Disarming Employees: How American Employers Are Using Mandatory Arbitration to Deprive Workers of Legal Protection*, 80 BROOK. L. REV. 1309, 1310 n.9, 1344–45 (2015).

be treated that way unless the party seeking invalidation can satisfy the traditional common-law standard of unconscionability. Boilerplate restrictions, they sometimes add, have been vehicles for competitive innovation, reducing potentially ruinous litigation costs and enabling companies to offer a wide variety of goods and services on a more cost-effective basis.[66] Critics argue that the widespread proliferation of boilerplate effectively substitutes private regulation for many matters in which the law should take a more active interest, and that the traditional unconscionability standard is wholly inadequate to describe what is troubling about modern marketplace relationships.[67] The rhetoric of consent, they argue, conceals a vanishingly thin conception of individual agency, consisting of little more than the ability to decline a transaction. On that view, notice-and-consent is more properly characterized as notice-and-waiver.

Challenges to the validity of boilerplate waivers generally have not persuaded courts, but the expansive scope afforded for practices of notice-and-waiver in the information privacy context is unlike that in any other area of substantive law. Although the Court has extended the reach of arbitration more and more widely, it also has consistently insisted that requiring arbitration is not the same thing as requiring individuals to waive their statutory rights altogether.[68] Whether or not that is right as a general matter, the purported distinction between preservation of claims and consensual waiver of litigation fails utterly

66. *See, e.g.*, Christopher R. Drahozal, *Arbitration Costs and Forum Accessibility: Empirical Evidence*, 41 U. MICH. J.L. REFORM 813, 840 (2008) (arguing that arbitration's lower costs increase access to fora for dispute resolution); Jason S. Johnston, *The Return of Bargain: An Economic Theory of How Standard-Form Contracts Enable Cooperative Negotiation Between Businesses and Customers*, 104 MICH. L. REV. 857, 879 (2006) (arguing that boilerplate clauses have reputational value and affect bargaining on that basis); Steven J. Ware, *Paying the Price of Process: Judicial Regulation of Consumer Arbitration Agreements*, 2001 J. DISP. RESOL. 89 (2001) (arguing that the cost savings from arbitration are passed on to consumers through competitive pricing).

67. *See generally* NANCY S. KIM, WRAP CONTRACTS: FOUNDATIONS AND RAMIFICATIONS (2013); MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2013).

68. *See Am. Express*, 133 S. Ct. at 2311 ("The class-action waiver merely limits arbitration to the two contracting parties. It no more eliminates those parties' right to pursue their statutory remedy than did federal law before its adoption of the class action for legal relief in 1938."); 14 Penn Plaza LLC v. Pyett, 556 U.S. 247, 265 (2009) (noting "that federal antidiscrimination rights may not be prospectively waived" but holding that agreement to arbitrate does not automatically amount to "a prospective waiver of the substantive right"); Mitsubishi Motors Corp. v. Soler Chrysler-Plymouth, Inc., 473 U.S. 614, 637 n.19 (1985) ("[I]n the event the choice-of-forum and choice-of-law clauses operated in tandem as a prospective waiver of a party's right to pursue statutory remedies for antitrust violations, we would have little hesitation in condemning the agreement as against public policy."). Critics argue that these decisions define statutory rights so narrowly and formalistically that they pay only lip service to the preservation of substantive claims. *See* Glover, *Disappearing Claims*, *supra* note 63, at 3076–83.

in the information privacy context because the reigning conceptualization of privacy interests as processes of self-management locates consent—and hence the possibility of waiver—at the very core of the entitlement.[69] Waiver is *ordinary and expected* and therefore untroubling to courts even when it attaches to all uses of information now or hereafter contemplated.

Courts do recognize that consent for one purpose does not automatically translate into consent for all purposes, and this limitation imposes certain procedural constraints on the implementation of notice-and-waiver strategies. Effective waiver requires attention to site design, and as a pair of recent opinions from the Ninth and Seventh Circuits makes clear, not just anything will do.[70] Among other things, an information provider must make clear that the waiver relates to the collection and processing of personal information, as opposed to other matters, and users must be given the opportunity to review the full set of disclosures and to accept the terms or reject the transaction.[71]

There is good reason to doubt, however, that the format changes deemed so significant by the courts matter much, or at all, to users. First, decades' worth of research on consumer behavior makes clear that consent is highly dependent on the way a transaction framed and therefore is highly manipulable.[72] More generally, the literature on the behavioral economics of information privacy contains a growing wealth of evidence related to user comprehension of the disclosures in privacy policies and user behavior in response to those disclosures. That evidence describes circumstances that are very different than those posited by the privacy self-management paradigm.[73] By design, privacy policies convey very little specific information about how consumer information will be used, nor do they attempt to explain the tradeoffs inherent in an information economy based on mass data harvesting, and users generally do not attempt to locate such information en route to making fully informed decisions. Instead, user behaviors and choices with regard to information privacy are most aptly characterized not by knowledge and consent, but rather by resignation.[74]

69. *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013).

70. *See* Sgouros v. TransUnion Corp., 817 F.3d 1029, 1035 (7th Cir. 2016); Lee v. Intelius, 737 F.3d 1254, 1261–62 (9th Cir. 2013).

71. *Lee*, 737 F.3d at 1260, 1262; *Sgouros*, 817 F.3d at 1035–36.

72. For good summaries, see Lauren E. Willis, *Performance-Based Consumer Law*, 82 U. CHI. L. REV. 1309, 1322–25 (2015); Lauren E. Willis, *When Nudges Fail: Slippery Defaults*, 80 U. CHI. L. REV. 1155, 1170–1200 (2013).

73. Alessandro Acquisti et al., *The Economics of Privacy*, J. ECON. LIT., June 2016, at 442–43.

74. Joseph Turow et al., *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation*, ANNENBERG SCH. COMM., June 2015, at 7; *see*

Although consumers sometimes may choose among different providers of particular services, the decision to enter the relational landscape of the twenty-first century information society is not a choice and the conditions of entry are not open to negotiation. Under the circumstances, consumers who decline to spend hours parsing their own data trails are behaving rationally, but resignation is not the same as consent.

The current climate of extreme deference to (presumed) consumer waiver has produced a powerful historical irony. As Part II.C discussed, at the dawn of the mass manufacturing age, the concept of privity of contract was deployed to minimize manufacturer liability to those injured by defective products even when injury to *someone* was foreseeable. Relying on *Winterbottom v. Wright*, a nineteenth-century English case in which denial of liability flowed in part from the form of pleading that the plaintiff had selected, manufacturers of consumer goods wove a compelling tale within which privity functioned as a necessary and appropriate safeguard against potentially unlimited liability.[75] Today, as a new generation of consumer-service purveyors seek to limit liability for information harms, they deploy (radically reenvisioned) concepts of privity to keep consumers close, barring them from asserting a variety of claims that the conduct of information businesses otherwise might support.

The definitive twentieth-century rejoinder to *Winterbottom* was *Henningsen v. Bloomfield Motors*, in which the New Jersey Supreme Court offered a detailed and decisive rejection of a car manufacturer's attempt to rely on a contract-based theory of warranty disclaimer to limit its liability for harms caused by defective manufacture.[76] Today's users are required to interact with disclaimers more actively by clicking through agreements to waive their claims, but that difference likely is not one that would have persuaded the *Henningsen* court to

---

also Kirsten Martin, *Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online*, 34 J. PUB. POL'Y & MKTG. 210 (2015); Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEGAL STUD. (forthcoming 2017).

75. Winterbottom v. Wright [1842] 152 ENG. REP. 402, 405 (Exch.); *see* Henningsen v. Bloomfield Motors, Inc., 161 A.2d 69, 80–84 (N.J. 1960) (discussing the privity requirement's unsuitability to the modern economy and the growing momentum to reject it); Priest, *supra* note 48 (tracing the gradual abandonment of privity-based theories of duty en route to the modern view of enterprise liability); Robert L. Rabin, *The Historical Development of the Fault Principle: A Reinterpretation*, 15 GA. L. REV. 925 (1981) (arguing that in the pre-industrial legal system, status-based no-duty rubrics produced a generally prevailing no-liability rule).

76. *Henningsen*, 161 A.2d at 84. The *Henningsen* court attempted to develop a more robust warranty of nondefectiveness sounding in tort; ultimately, however, the evolution of strict products liability took a different path. *See* sources cited *supra* note 48.

adopt a different rule about the enforceability of blanket disclaimers. Instead, that court focused squarely on the relational objections to abusive consumer contracting practices.[77]

In the intervening decades, however, the strange has become familiar. Form contracts have become the norm, and courts confronted with unthinkable numbers of transactions and relationships mediated by boilerplate have lost interest in parsing the terms of such arrangements. Emboldened by judicial inattention, information businesses now routinely use boilerplate terms to rearrange default entitlements and obligations covering a wide variety of matters.[78] Virtual agreements defining a broad range of permitted information practices and a narrow and possibly nonexistent range of permitted remedies sketch an information environment characterized by starkly uneven distributions of power. In validating those agreements, consent-based dismissals of information privacy claims constitute a powerful statement of institutional disengagement from the conditions of contemporary commercial life.

B. Mass Data Harvesting as Extremely Widespread and Incredibly Uncommon Injury

Some information privacy claims, typically those alleging unauthorized disclosure to or use of personal information by third parties, evade blanket defenses based on waiver.[79] Plaintiffs who seek class certification for such claims, however, may face technical and conceptual challenges that are more complex than those surrounding other types of consumer class actions. Both the technologically mediated character of information privacy violations and the presumed variabil-

77. The gross inequality of bargaining position occupied by the consumer in the automobile industry is thus apparent. There is no competition among the car makers in the area of the express warranty. Where can the buyer go to negotiate for better protection? Such control and limitation of his remedies are inimical to the public welfare and, at the very least, call for great care by the courts to avoid injustice through application of strict common-law principles of freedom of contract. Because there is no competition among the motor vehicle manufacturers with respect to the scope of protection guaranteed to the buyer, there is no incentive on their part to stimulate good will in that field of public relations.

Id. at 87.

78. For good discussions of this shift, see generally KIM, *supra* note 67; RADIN, *supra* note 67.

79. For example, the federal Electronic Communications Privacy Act prohibits the unauthorized interception and disclosure of wire and electronic communications. *See* 18 U.S.C. § 2511(1) (2012). Assuming for purposes of this section that emerging conventions for notice-and-waiver convey valid consent, an email provider such as Google can determine whether its own customers have consented to have their emails scanned for purposes of targeted marketing. It cannot, however, easily determine consent for its customers' correspondents who are not Google customers.

ity of privacy effects have presented courts with new opportunities to deny or limit class treatment.

To begin with, the actions of today's giant information businesses may implicate so many consumers, in such technically arcane ways, that simply delineating the class is quite difficult.[80] In class actions involving consumer products, courts traditionally have not required the named plaintiffs to demonstrate their ability to identify absolutely every purchaser; if such a showing were required, no consumer class action would ever be certified.[81] Interactions involving consumers' personally identifying information, however, often are embedded deeply within the operating protocols of mobile phones or web browsers and may involve complex commercial relationships among multiple companies. When firms that benefit from those complex, networked arrangements are accused of violating information privacy statutes, they often argue that the methods proposed for ascertaining the group of affected consumers are just too imprecise and conceal too much possible variation. For example, in litigation alleging that media streaming service Hulu's technical protocols violated the Video Privacy Protection Act by disclosing viewing selections and personally identifying information to third parties, the arguments about class definition required detailed expert analysis of the technical protocols used by both Hulu and Facebook to keep track of users. Hulu argued that class membership could not be verified accurately due to the number of possible variables affecting user tracking.[82] Defendants also argue that broad class definitions in actions for statutory damages threaten them with potentially crippling liability—an objection that seems to boil down to the proposition that some classes are just "too big to certify."[83] Courts reject some of these ascertainability challenges, but they also routinely decline requests to certify classes con-

80. In most circuits, a putative class plaintiff must prove that a proposed class is both sufficiently numerous to warrant class-based adjudication and sufficiently definite that its membership is ascertainable. *See* Fed. R. Civ. P. 23(a)(1); Marcus v. BMW of N. Am., LLC, 687 F.3d 583, 592–93 (3d Cir. 2012). *But see* Mullins v. Direct Dig. LLC, 795 F.3d 654, 657–58 (7th Cir. 2015) ("Nothing in Rule 23 mentions or implies this heightened requirement under Rule 23(b)(3), which has the effect of skewing the balance that district courts must strike when deciding whether to certify classes.").

81. *See, e.g.*, *In re* Scotts EZ Seed Litig., 304 F.R.D. 397, 407 (S.D.N.Y. 2015); Ries v. Ariz. Beverages USA LLC, 287 F.R.D. 523, 535 (N.D. Cal. 2012).

82. *In re* Hulu Privacy Litig., No. C-11-037640-LB, 2014 WL 2758598, at *14 (N.D. Cal. Nov. 18, 2014).

83. For detailed consideration of this question, see Parker v. Time Warner Entertainment Co., 331 F.3d 13, 25–29 (2d Cir. 2003) (Newman, J., concurring) (suggesting that very large aggregated awards threaten due process violations and arguing that courts should construe statutory damages provisions as authorizing smaller awards to each individual class member); Bert I. Huang, *Surprisingly Punitive Damages*, 100 VA. L. REV. 1027, 1046–56 (2014).

sisting of all consumers affected by the challenged activity, opting instead to certify subclasses whose involvement can be verified more precisely.[84]

Another set of challenges relates to the showing that common questions of fact or law predominate over individualized issues.[85] Here an initial problem relates, again, to waiver; this time reframed as an obstacle to mass disposition. For example, when non-Gmail customers sued Google under the wiretap laws for unauthorized scanning of emails that they had sent to or received from holders of Gmail accounts, the district court noted that questions about knowledge and waiver were integral to resolution of those claims. It reasoned that—in part because of Google's continual and widely publicized revisions of its privacy disclosures—such questions required individualized resolution, and it therefore concluded that the putative class action therefore presented insufficient predominance of common issues relating to injury.[86] In some metaphysical sense, that reasoning may even be right: Perhaps it is only in our failure to acquiesce unthinkingly to the practices of mass data harvesting that have become our background reality that we emerge as individuals. But there is an undeniable tension between the reasoning that imputes consent—purportedly the ultimate autonomous act[87]—based on acts performed unthinkingly and en masse and the reasoning that infers individuality from the absence of an opportunity to click. In neither case, moreover, does preserving actual autonomy for users of networked information services seem to be the point of the exercise. Both kinds of reasoning avoid confronting the underlying claims of injury, which allege a persistent pattern of industry conduct directed toward total electronic surveillance of consumers.

---

84. *See, e.g.*, Opperman v. Path, Inc., No. 13-cv-00453-JST, 2016 U.S. Dist. LEXIS 92403, at *8 (N.D. Cal. July 15, 2016) (declining to certify class of all users of the invasive versions of Path's software and instead limiting class to those registered as users during four-month period in which the software downloaded iDevice Contacts from all users); *In re* Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 WL 3029783, at *26 (N.D. Cal. May 27, 2016) (limiting class to those consumers who had already paid for credit monitoring or stated that they had expended personal time on credit monitoring); *In re* Hulu Privacy Litig., 2014 WL 2758598, at *14 (denying without prejudice motion to certify class of "users of both Facebook and Hulu during the class period" and suggesting possible methods of defining subclasses based on variables such as whether users remained logged in and whether and how they cleared cookies).

85. That showing is required in actions for monetary relief certified under Fed. R. Civ. P. 23(b)(3).

86. *In re* Google, Inc. Gmail Litig., No. 12-MD-02430-LHK, 2014 WL 1102660, at *13–21 (N.D. Cal. Mar. 18, 2014); *see also* Backhaut v. Apple Inc., 2015 WL 4776427, at *14–15 (N.D. Cal. Aug. 13, 2015) (following reasoning in *In re Google*).

87. *See* RADIN, *supra* note 67, at 82–98; Robin Kar, *Contract as Empowerment*, 83 U. CHI. L. REV. 759, 808–12 (2016).

Even when consent is not the critical issue, a proposed class may still fail the predominance inquiry if the court thinks that the asserted injury is too individualized to make aggregate disposition feasible. Like other would-be class claimants, information privacy litigants alleging a structural theory of wrongdoing in which common issues predominate must contend with the Court's 2011 decision in *Wal-Mart Stores v. Dukes*, which reversed the certification of a nationwide class of female Wal-Mart employees alleging a pattern of discrimination in pay and promotion.[88] Writing for a five-justice majority, Justice Scalia reasoned that because of the discretion surrounding pay and promotion decisions, the plaintiffs had not shown and could not show that they had all been discriminated against in the same way.[89] Information privacy defendants now routinely argue that *Dukes* should defeat certification of claims alleging enterprise-wide violations of information privacy rights. As support for that position, they rely on the arguments about the irreducible individuality of privacy harm that have proved so appealing to courts in the standing context.[90]

Most lower courts, however, have found class claims for violation of statutory information privacy rights more closely analogous to consumer class actions and therefore more aptly controlled by other strands of the Court's class action jurisprudence. To borrow a distinction suggested by the late Richard Nagareda, some information-era class complaints assert structural theories of civil wrongdoing roughly analogous to mass torts while others "involve the invocation of markets as the source of some common wrong."[91] For cases in the latter category, certification is the ordinary result, though it may be avoided

88. Wal-Mart Stores v. Dukes, 564 U.S. 338, 342 (2011).

89. *Id*. at 352 ("Without some glue holding the alleged *reasons* for all those decisions together, it will be impossible to say that examination of all the class members' claims for relief will produce a common answer to the crucial question *why was I disfavored*."). In fact, managerial discretion played a key role in the *Dukes* plaintiffs' theory of the case; they argued that the discretion permitted by company policy had allowed a pattern or practice of discrimination based on social stereotyping to take root. *Wal-Mart Stores*, 564 U.S. at 355; *see id*. at 371 (Ginsburg, J., dissenting) ("Wal-Mart's supervisors do not make their discretionary decisions in a vacuum. . . . The plaintiffs' evidence, including class members' tales of their own experiences, suggests that gender bias suffused Wal-Mart's company culture." (footnotes omitted)). As commentators have noted, the reversal of certification likely reflects the majority's rejection of that theory, which advances a contested interpretation of the governing law. *See* Tobias Barrington Wolff, *Managerial Judging and Substantive Law*, 90 WASH. U. L. REV. 1027, 1057–58 (2013); *see also* Richard A. Nagareda, *Class Certification in the Age of Aggregate Proof*, 84 N.Y.U. L. REV. 97 (arguing, pre-*Dukes*, that many class certification disputes really are disputes about the underlying substantive law).

90. *See, e.g.*, Bee, Denning, Inc. v. Capital All. Grp., 310 F.R.D. 614, 626 (S.D. Cal. 2015); Gossoo v. Microsoft Corp., No. CV-13-2043-SVW, 2013 WL 5651271, at *2 (C.D. Cal. Oct. 9, 2013).

91. *See* Nagareda, *Class Certification*, *supra* note 89 at 133–35.

if the market is complex and the plaintiff's expert economic report does not isolate the alleged market effect with sufficient precision.[92] As noted in Part II.A, many information privacy statutes authorize statutory damages, and some also authorize awards of profits from the unlawful activity. Arguably, claims for those remedies invoke legislative classifications of privacy harms as market-originating harms, for which all plaintiffs are entitled to uniform redress. Courts have used variants of this theory to certify classes in a number of cases, and have reasoned that even the prospect of an individuated damages determination need not defeat certification when all claims stem from the same alleged statutory violation.[93]

A judge in the influential Northern District of California, though, recently indicated that lack of predominance of common questions as to remedy may be an avenue for refusing to certify statutory information privacy claims. The context was a lawsuit brought against Facebook for scanning private messages sent between its users, and the guiding decision was not *Wal-Mart v. Dukes*, but rather *Comcast v. Behrend*, a consumer antitrust action alleging illegal acquisition of monopoly power in a regional cable television market.[94] According to a five-justice majority of the Court, the proposed class failed the predominance test because the statistical model proffered for measuring damages on a class-wide basis did not measure only the precise damages attributable to the particular antitrust injury alleged.[95]

As *Comcast* illustrates, some types of market-originating harms must be modeled, and the need for modeling to isolate the relevant portion of Facebook's profits allowed reasoning about the inherently

92. *See* Halliburton Co. v. Erica P. John Fund, Inc. 134 S. Ct. 2398, 2416–17 (2014) (holding that fraud-on-the-market defendant may contest loss causation at the certification stage); Comcast Corp. v. Behrend, 133 S. Ct. 1426, 1433–34 (2013) (holding that antitrust defendant may contest ability of plaintiff's model to isolate antitrust impact with sufficient precision at the certification stage); Nagareda, *Class Certification*, *supra* note 89, at 135–49. *Dukes*, by contrast, falls into the former category. *See* Nagareda, *Class Certification*, *supra* note 89, at 158 (criticizing later-reversed appellate decision in *Dukes* and analogizing plaintiffs' theory of discrimination to theories of "enabling torts" urged by some scholars to impose liability on facilitators of systemic harm).

93. *See, e.g.*, Eggen v. Westsconsin Credit Union, No. 14-cv-873-bbc, 2016 WL 2642255, at *1 (W.D. Wis. May 6, 2016) (Drivers' Privacy Protection Act); Bee, Denning, Inc. v. Capital All. Grp., 310 F.R.D. 614, 625 (S.D. Cal. 2015) (Telephone Consumer Protection Act); Larson v. Trans Union LLC, No. 12-cv-05726-WTD, 2015 WL 3945052, at *1 (N.D. Cal. June 26, 2015) (Fair Credit Reporting Act); *In re* Hulu Privacy Litig., No. c-11-03764-LB, 2014 WL 2758598, at *12 (N.D. Cal. Jun. 17, 2014) (Video Privacy Protection Act); *see also* Opperman v. Path, Inc., No. 12-cv-00453-JST, 2016 WL 3844326 (N.D. Cal. July 15, 2016) (tortious intrusion upon seclusion).

94. Comcast Corp. v. Behrend, 133 S. Ct. 1426 (2013).

95. *Id.* at 1433.

individualized nature of privacy harm to find a new point of entry. The plaintiffs in *Campbell v. Facebook* supported their claim for ill-gotten profits with an economic model that used a series of inferences and assumptions to isolate the portion of Facebook's profits resulting from the challenged message-scanning activity.[96] Citing *Comcast*, the district court took issue with several of the model's assumptions about that allocation and also criticized the decision to allocate an equal fractional share of those profits to each private message scanned. The court thought it wrong to assume that all customers and all messages were equally profitable and therefore concluded that common questions did not predominate in the claim for profits.[97] It further concluded that because awards of statutory damages under the wiretap laws are committed to the court's discretion, such decisions require consideration of each claimant's circumstances, so common questions did not predominate in the claim for statutory damages either.[98] That reasoning relies on the presumption of inherently individualized privacy injury from start to finish. Its logical implication is that in information privacy litigation, no class claims may be maintained for monetary relief of any sort, even when the wrongdoing consists of market-wide conduct for which Congress has provided a uniform remedy.

The combined reasoning of the *Google Gmail* and *Campbell* opinions may signal newly uncertain prospects for class-wide monetary relief in information privacy litigation, or at least for such relief under the wiretap laws. It is difficult to make such predictions, though, both because the larger class action landscape continues to shift and because the torrent of information privacy class actions continues to grow. A week after the certification motion in *Campbell v. Facebook* was argued and submitted, the Court held in *Tyson Foods v. Bouaphakeo* that plaintiffs in an action for back pay under the Fair Labor Standards Act could use statistical evidence to establish the predominance of common questions as to liability where the evidence filled a gap created by the employer's failure to keep proper records and each individual plaintiff would have needed to rely on the same evidence to sue separately.[99] Arguably, that reasoning changes the result in cases like *Campbell*, but there are also important differences between the two fact patterns. In particular, *Tyson Foods* involved a

96. Campbell v. Facebook Inc., No. 13-cv-5996-PJH, 2016 WL 2897936, at *13 (N.D. Cal. May 18, 2016).

97. *Id.* at *13–14.

98. *Id.* at *14–15.

99. Tyson Foods, Inc. v. Bouaphakeo, 136 S. Ct. 1036, 1046-47 (2016).

statute that the Court traditionally has construed liberally and a defendant that was already operating under a federal injunction to correct the challenged practices; *Campbell*, in contrast, expresses the usual skepticism about whether privacy harms even exist. Additionally, to the extent that future questions about statistical evidence and predominance turn on the Court's view of the underlying substantive question; *Comcast* may more accurately reflect the Court's consistently dismissive stance toward class action litigation involving low-dollar, high-volume consumer claims.[100]

Information privacy plaintiffs asserting structural theories of wrongdoing still may be able to assert class claims for injunctive or declaratory relief under Rule 23(b)(2), which does not require a predominance inquiry.[101] It is unclear, however, whether courts will be willing to craft discovery and remedial orders of sufficient breadth. So far, the results are not encouraging. The *Campbell* court did grant a Rule 23(b)(2) certification, but then denied plaintiffs' motion to compel discovery about the particulars of Facebook's message-scanning functionality over the three-year period in suit.[102] The judge who presided over the *Google Gmail* litigation recently certified a Rule 23(b)(2) class action against Yahoo for unauthorized email scanning, but then approved a narrowly drafted settlement that left Yahoo free to scan emails once they were no longer "in transit."[103]

C. The Filing-to-Settlement Pipeline and the Sublimation of Remedies

Debates about the standards for certification of information privacy class actions, however, may prove to be largely irrelevant for a reason that is far more fundamental: To the extent that information privacy

100. *See generally* J. Maria Glover, *Procedural Formalism and the Supreme Court's "Non-Trans-Substantive" Class Action*, 165 U. PA. L. REV. (forthcoming 2017) (arguing that the substantive question is the key in statistical evidence cases but suggesting that *Tyson Foods* and *Comcast* cannot be reconciled).

101. *See* Fed. R. Civ. P. 23(b)(2) (requiring a determination that "the party opposing the class has acted or refused to act on grounds that apply generally to the class").

102. *Campbell*, 2016 WL 2897936, at *15–16; *see also* Campbell v. Facebook Inc., 2016 WL 7888026 (N.D. Cal. Oct. 14, 2016).

103. *In re* Yahoo Mail Litig., 308 F.R.D. 577, 601 (N.D. Cal. 2015); David Kravets, *The Most Absurd Internet Privacy Class-Action Settlement Ever*, ARS TECHNICA (Aug. 30, 2016), https://arstechnica.com/tech-policy/2016/08/the-most-absurd-internet-privacy-class-action-settlement-ever/ (describing eventual settlement in the Yahoo litigation, which leaves Yahoo free to scan emails once they are no longer "in transit"); *see also* Parker v. Time Warner Entm't Co., 239 F.R.D. 318, 332 (E.D.N.Y. 2007) (declining to certify Rule 23(b)(2) settlement class in action for sale of subscriber personal information because "the defendants in this case altered their practices almost immediately with respect to the language of the original notice as well as the list sales business itself").

lawsuits continue to move forward, whether as class actions or as individual actions, they do not seem to be getting litigated. Like contemporary mass tort claims, most information privacy claims against large information businesses are funneled into consolidated multidistrict litigation proceedings. There, the claims that are denied class certification seem to disappear, while those certified as class actions tend to settle for amounts that, though widely publicized, in fact are relatively trivial.[104] Some of those settlements, moreover, have begun to follow an unusual path, coopting a device traditionally used for distribution of residual settlement funds to route payments to third parties and denying individual plaintiffs any recovery at all.

Scholars who specialize in complex litigation have begun to pay close attention to the federal courts' increasingly heavy reliance on consolidated multidistrict litigation (MDL) proceedings as a way of aggregating certain types of individual claims for more efficient processing.[105] Relative to class actions, MDL proceedings allow courts more flexibility in identifying common issues, grouping cases, and crafting comprehensive settlement decrees, a comparative advantage that has increased as the Court has ratcheted back access to class actions.[106] Class actions, however, have the benefit of formal identifi-

---

104. *See, e.g.*, Wendy Davis, *comScore Agrees to $14 Million Privacy Settlement with Panelists*, MEDIAPOST (June 3, 2014, 3:44 AM), http://www.mediapost.com/publications/article/227210/comscore-agrees-to-14-million-privacy-settlement.html; Ahiza Garcia, *Target Settles for $39 Million Over Data Breach*, CNN (Dec. 2, 2015, 5:48 PM), http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/ (describing settlements totaling $39 million to banks, $10 million to customers, and $67 million to Visa); Vindu Goel, *LinkedIn Settles Class-Action Suit Over Weak Password Security*, N.Y. TIMES: BITS (Feb. 23, 2015, 11:08 AM), https://bits.blogs.nytimes.com/2015/02/23/linkedin-settles-class-action-suit-over-weak-password-security/?_r=0 (noting the $1.25 million settlement fund); Brent Kendall, *Facebook's Settlement on 'Beacon' Service Survives Challenge*, WALL ST. J. (Nov. 4, 2013, 4:16 PM), https://www.wsj.com/articles/SB10001424052702303936904579177622940903610 ($9.5 million); Jim Puzzanghera, *AT&T to Pay $25 Million to Settle Probe of Call Center Data Breaches*, L.A. TIMES (April 8, 2015, 10:57 AM), http://www.latimes.com/business/la-fi-att-data-breach-fcc-settlement-20150408-story.html; Ryan Singel, *Online Tracking Firm Settles Suit Over Undeletable Cookies*, WIRED (Dec. 5, 2010, 2:02 AM), http://www.wired.com/2010/12/zombie-cookie-settlement/ ($2.4 million); Ross Todd, *Phone Makers Settle Carrier IQ Privacy Suits*, RECORDER (Jan. 25, 2016), http://www.therecorder.com/id=1202747932772/Phone-Makers-Settle-Carrier-IQ-Privacy-Suits?slreturn=20160701054508.

105. *See generally* Elizabeth Chamblee Burch, *Judging Multidistrict Litigation*, 90 N.Y.U. L. REV. 71 (2015); Elizabeth Chamblee Burch, *Procedural Justice in Nonclass Aggregation*, 44 WAKE FOREST L. REV. 1 (2009); J. Maria Glover, *Mass Litigation Governance in the Post-Class Action Era: The Problems and Promise of Non-Removable State Actions in Multi-District Litigation*, 5 J. TORT L. 1 (2014); Samuel Issacharoff, *Private Claims, Aggregate Rights*, 2008 SUP. CT. REV. 183, 214–20 (2008); Alexandra D. Lahav, *Bellwether Trials*, 76 GEO. WASH. L. REV. 576 (2008); *see also* Deborah R. Hensler, *Justice for the Masses? Aggregate Litigation and Its Alternatives*, DAEDALUS, Summer 2014, at 73.

106. *See* Glover, *Mass Litigation*, *supra* note 105, at 1–3; Glover, *The Structural Role of Private Enforcement Mechanisms in Public Law*, *supra* note 63, at 1213–14.

cation of common issues and are subject to regularized procedural rules, while MDL proceedings are more opaque.[107] Any procedural advantage that accrues to class actions may be illusory, though, because many putative class actions move into MDL before being certified and most cases settle while still in the preliminary stages, so the certification decision is made in the context of a motion to certify a settlement class.[108]

Information privacy litigation has followed the general patterns of opacity and orientation toward settlement that those scholars identify. Once inside the MDL process, formerly headline-grabbing lawsuits have seemingly vanished. For example, litigation over whether the Google Street View program had violated federal wiretap laws by instructing its vehicles to detect and map private wireless networks produced a widely-publicized appeal to the Ninth Circuit. Once the Ninth Circuit held that the litigation could proceed and the Supreme Court denied certiorari on the statutory interpretation question, the lawsuit was cleared to move forward.[109] That was 2014, and as of this writing the court has not yet ruled on the request for class certification.

The few lawsuits that are certified as class actions tend to settle soon afterward for dollar amounts that seem large in absolute terms—as, for example, with the $9.5 million Facebook Beacon payout or the $8.5 million Google Buzz payout—but that are minimal relative to the number of individuals affected and more minimal still when measured against the profits resulting from the challenged activity.[110] Put differently, a consequence of treating information privacy class actions as analogous to consumer class actions is that information privacy settlements tend to be priced as though the challenged conduct had produced no effects more significant than a one-time overpayment. The failure to price information privacy violations as wrongs producing substantial, continuing effects has had clear and predictable results. Information privacy settlements are widely regarded as having produced almost no meaningful change in business practices relating to

107. *See* Burch, *Judging Multidistrict Litigation*, *supra* note 105, at 79–84.

108. *See, e.g.*, *In re* LinkedIn User Privacy Litig., 309 F.R.D. 573, 584 (N.D. Cal. 2015); *In re* Netflix Privacy Litig., No. 11-CV-00379-EJD, 2012 WL 2598819, at *2–4 (N.D. Cal. July 5, 2012); *In re* Google Referrer Header Privacy Litig., No. 10-cv-04809-EJD, 2014 WL 1266091, at *2–4 (N.D. Cal. Mar. 26, 2014).

109. *In re* Google Inc. St. View Elec. Comm'n Litig., 794 F. Supp. 2d 1067 (N.D. Cal. 2011), *aff'd*, 729 F.3d 1262 (9th Cir. 2013), *amended on reh'g sub nom. by* Joffe v. Google, Inc., 746 F.3d 920, (9th Cir. 2013), *cert. denied*, 134 S. Ct. 2877 (2014).

110. For discussion of this point and detailed analysis of several recent settlements, see generally Marc Rotenberg & David Jacobs, *Enforcing Privacy Rights: Class Action Litigation and the Challenge of* Cy Pres, *in* ENFORCING PRIVACY (David Wright & Paul de Hert eds., 2015).

the collection, processing, and exchange of consumer personal information.[111]

In a growing number of information privacy cases, the court-approved settlements forego individual compensation entirely. Instead, those settlements adopt the *cy pres* device, which in recent history had been used principally as a device for disposing of unclaimed settlement funds by rerouting them to beneficiaries who might serve the purposes of the settlement.[112] At the urging of information businesses and the information privacy bar, it is becoming a device for diverting settlement funds in their entirety. The bulk of the Facebook Beacon settlement, for example, was conveyed to a newly-established entity, the Digital Trust Foundation, governed by a board that included a Facebook employee, to disburse the funds as grants to law schools and public interest organizations for projects to educate consumers on issues of online privacy and security.[113] The Ninth Circuit approved the arrangement, reasoning that the proposed use bore a "substantial nexus to the interests of the class members."[114] As the grants were doled out, what had seemed a substantial sum seemed to undergo a process of sublimation. Like ice suddenly transformed into air, it vanished, leaving only the barest traces that it had ever existed. Meanwhile, Facebook—prohibited only from continuing the Beacon program under its original name—devised very similar programs to replace it.

The ostensible rationale for *cy pres* settlements in information privacy cases is that, since the costs of distributing payments to each class member would exceed the individual payment amounts, the funds should be put to the next best use. That reasoning, though, validates the ongoing construction of privacy harms as minor inconveniences, worth less to the average consumer than the costs of a faulty digital storage device or an overcharge from an ebook store.[115] And condi-

111. *See id*. at 325–26; *see also* Kravets, *supra* note 103. This does not mean that there have been no changes in firm behavior. *See generally* KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE (2015) (discussing emergence of privacy compliance culture and management structures within firms).

112. For a review of the doctrine and its history, see Rhonda Wasserman, Cy Pres *in Class Action Settlements*, 88 S. CAL. L. REV. 97, 114–17 (2014).

113. *See* Rotenberg & Jacobs, *supra* note 111, at 321.

114. Lane v. Facebook, Inc., 696 F.3d 811 (9th Cir. 2012), *cert. denied*, 134 S. Ct. 8 (2013).

115. *See, e.g.*, *In re* Nvidia GTX 970 Graphics Chip Litig., No. 4:155-cv-00760 (N.D. Cal. Dec. 7, 2016) (approving settlement entitling eligible consumers to $30 per qualifying device); *In re* Optical Disk Drive Antitrust Litig., No. 3:10-md-021430RS (N.D. Cal. Apr. 14, 2016) (approving settlement entitling eligible consumers to "up to $10" per qualifying device); *In re* Apple eBooks Antitrust Litig., ECF No. 686, No. 11-md-02293 (Nov. 21, 2014) (approving settlement entitling

tioning *cy pres* awards on commitments to educate the public about the privacy and security issues generated by the data harvesting activities of information businesses effectively validates those activities, reinforcing the notion that privacy erosion is both inevitable and nonredressable by conventional means.

The jurisprudence of the *cy pres* settlement is still evolving, so it's possible that the courts will impose additional restrictions on its use. The Ninth Circuit's approval of the Facebook Beacon arrangement elicited two strongly worded dissents, and although the Supreme Court denied certiorari, a rare separate statement by Chief Justice Roberts signaled that the Court is paying close attention.[116] In the meantime, though, lower courts seem to be embracing the *cy pres* device with enthusiasm.[117]

* * *

Returning to the themes of deep capture and institutional path-dependence that emerged from Part II's exploration of the injury-in-fact doctrine, we can see both factors continuing to shape the judicial response to those information privacy claims that survive standing challenges. For starters, decisions about waiver of claims, class ascertainability and commonality of injury (or lack thereof), and the structure of settlement payouts seem inevitably bound up with the substantive characterizations of privacy injury that Part II explored. When courts issue decisions dismissing information privacy claims or deflecting putative class claims, their reasons tend to track the prevailing conceptualization of privacy injury as individualized, evanescent, and ultimately noncompensable. Once again, though, struggles over the proper conceptualization of information privacy litigation also widen to implicate—and coopt—foundational conceptions of institutional role and structure. The arguments for dismissing or deflecting information privacy claims impliedly represent such claims as *simultaneously* too individualized and too widespread to remedy. They both rely on and reinforce conceptions of litigation as inherently individual-

eligible consumers to $6.93 for each New York Times bestseller and $1.57 for all other books). On the possible benchmarking effects of such settlements, see generally Ben DePoorter, *Law in the Shadow of Bargaining: The Feedback Effect of Civil Settlements*, 95 CORNELL. L. REV. 957 (2010).

116. *See* Lane v. Facebook, Inc., 696 F.3d 811, 834 (9th Cir. 2012) (Kleinfeld, J., dissenting), *cert. denied*, 134 S. Ct. 8 (2013); Lane v. Facebook, Inc., 709 F.3d 791, 793 (9th Cir. 2013) (Smith, J., dissenting from denial of rehearing en banc).

117. *See generally* Rotenberg & Jacobs, *supra* note 111; Matt Vella, *Google and Facebook's New Tactic in the Tech Wars*, FORTUNE (July 30, 2012), fortune.com/2012/07/30/google-and-facebooks-new-tactic-in-the-tech-wars/.

ized and of judicial institutions as having only limited capacity to address mass harms.

The preferred mechanisms for disposing of information privacy claims—devolution to private ordering, narrowing or dismissal of class claims on grounds of impermissible variability, sublimation of remedies via *cy pres* payouts for educational efforts that reinforce the status quo—are best understood and evaluated as contingent institutional formations. Casting about for new ways of handling unfamiliar logistical and conceptual problems, courts are responding to strategic interventions by powerful repeat players interested first and foremost in shielding their business models and information processing practices from judicial oversight. Through their efforts, a new model of procedural justice is taking shape—one that comports in some respects with the demands of the networked information economy but that also is heavily inflected by the more parochial concerns of information capitalists.

IV. Privacy, Power, and the Logic of Judicial Irrelevance

Why assume, though, that the courts are the appropriate forum in which to challenge widespread practices of information collection, processing, and use? As Part II noted, some privacy scholars have argued that although the complex questions surrounding information industry structure and organization have privacy implications, those questions do not automatically translate into judicially cognizable privacy injuries.[118] The information industries, meanwhile, have consistently argued that striking the proper balance between privacy and innovation is not a job for courts.[119] The arguments advanced in debates about standing and class certification in information privacy cases parallel those advanced for the last several decades in debates about the efficacy of mass tort litigation and the desirability of mass tort reform. Some have argued that insurance markets can regulate product safety more effectively, while others maintain that the administrative state is better-equipped to address complex harms that implicate the structure of entire industries.[120]

---

118. *See supra* note 38 and accompanying text.

119. *See supra* note 2 and accompanying text.

120. For a sampling of perspectives on those questions, see generally The Liability Maze: The Impact of Liability Law on Safety and Innovation (Peter W. Huber & Robert E. Litan eds., 1991); New Directions in Liability Law (Walter Olson ed., 1988); Tort Law and the Public Interest: Competition, Innovation and the Consumer Welfare (Peter Schuck ed., 1991); John C.P. Goldberg & Benjamin C. Zipursky, *The Easy Case for Products Liability Law: A Response to Professors Polinksy and Shavell*, 123 Harv. L. Rev. 1919, 1928–34 (2010); Mark M. Hager, *Civil Compensation and Its Discontents: A Response to Huber*, 42 Stan.

While the institutional competence inquiry is important, it also risks holding constant what ought to be (and in fact already is) in motion. First and most basically, the relationships between and among courts, agencies, and the political process are dynamic. Litigation outcomes can reinforce administrative inertia or spur administrative action. More fundamentally, legal institutions are not "fixed, Archimedean points around which modes of economic development shift and cohere."[121] Institutional design responds to prevailing modes of economic and sociotechnical development, and at times of rapid change in modes of development, institutions too are in flux. The questions now on the table—for courts and administrative entities alike—concern the best paths for institutional evolution in an era when informationalism is emerging as the prevailing mode of economic development and when that shift has exposed harms that are systemic, networked, and collective.[122]

The patterns of harm and benefit in the networked information economy are complex and difficult to unravel, and relationships between business and consumers typically involve instrumentalities that are much less concrete than cars and soda bottles. It seems relatively easy to point to the manufacturing specifications for a glass bottle or a set of tires but much more complicated to identify the specifications needed to minimize privacy harms in the networked information environment. It is difficult to agree what might constitute a data processing defect, and the background conventions and practices are themselves undergoing rapid change. By comparison with these uncertainties, the interlinked narratives of virtuous labor and innovation advanced by the data processing industries to dissuade courts from interfering with new business models seem compelling.[123]

L. REV. 539 (1990) (reviewing PETER W. HUBER, LIABILITY: THE LEGAL REVOLUTION AND ITS CONSEQUENCES (1988)); Richard A. Nagareda, *Turning from Tort to Administration*, 94 MICH. L. REV. 899 (1996); Joseph A. Page, *Deforming Tort Reform*, 78 GEO. L.J. 649 (1990); Robert L. Rabin, *Some Thoughts on the Efficacy of a Mass Toxics Administrative Compensation Scheme*, 52 MD. L. REV. 951 (1993).

121. Julie E. Cohen, *The Regulatory State in the Information Age*, 17 THEORETICAL INQ. L. 369, 371 (2016).

122. On the shift from industrialism to informationalism, see *id*. at 370–73. *See* 1 MANUEL CASTELLS, THE INFORMATION AGE: ECONOMY, SOCIETY AND CULTURE 14–18 (1996); DAN SCHILLER, HOW TO THINK ABOUT INFORMATION 3–35 (2007). *See generally* JAMES R. BENIGER, THE CONTROL REVOLUTION: TECHNOLOGICAL AND ECONOMIC ORIGINS OF THE INFORMATION SOCIETY (1986).

123. On the narratives that underpin the personal data processing economy, see generally Julie E. Cohen, *The Surveillance-Innovation Complex: The Irony of the Participation Turn*, *in* THE PARTICIPATORY CONDITION 207 (Darin Barney et al. eds., forthcoming 2016); Julie E. Cohen, *The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy*, 30 PHIL. & TECH. (forthcoming 2017), https://link.springer.com/article/10.1007/s13347-017-0258-2.

And yet the challenges now confronting the courts are less unfamiliar than they appear. Both the products liability revolution and the emergence of mass torts required new types of inquiries. As the products liability revolution got underway, assigning liability for manufacturing defects required judgments about both the specifications for individual product units and the design of the factory production line, and those judgments too had to be made at a time when products and manufacturing standards were evolving rapidly. Mass tort litigation required courts to contend with still more complex harms occurring as unintended byproducts of development. Assigning liability for mass torts required judgments about the effects of chemical or pharmaceutical exposure, and those judgments relied on new epidemiological constructs for modeling and measuring harms. Then, as now, manufacturers made arguments about the economic value of their activities and the necessary costs of innovation in production and distribution.

Although courts and legislatures initially accepted manufacturers' arguments about the costs to innovation, the risks of decision making under uncertainty, and the jurisprudential pitfalls of probabilistic causation, they became more skeptical as the toll of those injured by industrial products and byproducts continued to mount. Then, as now, certain types of issues ultimately required institutional settlements characterized by significant reliance on the regulatory state. For example, courts were not equipped to supervise passive restraint implementation or other technical standards affecting vehicle crashworthiness, both matters that are now the subject of detailed regulations.[124] Nor were they equipped to oversee new-drug approval processes, conduct safety testing on chemicals used in consumer products, or determine ambient pollutant limits.[125] At the same time, though, both product liability litigation and mass tort litigation played useful roles in catalyzing a societal shift toward a thicker notion of industrial responsibility.[126] And to the extent that the eventual regulatory settlements fell short of the standard that some proponents of

124. *See* 15 U.S.C. § 1232 (2012) (establishing standards for labeling relating to NHTSA's crash ratings); 49 C.F.R. § 571.208 (establishing vehicle crashworthiness standards); 49 C.F.R. § 572 (establishing standards for use of dummies in crash testing).

125. *See, e.g.*, 21 C.F.R. § 314.1 *et seq*. (establishing process for new drug approval); 16 C.F.R. Part 1500 (defining procedures for consumer product safety testing pursuant to the Federal Hazardous Substances Act); 40 C.F.R. Part 50 (establishing standards for ambieint air quality)

126. On the ways that litigation and regulation can facilitate complementary processes of knowledge production about risk of harm, see generally Mary L. Lyndon, *Tort Law and Technology*, 12 YALE J. ON REG. 137 (1995).

strict liability may have wanted, that too seems inevitable; institutional realignment is at its core a process of compromise.[127]

The question is not whether information privacy litigation alone will move the information industries toward desired levels of precaution and accountability, but rather whether a governance system in which the policy lever of aggregate litigation has been disabled will do so. Here it is worth considering what would have happened if the courts in the defective products cases had chosen to treat the risks as structural and nonredressable, or if the courts in the mass tort cases of the 1970s and 1980s had chosen to treat the harms as too individuated for mass resolution to make sense. The result might have been a robust regime of private safety certification—perhaps with top-drawer ratings bodies such as Underwriters' Laboratories and Consumer Reports playing a much more prominent role—or it might have been a regime of administrative controls on consumer product manufacturing whose reach was far more comprehensive. Those speculations, however, do not align well with the patterns of power and disempowerment now emerging in the contemporary information economy.

The pressure on our cobbled-together system of partial and largely consent-based information privacy protections is growing. The complex patchwork of sector specific fair-information-practices regulations, consent decrees enshrining data security obligations tethered to evolving industry best practices, and state-specific data breach notification laws has produced incomplete and ineffectual protection

127. Nor are the results necessarily durable. For an extended exploration of efforts over the last four decades to undo the mid-twentieth-century regulatory settlements in the domains of product safety, worker safety, and consumer protection, see generally THOMAS O. MCGARITY, FREEDOM TO HARM: THE LASTING LEGACY OF THE LAISSEZ FAIRE REVIVAL (2013). For examples of decisions illustrating the back-and-forth between courts and agencies in the domain of automotive safety, see Williamson v. Mazda Motor of Am., Inc., 562 U.S. 323, 332 (2011) (holding that 49 C.F.R. § 571.208, permitting auto manufacturers to choose between lap belts and lap-and-shoulder belts in rear seats, did not preempt a design defect suit brought under state tort law because the choice offered to manufacturers was not "a significant regulatory objective"); Geier v. Am. Honda Motor Co., 529 U.S. 861, 864–65 (2000) (holding that Federal Motor Vehicle Safety Standard 208, which established a phase-in period for passive restraints in vehicles, preempted a design defect suit brought under state tort law). For decisions illustrating similar processes in federal food and drug regulation, see, e.g., PLIVA, Inc. v. Mensing, 564 U.S. 604, 613 (2011) (holding that the FDA's interpretation of certain regulations as imposing a duty of "sameness" on generic drug labels preempted a labeling defect suit brought under state tort law); Wyeth v. Levine, 555 U.S. 555, 558–59 (2009) (holding that FDA labeling regulations did not preempt a failure-to-warn suit brought under state tort law); Altria Grp., Inc. v. Good, 555 U.S. 70, 72–73 (2008) (holding that the Federal Cigarette Labeling and Advertising Act did not preempt a suit for fraudulent labeling brought under the Maine Unfair Trade Practices Act); Riegel v. Medtronic, Inc., 552 U.S. 312, 330 (2008) (holding that FDA safety requirements for catheters preempted a design defect suit brought under state tort law).

against the growing costs of information entropy.[128] There is no regulatory entity with general jurisdiction over data protection in the United States and little momentum to create one.[129] Corrective measures now being put in place by industry consensus, such as the incompletely implemented scheme for microchip-based point-of-sale protection that replicates some (but not all) features of the more robust and effective European regime for preventing credit card fraud, do not seem to be working to stem the flood of payment fraud and identity theft.[130] And almost nothing seems to constrain the burgeoning data-processing market, which rewards new methods of sorting consumers for maximal surplus extraction.

As this capsule summary of regulatory dysfunction suggests, moreover, the administrative state is currently confronting a crisis of its own with the same root causes. Across vast sectors of the economy, administrative processes are widely regarded as having failed to respond adequately to the regulatory problems created by the emergence of informationalism as the principal mode of economic development and by the increasing involvement of networked, digital information technologies in regulated processes of all sorts.[131] Regulatory paradigms like market power and antidiscrimination no longer cohere in a world characterized by information overload and platform-based, algorithmic intermediation.[132] And regulatory processes designed for a

128. On information entropy and its costs, see Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1749–50 (2010).

129. The information industries and their advocates in pro-business and libertarian think tanks have consistently argued that striking the proper balance between privacy and innovation is not a job for regulators, either. *See, e.g.*, *Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 112th Cong., 2d Sess. 146–49 (2012) (statement of Michael Zaneis, Senior Vice President and General Counsel, Interactive Advert. Bureau); Letter from Daniel Castro, Dir., Ctr. for Data Innovation, to Nicole Wong, White House Office of Sci. & Tech. Pol'y (Mar. 31, 2014), http://www.itif.org/publications/public-policy-implications-big-data; *see also* Larry Downes, *A Rational Response to the Privacy "Crisis,"* CATO INST. POL'Y ANALYSIS (Jan. 7, 2013), http://www.cato.org/sites/cato.org/files/pubs/pdf/pa716.pdf; Berin Szoka & Adam Thierer, *Targeted Online Advertising: What's the Harm and Where Are We Heading?*, PROGRESS ON POINT, June 2009, at 1. *See generally* Julie E. Cohen, *The Surveillance-Innovation Complex*, *supra* note 123.

130. *See*, *e.g.*, Erika Harrell, *Victims of Identity Theft, 2014*, U.S. BUREAU OF JUST. STAT. (Sept. 2015), http://www.bjs.gov/content/pub/pdf/vit14.pdf; Press Release, U.S. Bureau of Justice Statistics, 17.6 Million U.S. Residents Experienced Identity Theft in 2014 (Sept. 27, 2015), http://www.bjs.gov/content/pub/press/vit14pr.cfm. As Adam Levitin explains, the regime reflects a pragmatic compromise among banks and payment providers on one hand and merchants on the other, and also is influenced by the background division of liability for card-present versus card-not-present (e.g., online) fraud. *See* Adam J. Levitin, *Private Disordering? Payment Card Fraud Liability Rules*, 5 BROOK. J. CORP., FIN. & COM. L. 1 (2010).

131. *See generally* Cohen, *Regulatory State*, *supra* note 121.

132. *See id.* at 375–89.

different era are struggling to assimilate the new regulatory challenges posed by software-based control of industrial, financial, and informational activities.[133]

At a time of institutional ferment that spans multiple branches of government, it is no answer to say that the risks to consumers from widespread data harvesting, processing, and exchange are systemic or structural in a way that forecloses, or ought to foreclose, the very idea of litigated relief. The idea that arguments about *risk* should not be cognizable as arguments about *harm* makes sense only if we posit the risk in question as a background feature of an invariant physical environment. That might make sense if we are thinking about the risk of being struck by lightning or hit by a falling meteorite. It is wholly inadequate as an account of responsibility for risks that arise as contingent and path-dependent features of the built environment.[134]

More precisely, as we continue busily constructing classes of consumers who lack remedies before the law, it is important to recognize that the condition of legal disability is artificial and institutionally determined. This point parallels Lee Fennell's argument about the ways that different designs for property institutions redistribute resource access costs.[135] In the context of the tort system, different institutional design features redistribute the costs of market participation, sometimes allocating those costs in ways that prompt internalization of an activity's costs and sometimes allocating costs in other ways. Conversely, if a different pattern of cost distribution is desired, common law or statutory liability for privacy harms may play a useful role in forcing it.

By the same token, it also is no answer to posit timeless, invariant distinctions between institutional forms and competencies—based, for example, on the difference between individual and collective claims, or between retrospective and prospective relief. As the rise of MDL proceedings illustrates, reality has a way of complicating such neat academic dichotomies. The fact that courts have become increasingly hostile to experimentation with the class action device does not mean that the judicial system has become hostile to innovation with new methods for processing and resolving mass claims. Disputes about information-economy problems are calling forth new litigation hybrids

133. *See id*. at 402–13.

134. *Cf*. Mari J. Matsuda, *On Causation*, 100 COLUM. L. REV. 2195, 2209–11 (2000) (arguing that facially neutral rules allocating responsibility can conceal important background questions about both accountability and distributive justice).

135. *See generally* Lee Anne Fennell, *The Problem of Resource Access*, 126 HARV. L. REV. 1472 (2013).

(and new administrative hybrids as well).[136] One possible future for the courts, to borrow from Seth Kreimer, is that the judicial system simply will become increasingly irrelevant in the era of networked, systemic, information-based harms.[137] But the facts on the ground already hint at a more complex set of possibilities.

Courts now refusing to engage directly with information privacy claims are not just passing the buck to other legal institutions; they also are working actively to define another possible future—one in which different kinds of claims and claimants are accorded different kinds of process and in which mass actions are systematically deprived of their potential force as a lever for broader sociotechnical change. They would do better to reckon more directly and deliberately with what is at stake. In an era of systemic, networked harms that inevitably generate mass claims, the judicial system can remain a force for transformative legal change only if it also is willing to embrace transformation for itself.

V. Conclusion

Questions about standing, waiver, joinder, and so on are more than just questions about purity of institutional form. They are questions about the precise location of the fault line between the rule of law and the rule of economic power. The information privacy lawsuits now inundating the courts are part of a larger process of institutional change, both the scope and direction of which are contested. The outcomes of information privacy lawsuits will help to determine the extent of powerful new industries' ability to act in the market with relative impunity for harms to individual consumers and to the public. They also will help to shape the institutional forms of law in the information era.

136. On MDL and litigation hybrids, see *supra* note 105 and accompanying text; *see also* Peter H. Schuck, *Mass Torts: An Institutional Evolutionist Perspective*, 80 Cornell L. Rev. 941, 956–63 (1995). On administrative hybrids, see Richard A. Nagareda, *Future Mass Tort Claims and the Rule-Making/Adjudication Distinction*, 74 Tul. L. Rev. 1781, 1788–92 (2000). *See generally* Nagareda, *Class Certification*, *supra* note 120 (urging the development of hybrid administrative proceedings for supervising the disposition of mass tort claims); Michael D. Sant'Imbrogio & Adam S. Zimmerman, *The Agency Class Action*, 112 Colum. L. Rev. 1992 (2012); Adam S. Zimmerman, *Distributing Justice*, 86 N.Y.U. L. Rev. 500 (2011); Administrative Conference of the United States, Aggregation of Similar Claims in Agency Adjudication 3–6 (June 10, 2016), https://www.acus.gov/sites/default/files/documents/aggregate-agency-adjudication-final-recommendation_1.pdf.

137. Kreimer, *supra* note 7, at 795–96.