The Danger of Contextual Integrity

Mihailis E. Diamantis
University of Iowa College of Law, USA

Contextual integrity has now become a (the?) dominant academic theory of privacy. It identifies privacy as both complex and social, two alluring attributes that other leading theories reject. Scholars who engage contextual integrity mostly do so only to convey their confidence in it as their working framework. Even passingly critical notes are rare. This article offers a legal realist critique: Were contextual integrity adopted as a legal standard, it would undermine the very values it was intended to protect, systematically favoring data-hungry corporations at the expense of an already shrinking zone of protected individual privacy. Contextual integrity is dangerous precisely because of the complexity and sociality that draw so many scholars to it. In an adversarial courtroom that pits corporate data interests against aggrieved individuals, these theoretical virtues favor the more sophisticated, well-funded, repeat player.

Key Words: data privacy, legal realism, contextual integrity, corporate power

Trojan Horse:
"A computer program that appears to have a useful function, but also has a hidden and potentially malicious function."[1]

"Privacy itself is in jeopardy."[2] Before contextual integrity was first proposed, there was good reason to worry. In the pages of law journals and judicial opinions, privacy was fighting with one hand tied behind its back. Legal scholarship at the time had largely embraced a notice-and-choice paradigm that allowed corporate parties to collect and use personal data in any way so long as it was disclosed in their terms of service.[3] Since consumers do not read or understand these documents (in no small part because corporations make them difficult to read and understand),[4]

[1] Michael Niels et al., An Introduction to Information Security 86 (2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.

[2] Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life 6 (2010).

[3] Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880, 1882–83 (2013).

[4] Mihailis E. Diamantis et al., *Forms of Disclosure: The Path to Automating Closed Book Privacy Audits*, 37 Harv. J. L. & Tech. 1265, 1268 (2024) ("Big tech put consumers on formal notice about data practices, usually in long, technical, and loophole-riddled documents. Eventually, though, it became apparent that 'notice and choice' was synonymous with 'anything goes.'").

Business Ethics Quarterly (2025), pp. 1–21. DOI:10.1017/beq.2025.10085
Published by Cambridge University Press on behalf of the Society for Business Ethics.

corporate parties effectively had free rein.[5] Legal doctrine was saddled with a strict historical dichotomy between public and private data. The law's position on public data—which included any personal information that an individual ever made available to a third party—was that just about "anything goes."[6] In a society and economy increasingly intermediated by third-party social media platforms, online retailers, internet service providers, and apps, corporate parties unrelentingly hoovered up, packaged, and resold information that consumers made available to an ever-expanding data ecosystem.[7]

Contextual integrity offered a new perspective on privacy to an eager audience. It promised nuance that simplistic dualities like consensual/coerced and private/public could not.[8] It shifted the focus from static data to dynamic flows of information. These latter were to be characterized not by singular on-off switches, but by five scalar parameters. Since the norms that govern information flows vary with social context, all the subtleties of social inquiry came to bear. With this sophisticated theoretical apparatus, contextual integrity could explain how, for example, one could retain privacy interests even while in public or even after revealing information to a trusted third party.

While the growing body of (mostly) state privacy law in the United States has continued to root itself by and large in the notice-and-choice framework,[9] contextual integrity has spread widely in academic circles. It is not unfair to say that contextual integrity has now become a (if not *the*) dominant theory of privacy among policy-oriented scholars in law and computer science.[10] A systematic study of computer scientists who discuss contextual integrity found various levels of comprehension, but no dissenters.[11] A review of law articles from the last five years that mention

[5] Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 4 DAEDALUS 32, 35 (2011) ("[A]mple evidence reveals that people do not read privacy policies, do not understand them when they do, and realistically could not read them even if they wanted to."); Christopher G. Bradley, *Privacy for Sale: The Law of Transactions in Consumers' Private Data*, 40 YALE J. REG. 127, 133 (2023); CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 146–47 (2016).

[6] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 136–37 (2004).

[7] Mihailis E. Diamantis, *Privileging Privacy: Confidentiality as a Source of Fourth Amendment Protection*, 21 U. PA. J. CONST. L. 485, 487–88 (2018).

[8] NISSENBAUM, *supra* note 2, at 11 ("[T]he framework of contextual integrity is sufficiently expressive to model peoples' reactions to troubling technology-based systems and practices as well as to formulate normative guidelines for policy, action, and design.").

[9] *See generally* Lakshmi Gopal, *State Privacy Law Update*, 79 BUS. LAWYER 221 (2023) (summarizing state privacy laws).

[10] Despite being published two decades ago, the paper that introduced contextual integrity to legal scholarship, "Privacy as Contextual Integrity," is still ranked fifth for annual accesses on HeinOnline among articles that mention "privacy" in their title. *See also* Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039, 1042 (2018) (listing "the three dominant conceptions of privacy: access (the law and economics conception of privacy as concealment), control, and context"); NEIL RICHARDS, WHY PRIVACY MATTERS 80 (2021) (describing contextual integrity as a "highly influential" "leading theor[y]"); Huichan Xia, *A Critique of Using Contextual Integrity to (Re)consider Privacy in HCI*, in INFORMATION FOR A BETTER WORLD: NORMALITY, VIRTUALITY, PHYSICALITY, INCLUSIVITY 251, 252 (I. Sserwanga et al. eds. 2023) (describing contextual integrity as "more popularized [than competing theories] in HCI [human computer interaction]").

[11] *See generally* Sebastian Benthall, Seda Gürses, & Helen Nissenbaum, *Contextual Integrity Through the Lens of Computer Science*, 2 FOUNDS. & TRENDS PRIVACY & SEC. 1 (2017).

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press

"contextual integrity" uncovers much the same[12]—occasional off-hand expressions of concern, but mostly various formulations of "[t]his Article adopts … contextual integrity theory to conceptualize privacy."[13] If (as every law professor hopes) trends in legal scholarship foreshadow trends in law, anyone interested in where privacy policy is headed should take note of contextual integrity.

Last year, contextual integrity turned twenty.[14] Its fledgling days are long passed. The time has come to reckon not only with the view's exciting possibilities, but also with the weaknesses that inevitably plague any ambitious theory. Contextual integrity has had scattered critics over the years, mostly among theorists.[15] Michael D. Birnhack, Alexandra Prégent, and James B. Rule separately argued on philosophical and sociological grounds that contextual integrity is an ambiguous theory that does not yield determinate results (I will return to this critique below).[16] Nora McDonald and Andrea Forte use critical studies to conclude that contextual integrity would further marginalize vulnerable populations.[17] And Neil Richards devotes five pages of his most recent book to characterizing contextual integrity as a manipulable "theory of creepy."[18] Contextual integrity's architects have yet to meaningfully these critiques.[19]

This article turns from theory to practice, aspiring to provoke a hard look at how contextual integrity would affect privacy rights if it were adopted as a rule of legal decision. Below, I try to predict the sorts of conclusions human judges applying

[12] A search of Westlaw's "Secondary Sources" database returns 151 sources published in 2019 or later. Only ten provide critical discussion of contextual integrity and opt for another privacy framework. Data available from author upon request.

[13] Jiaying Jiang, *Privacy Implications of Central Bank Digital Currencies*, 54 SETON HALL L. REV. 69, 76 (2023).

[14] "Contextual integrity" and "privacy" first appeared in the same paragraph of a law journal issue in 2004. Nissenbaum, *supra* note 6 at 120.

[15] Unfortunately, I do not have space for a comprehensive survey of existing, albeit limited, criticism of contextual integrity. Where relevant, I cite many of the view's critics below.

[16] Michael D. Birnhack, *A Quest for a Theory of Privacy: Context and Control*, 51 JURIMETRICS 447, 471 (2011) ("Although [contextual integrity] results in a seemingly neutral decision heuristic, many of its stages require its users to make normative judgments" which "inevitably depend[] on the eyes of the beholder."); Alexandra Prégent, *Why You Should Not Use CI to Evaluate Socially Disruptive Technology*, 38 PHIL. & TECH. 6, 8–19 (2025); James B. Rule, *Contextual Integrity and Its Discontents: A Critique of Helen Nissenbaum's Normative Arguments*, 11 POL'Y & INTERNET 260, 272 (2019) ("It is not reasonable to imagine that different analysts, however conscientious, would necessarily arrive at the same conclusions [by applying contextual integrity], even if confronted with the same facts.").

[17] Nora McDonald & Andrea Forte, *The Politics of Privacy Theories: Moving from Norms to Vulnerabilities*, 1 CHI'20, paper 40, 1 (2020) ("[T]he unique privacy concerns of vulnerable populations can slip through [contextual integrity's] norm-based analyses of privacy requirements.").

[18] RICHARDS, *supra* note 10, at 81–82 (2021).

[19] Indeed, in a survey of papers by Nissenbaum and others who have coauthored with her on multiple occasions (a group that includes at least 55 authors), only six have cited the critical papers referenced here. Only one acknowledges the cited paper's critique. *See* Daniel Susser & Laura Y. Cabrera, *Brain Data in Context: Are New Rights the Way to Mental and Brain Privacy?*, 15 AJOB NEUROSCI. 122, 126 n.9 (2024) ("For a longer, critical discussion about the relationship between contextual integrity and control theories of privacy, see (Brinhack 2012)."). This analysis was conducted in September 2025 using the "cited by" function in Google Scholar. It must be acknowledged that Google Scholar's database, while comparatively comprehensive, does have gaps.

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press

contextual integrity would reach in cases that pit data-hungry corporations against individuals whose privacy is at stake. The methodology I adopt aspires to realism rather than idealism, so the political economy of the modern world will play an important role. From this perspective, several new concerns about contextual integrity emerge. I argue we should expect neutral judges applying contextual integrity generally to favor corporate parties. The theory is not just ambiguous, marginalizing, and "creepy"—it threatens the very values it seeks to protect.

The goal of this article is to advance an internal critique of contextual integrity, not to advocate for any alternative theory. I do very little to compare contextual integrity to other views. The law desperately needs a workable theory of privacy. My only hope is to offer a note of caution to the wave of uncritical adoption of contextual integrity that I observe, mostly among law and computer science scholars.[20] If I can show that contextual integrity would hasten privacy's demise, I will consider my job done. Every other available theory of privacy may, for all I have to say, be worse. But we should hardly invite a weasel into the privacy henhouse simply because it would kill fewer chickens than the proverbial fox. Perhaps all sides need to fundamentally rethink what privacy is and how to protect it.

The article begins (Section 1) by summarizing contextual integrity, the various parameters it considers, and the two-step process it prescribes for assessing privacy claims. It then adopts (Section 2) the perspective of a neutral judge who sincerely tries their hardest to faithfully apply contextual integrity. Legal realist dynamics predict (Section 3) that these uncertainties will, over the long run, allow corporate parties to systematically shrink the zone of protected privacy interests. Proponents of contextual integrity could mitigate some of its most concerning consequences (Section 4), but only by abandoning defining features of the theory.

1. DEFINING CONTEXTUAL INTEGRITY

Contextual integrity's architects sought to remedy shortcomings of earlier privacy frameworks that surfaced as government and corporate surveillance became an increasingly ubiquitous feature of modern society.[21] The initial goal of contextual integrity was to account for the common intuition that, even in public and even after sharing information with trusted third parties, people can still retain nuanced privacy interests. There were two key moves. The first was to shift the focus of the privacy

[20] In the study described above, *supra* note 12, of articles that do more than merely mention contextual integrity, 85 percent adopt the theory with no critical discussion.

[21] Nissenbaum, *supra* note 6, at 137 ("A central tenet of contextual integrity is that there are no arenas of life not governed by norms of information flow, no information or spheres of life for which 'anything goes.'"); Benthall, Gürses, & Nissenbaum, *supra* note 11, at 9 ("[Contextual integrity] addresses gaps in prior entrenched conceptions [of privacy] allowing it to identify privacy threats to which other accounts were blind (e.g., 'privacy in public')."); Chief Judge Alex Kozinski & Mihailis E. Diamantis, *An Eerie Feeling of Déjà Vu: From Soviet Snitches to Angry Birds*, in CAMBRIDGE HANDBOOK OF SURVEILLANCE 420, 420 (David Gray & Stephen E. Henderson eds., 2017) ("[C]orporations meticulously record every transaction we have with them, and many transactions we don't. For a price, it's all transferable to the government—or anyone else willing to pay—with the click of a button.").

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press

inquiry from types of information to flows of information. Flow is "movement or transfer of information from one party to another or others."[22] This shift allowed contextual integrity to "recognize[] a richer, more comprehensive set of relevant parameters":

- the sender of the information
- the recipient
- the subject (i.e., who the information is about)
- the type of information (e.g., the subject's breakfast cereal preference or gender identity), and
- any applicable transmission principles (i.e., social norms governing the transfer of information).[23]

These five parameters characterize every flow of information.

The second key move that contextual integrity's architects made was to abandon binary evaluative metrics—such as public/private or consensual/coerced—in favor of nuanced metrics embedded in the social contexts in which information flows. "Contexts are structured social settings characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes)."[24] Social contexts can be personal (like friendships) or transactional (like visiting a library). They can be intimate (like a marriage) or anonymous (like a chatroom). Each includes norms and expectations (i.e., transmission principles) about how information will flow within and out of a context. For example, in a marriage, reciprocal transparency is often a strong norm (free flow of information within the marriage), as is confidentiality (restricted flow of information out of the marriage). When these transmission principles are violated, contextual integrity tells us privacy may have been infringed.

The new technologies that give rise to most present-day concerns over privacy create novel social contexts that have yet to develop their own idiosyncratic norms. In such cases, contextual integrity prescribes a two-step procedure for evaluating a flow of information. First, one must identify a preexisting social context that is analogous to the novel one under consideration (i.e. one that involves similar actors and types of information).[25] For example, when assessing internet search engines several years ago, contextual integrity scholars compared them to public libraries,

[22] Nissenbaum, *supra* note 6, at 140.

[23] Benthall, Gürses, & Nissenbaum, *supra* note 11, at 9–10 ("Informational norms are well-formed only if they refer to five parameters: sender, recipient, and information subject, information types (topics, attributes), and transmission principle."); Nissenbaum, *supra* note 5, at 33 ("The key parameters of informational norms are actors (subject, sender, recipient), attributes (types of information), and transmission principles (constraints under which information flows).").

[24] NISSENBAUM, *supra* note 2, at 132; Benthall, Gürses, & Nissenbaum, *supra* note 11, at 9 ("[Contexts] refers to social contexts" which "are formally characterized in terms of key elements, which include paradigmatic activities, roles (or capacities), practices, and norms … goals, ends, purposes, and values.").

[25] NISSENBAUM, supra note 2, at 191 ("When new technologies are the enablers of such systems and practices, they may facilitate activities that were previously inconceivable. In such cases, the strategies

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press

which people could also freely access to conduct research.[26] If the flow under consideration respects the transmission principles internal to the analogous preexisting social context, contextual integrity deems it appropriate in the novel context too.[27] If, however, a flow deviates in any way from the transmission principles, contextual integrity deems it suspect.[28]

Once a flow of information is deemed suspect, it moves to the second step of contextual integrity's analysis. While the first step is essentially an exercise in descriptive sociology, the second step incorporates a more prescriptive dimension.[29] It evaluates deemed-suspicious flows of information in light of two sets of values: 1) "general moral and political considerations"[30] and 2) the "ends and purposes" of the social context within which it occurs.[31] If a deemed-suspicious information flow meaningfully advances either set of values, contextual integrity may conclude that it does not infringe privacy after all.[32] For example, a public library that shared a patron's book history with an outside party probably violates relevant transmission principles (subject to very narrow exceptions). It would follow in the first step of a contextual integrity analysis that, by sharing our search history with anyone, Google initiates a suspicious information flow. But contextual integrity might nonetheless greenlight this sharing if Google can persuasively argue that the flow advances our research goals—for example, because (contrary to fact) Google only shares our search history to connect us to relevant experts.

developed to comparatively evaluate new with entrenched practices can also guide an evaluation of new systems and practices.").

[26] Nissenbaum, *supra* note 5, at 43.

[27] Nissenbaum, *supra* note 6, at 138 ("Contextual integrity is maintained when [norms of appropriateness and norms of flow] are upheld, and it is violated when either of the norms is violated."); *id.* at 138 ("Norms of appropriateness dictate what information about persons is appropriate, or fitting, to reveal in a particular context.").

[28] NISSENBAUM, *supra* note 2, at 140 ("Contextual integrity is defined in terms of informational norms: it is preserved when informational norms are respected and violated when informational norms are breached.").

[29] NISSENBAUM, *supra* note 2, at 150 ("[Contextual integrity can] describe[e] and predict[] common reactions but … the framework, expanded to include a normative component, serves well as a prescriptive guide.").

[30] NISSENBAUM, *supra* note 2, at 165; Nissenbaum, *supra* note 6, at 146 ("Resolving these contested cases calls for reliable means of evaluating the relative moral standing of entrenched norms and the novel practices that breach or threaten them.").

[31] Kirsten Martin & Helen Nissenbaum, *Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables*, 18 COLUM. SCI. & TECH. L. REV. 176, 190 (2016); NISSENBAUM, *supra* note 2, at 166 ("The approach I recommend here is to compare entrenched normative practices against novel alternatives or competing practices on the basis of how effective each is in supporting, achieving, or promoting relevant contextual values.").

[32] Helen Nissenbaum, *Respect for Context as a Benchmark for Privacy Online: What It Is and Isn't*, *in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES 278, 289 (Beate Roessler & Dorota Mokrosniska eds., 2015) ("[W]e may not agree that *all* expectations deserve to be met, we can reasonably require a theory of privacy to account for the difference between those that do and those that do not. This is the challenge any normative theory of privacy should address."); Nissenbaum, *supra* note 6, at 146 ("A presumption in favor of status quo does not, however, rule out the possibility of a successful challenge where adequate reasons exist.").

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press

2. A LEGAL REALIST FRAMEWORK

Contextual integrity's adherents offer many persuasive examples of the privacy-protective prescriptions the theory can generate for emerging current technologies. Google Street View should not show individuals' faces.[33] Access to computerized public records should have limits.[34] And Facebook should not use correspondence between friends to serve manipulative ads.[35] These conclusions all accord with widely shared opinions among privacy scholars. Perhaps bolstered by this relative uniformity of opinion, adherents of contextual integrity often apply the theory with an air of finality and predetermination. The strong sense is that "the integrity of the contexts *themselves* [becomes] the arbiter of privacy practices."[36]

Of course, contexts cannot literally arbitrate anything. If contextual integrity were ever incorporated into law, a person would have to apply it.[37] Legal realism is an orientation toward the law that invites analysts to adopt a "predictive stance," focusing on the actual decisions people applying the law would make, rather than on what the "right" answers are.[38] This is where the rubber hits the road for privacy rights. To predict how contextual integrity would affect real people's privacy interests, we should consider whether a legal arbiter applying contextual integrity would reliably reach the same conclusions as contextual integrity's proponents. Even if contextual integrity *can* generate pro-privacy results in important cases, it would be worrisome if the theory had enough wiggle room that it could equally justify privacy-compromising results in the same cases.

This article invites its readers to temporarily assume what, for most of us, will be an unfamiliar posture. Imagine you are a neutral judge deciding "cases or controversies"[39] that pit two antagonistic and very partisan litigants against each other—corporations that collect data and the individuals who claim their privacy has been violated. Your goal is not to favor one side or the other, but simply to reach the best outcome by applying a law that incorporates the framework of contextual integrity.

Your judicial task is not an easy one. The technology is complex. The information flows are vast. And the social contexts are nuanced. But if, as the adherents of contextual integrity claim, the framework "provides rigorous, substantive" guidance,[40] a "shorter and more systematic path,"[41] perhaps you can still be confident that, with enough effort, your answer will be the right answer.[42]

---

[33] NISSENBAUM, *supra* note 2, at 217.

[34] Kirsten Martin & Helen Nissenbaum, *Privacy Interests in Public Records: An Empirical Investigation*, 31 HARV. J. L. & TECH. 111, 112 (2017).

[35] NISSENBAUM, *supra* note 2, at 222.

[36] Nissenbaum, *supra* note 32, at 297.

[37] Rule, *supra* note 16, at 20 ("It is very difficult—impossible, I would argue—to extract a form of analysis from Nissenbaum's statements that would lead all reasonable observers, regardless of their political world-views and their personal histories, to similar conclusions in any given case.").

[38] *See generally* OLIVER WENDELL HOLMES, JR., THE COMMON LAW (1881).

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

[40] NISSENBAUM, *supra* note 2, at 2.

[41] Nissenbaum, *supra* note 5, at 37.

[42] NISSENBAUM, *supra* note 2, at 2.

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press

3. CONTEXTUAL INTEGRITY WOULD ERODE PRIVACY

In the short term, a legal rule of contextual integrity may, as its proponents predict, favor David-the-consumer over Goliath-the-data-hungry-corporation. The framework has resources that, in today's world, in the hands of a well-meaning judge, could justify restrictions on some egregious forms of data collection. But over the long term, contextual integrity favors Goliath over David. In the adversarial courtroom where privacy rights are ultimately decided, contextual integrity's complexity and presuppositions favor whichever party is better resourced, more coordinated, and more persistent. The Davids of the world are individual consumers with disparate priorities and little more than their indignation or fear to fuel them. The Goliaths advance an unrelentingly united front backed by legal know-how, technological know-that, and billions of dollars from a data economy that they control. Contextual integrity makes matters worse because its defining sociality lends a permanence to Goliath's victories that it withholds from David's. Consumers' courtroom wins last only until corporations regroup and reissue the same data practice in a modified form. When Goliath wins, things are different. Data abuses that survive court challenge (whether rightly or not) can eventually become ingrained, merging into an ever-evolving social backdrop. Once they do, contextual integrity has few tools to argue for unwinding the court's precedent.

The remainder of this section applies a legal realist framework to predict how privacy would fare in courtrooms populated by neutral judges applying contextual integrity as a rule of decision. It anticipates privacy's demise. The next several subsections each uncover a privacy-undermining courtroom dynamic that contextual integrity either enables or necessitates.

3.1. What If the Decisionmakers Aren't Neutral?

As a quick aside, it bears noting that the present exercise stacks the legal realist deck in favor of contextual integrity by focusing on how neutral judges would decide cases. Many other parties, like legislators and regulators, also make decisions that affect individual privacy rights, but judges are a natural place to focus since the law's effects will ultimately turn on judicial interpretations of it. Judges also are more politically insulated, and, hence, less vulnerable to industry capture.

However, a *true* realist would assume that even judges will generally favor corporate interests.[43] Familiar power dynamics select for and cultivate judges with pro-business dispositions.[44] To the extent that there is more wiggle room in contextual integrity's framework than in alternatives, it would provide pro-corporate

[43] *See, e.g.,* Michael S. Kang & Joanna M. Shepherd, *The Partisan Price of Justice: An Empirical Analysis of Campaign Contributions and Judicial Decisions*, 86 N.Y.U. L. REV. 69, 85 (2011); David A. Logan, *Juries, Judges, and the Politics of Tort Reform*, 83 U. CIN. L. REV. 903, 919 (2015); John D. Echeverria, *Changing the Rules by Changing the Players: The Environmental Issue in State Judicial Elections*, 9 N.Y.U. ENVTL L.J. 217, 332-33 (2001).

[44] Herbert Hovenkamp, *Coase, Institutionalism, and the Origins of Law and Economics*, 86 IND. L.J. 499, 527 (2011) ("[Legal realists] tended to view business corporations as institutions that wielded great power.").

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press

judges with cover to enact pro-corporate policies.[45] This would exacerbate all the privacy-undermining dynamics described in the sections that follow.[46]

3.2. Errors Due to Value Indeterminacy

Contrary to the legal realist paradigm, this article assumes away any influence pro-corporate interests have on the judicial selection process. For purposes of the present exercise, our hypothetical judges applying contextual integrity are officially neutral between data-hungry corporate defendants and privacy-protective individual plaintiffs. But neutral judges are still human judges, and all humans have a rich array of conscious and unconscious biases, preferences, and priorities. The more determinate and concrete a decision process is, the more likely it is to filter out these distortions.

As I am far from the first to observe, contextual integrity is plagued by value indeterminacy.[47] Recall that the theory's final step for assessing a purported violation asks judges to "evaluate [information] flows against norms based on general ethical and political principles."[48] These general principles include an open-ended list of "moral, political, and social values,"[49] including "prevention of information-based harms," "informational inequality," "autonomy," "freedom," "preservation of important human relationships," "democracy, "freedom of speech," "pursuit of wealth," "efficiency," "security," and "other social values."[50] Proponents of contextual integrity hope that this impressive list of considerations will "allow for greater specificity—hence less ambiguity—in prescribing and prohibiting certain flows."[51]

But put yourself in a neutral judge's shoes, tasked with deciding whether some flow of information is legitimate in some novel social context. You genuinely want to get the right answer. Is the task made any more concrete by introducing the interests of freedom, wealth, democracy, efficiency, and "other social values"? One might worry that such an open-ended values inquiry confuses privacy with other important interests.[52] If one thing is certain, though, it is that these values themselves

[45] *See also* Echeverria, *supra* note 43, at 300.

[46] As Alexandra Prégent observes, such indeterminacy would "allow[] an ill-intentioned person to *manipulate* the evaluation." *Supra* note 16, at 9.

[47] To borrow terminology from discussions of legal realism, I am arguing that the "indeterminacy thesis" would be true of any law premised on contextual integrity. *See generally* Lawrence B. Solum, *On the Indeterminacy Crisis: Critiquing Critical Dogma*, 54 U. CHI. L. REV. 462 (1987). Ryan Calo has applied legal realist methods to privacy law generally and concluded that it satisfies the indeterminacy thesis. Ryan Calo, *Privacy Law's Indeterminacy*, 20 THEORETICAL INQUIRIES L. 33, 40 (2019). When developing a theory from scratch, one hopes to avoid the pathologies of current doctrine. This section and the next argue that, at least so far as indeterminacy is concerned, contextual integrity would make matters worse.

[48] Nissenbaum, *supra* note 5, at 38.

[49] Nissenbaum, *supra* note 6, at 123.

[50] *Id.* at 146–47; *see* Nissenbaum, *supra* note 32, at 289; NISSENBAUM, *supra* note 2, at 165.

[51] Benthall, Gürses, & Nissenbaum, *supra* note 11, at 3.

[52] Lisa Austin, *Privacy and the Question of Technology*, 22 L. & PHIL. 119, 133 (2003) ("There are many other examples of norms regarding the uses and misuses of information that are more precisely described in terms of concepts such as harassment, defamation, and negligent misstatement. … [A] focus on contextual norms in general may leave us unable to make these specific distinctions.").

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press

do not have settled meanings.[53] Does freedom refer to positive or negative freedom? Is wealth measured in dollars or love? Is democracy best respected by the expressed will of the people or by their hypothetical will? Are there any distributional constraints on efficiency? A deliberative process can be no more determinate than the considerations that go into it.[54]

Even if a neutral judge could confidently identify and define all implicated values, there is still the problem of how to sum them into a binary decision—that the information flow is legitimate or it is not. Contextual integrity offers no hierarchy of social and political values. It does not even say whether context relative goals matter more or less than other general social values. For a conscientious judge hoping to find the right answer, open-ended, multi-factor balancing tests like these are paralyzingly imprecise.[55]

Of course, judges will always encounter value indeterminacies, even if they were applying a different theory of privacy.[56] But indeterminacy comes in degrees; the greater the degree of indeterminacy, the more dangerous the legal dynamics discussed throughout this section become.[57] As a purely mathematical matter, contextual integrity must be less determinate than more focused alternatives simply because it requires judges to balance a greater number of essentially contested values. Notions like "consensual" and "public" on which competitor theories rely are ambiguous enough on their own. Adding notions like "democracy," "dignity," and "wealth" to the mix exponentially increases the number of open questions.

It may not be an exaggeration to say that under contextual integrity, there are no clear-cut violations. According to consent-based theories of privacy, if a firm never discloses a data practice to consumers, that is a clear-cut violation. According to publicity-based theories of privacy, an unwarranted search of a person's pillow-side diary is a clear-cut violation.[58] But, according to contextual integrity,

[53] Rule, *supra* note 16, at 268 ("Terms like justice, fairness, equality, social hierarchy, democracy and so on … are textbook cases of essentially contested concepts." [quotation marks and citations omitted]).

[54] NISSENBAUM, *supra* note 2, at 10 ("[A]ppeals to universal human values and moral and political principles take place in the stratospheres of abstraction.").

[55] A.L.A. Schechter Poultry Corp. v. United States, 295 U.S. 495, 541–42 (1935) (describing a law that instructed the president to balance just three factors as giving him "discretion [that] is virtually unfettered"). For this reason, it may perhaps be unsurprising that, in a survey of computer science papers adopting contextual integrity, "*[n]one* … used the normative aspect of contextual integrity as a basis for their technical contributions." Benthall, Gürses, & Nissenbaum, *supra* note 11, at 57.

[56] Interestingly, proponents of contextual integrity seem to be at pains to give the impression that their view is *more* determinate than competitors. Xiaowei Yu, *The Identifiability Problem in Transnational Privacy Regulation*, 56 VAND. J. TRANSNAT'L L. 1303, 1348–49 (2023) ("The formula [Nissenbaum] offers gives the impression that norms may be identified mathematically. It is very appealing, especially to computer scientists and technicians."); Rule, *supra* note 16, at 267 ("Implied here is a model of normative culture resembling a very complex and well-debugged computer program—with sub-routines governing every aspect of social life.").

[57] Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 1025–26 (2003).

[58] Kirsten Martin, *Manipulation, Privacy, and Choice*, 23 N.C. J.L. & TECH. 452, 494 (2022) ("[P]rivacy-as-concealment is easy to identify and model.").

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press

judges must first consider how efficiency, security, and every other implicated social/moral/political value bear on deemed-suspicious information flows before reaching a final conclusion.[59] Perhaps efficiency favors nondisclosure of some corporate data practices, and security favors public access to secret diaries. For every flow of information, there will be values it promotes and values it hinders. Judges applying contextual integrity would be routinely forced to select between two conflicting results, both of which have colorable defenses. Even if, on balance, one result is usually more justifiable than the other, few if any cases will be easy.

It bears noting that many of contextual integrity's proponents in computer science and law stop at the view's first step (i.e., identifying the social context and surfacing its norms of transmission).[60] In the second step, these proponents often populate the otherwise open-ended normative inquiry with a more limited range of norms important to them or their discipline.[61] This approach may eliminate, or at least significantly circumscribe, the value indeterminacy that a judge applying contextual integrity would face. However, as discussed in the remainder of this section, indeterminacies arise in contextual integrity's first step, too, and these could prove even more troublesome for a neutral judge.

3.3. Errors Due to Context Indeterminacy

Contextual integrity invites a second type of indeterminacy that penetrates more deeply to its conceptual core—indeterminacy of social context.[62] Recall that the first step for a neutral judge applying contextual integrity is to characterize the social context the parties inhabit. For this, the court must consider "who is gathering the information, who is analyzing it, who is disseminating it and to whom, the nature of the information, the relationships among the various parties, and even larger institutional and social circumstances."[63] This social context fixes the transmission norms in light of which the judge should start evaluating the contested flow of information. Contextual integrity also instructs judges to identify "context-specific purposes and values"[64] that arise from "the objectives around which [the] context is

[59] Ryan Calo has observed that outcomes in privacy cases under current law are unpredictable because "privacy is *nearly always* balanced or defined against an important competing value such as free speech or physical security." Calo, *supra* note 47, at 42. Contextual integrity makes matters worse because, according to it, "competing values" are not just external considerations; they are baked directly into privacy itself.

[60] Benthall, Gürses, & Nissenbaum, *supra* note 11 (noting that computer science scholars usually overlook contextual integrity's evaluative dimension).

[61] *See, e.g.*, Bradley, *supra* note 5 (applying contextual integrity to identify social contexts in bankruptcy disputes for evaluation using more traditional bankruptcy values); Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 615 (2011) (characterizing social media as a technosocial extension of the home/office and then discussing implications for existing Fourth Amendment search norms).

[62] Alexandra Prégent makes related observations in work published while this article was under review. *See supra* note 16, at 9–10.

[63] Nissenbaum, *supra* note 6, at 154–55.

[64] Nissenbaum, *supra* note 5, at 37; Nissenbaum, *supra* note 32, at 290 ("The third layer introduces a further set of considerations, namely, context-specific values, ends, and purposes.").

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press

oriented."[65] Envisioning how contextual integrity would play out in an adversarial courtroom forces us to reckon with the ambiguities and ambivalences inherent to understanding social context.

Proponents of contextual integrity normally take social contexts as given, singularly characterizable in the way they offer. In their view, netizens on Google are researchers,[66] "friends" on Facebook are friends as classically understood,[67] and Web-based financial institutions are banks.[68] These social context characterizations uniformly favor the vantage of individuals whose personal data is at stake.[69] But contextual integrity has no internal resources to dictate this sort of pro-consumer bias. Social contexts are necessarily co-constructed by the interactions, expectations, and purposes of all sides to an exchange. That is what makes them *social.* If anything, the theory itself demands impartiality because neither side gets to be the "sole arbiter" of social context.[70] A neutral judge would strive to bear in mind the perspectives of all parties to the conflict.[71]

---

[65] NISSENBAUM, *supra* note 2, at 134.

[66] Nissenbaum, *supra* note 5, at 43 ("Consulting a search engine, in this regard, is akin to conducting research, seeking information and association, searching a library catalog, and pursuing intellectual enlightenment."); NISSENBAUM, *supra* note 2, at 195 ("Perusal of library catalogs and reference books as well as library borrowing records serve as a plausible if not complete comparison point for a Web search, since the Web has emerged as a preeminent public repository of knowledge and information.").

[67] NISSENBAUM, *supra* note 2, at 223 ("I reject the idea that social networking sites define a newly emergent, sui generis social context with its own internal rules."); *id.* at 228 ("Bonds of trust, crucial to the myriad other duties and obligations of kinship and friendship, are one of many values supported by norms of information flow.").

[68] Nissenbaum, *supra* note 5, at 39 ("Whether you transact with your bank online, on the phone, or person-to-person in a branch office, it is not unreasonable to expect that rules governing information will not vary according to medium.").

[69] Benthall, Gürses, & Nissenbaum, *supra* note 11, at 4 (finding that computer scientists applying contextual integrity "often position users as central actors, highlighting their role and agency in engaging and transforming informational norms in a context and throughout time."); Kirsten Martin, *Understanding Privacy Online: Development of a Social Contract Approach to Privacy*, 137 J. BUS. ETHICS 551 (2015) (referencing the information norms expected by "consumers, users, and employees" fifteen times, but never the expectations of counterparties); *id.* at 562–63 ("[R]esearchers and organizations should ask *what are the privacy expectations of the users, customers, or employees in this situation?* rather than *do users, customers, or employees have any reasonable expectations of privacy here?*"); Martin & Nissenbaum, *supra* note 31, at 214 ("The finding suggests that the commercial use of information is considered inappropriate [by consumers] even when the information has been willingly disclosed."); Martin & Nissenbaum, *supra* note 34, at 113 ("[T]he respondents' [users'] judgments in our studies were highly sensitive to other contextual parameters.").

[70] Nissenbaum, *supra* note 32, at 293; *see also* Martin & Nissenbaum, *supra* note 34, at 117 ("[P]opular opinion is but one determinant of legitimate privacy expectations."). The close counterpart of contextual integrity, privacy as social contract, makes abundantly clear the importance of perspectives on both sides of an information flow. Martin, *supra* note 69, at 557 ("The social contract approach used here is a multilevel, contextually rich framework allowing for specific contractors within a contracting community the moral free space to develop authentic and legitimate privacy norms and expectations."). Social contract theory looks to resolve disputes by finding a "mutually beneficial and sustainable solution" for businesses and consumers. *Id.* at 553.

[71] There is an "antagonistic relationship between the owners and consumers of intellectual content stored in digital form." NISSENBAUM, *supra* note 2, at 109.

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press

Characterizing social context quickly becomes murky when there are conflicting perspectives among participants. This sort of conflict is exactly what we should expect a neutral judge to face in an adversarial courtroom. For example, Google is unlikely to accept the pro-consumer characterization according to which it is a public library and users of its search engine are researchers.[72] Rather, Google will probably say that its users are more like consumers (of its services) or products (for its advertisers).[73] The social context only becomes more intractable once we realize that Google and people running searches on its site are not the only participants. Content generators obviously interact with every Google search and display content on results pages. So do advertisers. Very likely, all four parties would characterize the social context differently. The worry is that all four perspectives are, in a sense, accurate but also irreconcilable. While other theories of privacy invite some differences of opinion—for example, on whether some data collection was consensual or some interaction occurred in public—the range of available perspectives is considerably narrower.

It might help if there were some external vantage point, an objective view from nowhere,[74] that could help judges decide between competing characterizations of social context. Indeed, proponents of contextual integrity suggest that the "work of reputable philosophers, social scientists, and social theorists" could offer something along those lines.[75] While drawing these disciplines into the inquiry would undoubtedly add nuance and flexibility, the worry is that they would also "compound[] indeterminacy."[76] The views of philosophers working "in the analytic tradition, Raimo Tuemelo, John Searle, Margaret Gilbert, and Seumas Miller,"[77] whom contextual integrity's proponents approvingly cite, conflict with each other and with the many other respected social ontologists not referenced by name.[78] Incorporating the complexities and internal debates of other disciplines would only further undermine the confidence that contextual integrity could give concrete guidance to neutral judges.

[72] NISSENBAUM, *supra* note 2, at 133 ("By [roles] I mean typical or paradigmatic capacities in which people act in contexts."). Don't take my word for it. Just ask Google! Google's AI Overview for the query "is google a public library" begins: "No, Google is not a public library." (on file with author).

[73] These themes emerge from Google's Terms of Service, which are linked on every Google page. Google, *Privacy and Terms*, https://policies.google.com/terms?hl=en&fg=1 (last visited June 10, 2025) (on file with author); Google, *How Our Business Works*, https://about.google/company-info/how-our-business-works/ (last visited June 10, 2025) (on file with author) ("We make money selling ad space to businesses—big and small, global and local—in two key ways. First, businesses can reach potential customers by showing ads on a range of Google products such as Search, Maps, and YouTube. Second, businesses can buy ad space that we show on sites and apps that partner with us, like news publications and blogs.").

[74] *See* THOMAS NAGEL, THE VIEW FROM NOWHERE (1986).

[75] Nissenbaum, *supra* note 6, at 137. Proponents of contextual integrity also suggest it may be helpful to incorporate the "insights of novels, movies, and poems." NISSENBAUM, *supra* note 2, at 240.

[76] Calo, *supra* note 47, at 34 ("[T]he application of social science to doctrine, if anything, compounds indeterminacy.").

[77] NISSENBAUM, *supra* note 2, at 131.

[78] Sociologist James B. Rule makes a similar point with respect to the social scientists that proponents of contextual integrity cite. Rule, *supra* note 16, at 268 ("But [the cited approach] is just one strain of social theory, far from the ascendant in western social science today.").

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press

3.4. Indeterminacy and Complexity Favor the Powerful Litigants

All else equal, ambiguous standards tend to favor sophisticated parties.[79] Clear-cut rules give less role for creative (i.e., expensive) advocacy. In the uncertain space where framing, fact development, and careful selection of values matter, litigants with better lawyers will tend to win. This dynamic predictably favors parties with more resources to craft narrative and identify loopholes. In the battle over privacy, these parties will invariably be the corporate proponents of free-flowing data.

Even if the previous two sections overstated contextual integrity's inherent indeterminacies, the framework would still favor corporate parties. Suppose that contextual integrity could—were it fully fleshed out, were all the facts known, and were all the relevant values fully understood—be rendered more determinate. It would still involve a massively "complex, delicate web of constraints"[80] implicating "a far more *complex* domain of social factors (fields, domains, contexts) than the one that typically grounds privacy theories."[81] Applying contextual integrity is "a messy task,"[82] like trying to "juggl[e] balls in the air, moving in sync."[83] Defenders of contextual integrity tout this complexity as a virtue that allows the theory to generate sensible results in a broad range of cases.[84] But, as with indeterminacy, complexity favors litigants who have the resources to pay for attorneys who can navigate it.[85] As proponents of contextual integrity acknowledge, "only a handful of deep experts would be able to piece together a full account" of some important information flows.[86] The economic reality is that most of these experts will work for the highest bidder.

Corporate litigants have other advantages when faced with indeterminacy and complexity that even well-funded individual plaintiffs do not. First, as a group, they have relatively well-defined, uniform, and aggressive positions about how they may collect and use personal data. In courtrooms across the country, they can present a consistent and coordinated attack on privacy that unorganized individuals with disparate interests cannot hope to muster. Second, firms have an outsized role in defining new social contexts even prior to litigation. As the architects of platforms and apps, they have much more power than individual consumers to set the terms of

[79] *See generally* Daniel T. Ostas, *Corporate Counsel, Legal Loopholes, and the Ethics of Interpretation*, 18 TEX. WESLEYAN L. REV. 703 (2012) (discussing corporate counsel's use vague law to identify and exploit legal loopholes); see also Michael Haber, *How the 1 Percent Pays Taxes, How the 99 Percent Could: The Subchapter T Worker Cooperative Tax Loophole*, 26 J.L. & POL'Y 267, 273–74 (2018) ("Tax loopholes are a highly divisive topic as they often benefit affluent taxpayers and large corporations, even when they were intended to benefit small businesses and less-affluent taxpayers at the time they were enacted.").

[80] NISSENBAUM, *supra* note 2, at 128; Nissenbaum, *supra* note 6, at 124.

[81] Nissenbaum, *supra* note 6, at 124.

[82] Nissenbaum, *supra* note 6, at 156.

[83] NISSENBAUM, *supra* note 2, at 145.

[84] NISSENBAUM, *supra* note 2, at 159 ("Because it invokes several parameters simultaneously … it avoids the impossible mire into which [any simpler theory] frequently leads when applied to the messy and contingent realms of privacy.").

[85] Russell Engler, *And Justice for All-Including the Unrepresented Poor: Revisiting the Roles of the Judges, Mediators, and Clerks*, 67 FORDHAM L. REV. 1987, 2045 (1999).

[86] Nissenbaum, *supra* note 5, at 35.

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press

exchange (and influence how outside parties will later perceive them). Finally, although privacy policies don't play the central role in contextual integrity that they do for consent-based models of privacy, these corporate documents still exist, and most users still click "I agree."[87] Neutral judges faced with a novel and multiply characterizable social context will understandably delve into whatever textual evidence is available to them. Privacy policies will often be the closest point of contact and only record of possible expectations shared by information senders and recipients. While critics of consent-based theories often worry that privacy policies are a way for corporations to legally launder abusive data practices,[88] contextual integrity raises similar concerns.

3.5. Heads Google Wins, Tails You Lose

To see how sophisticated corporate parties could weaponize contextual integrity to their advantage in the courtroom, consider once again an example that looms large in the literature: Google search. As noted above, proponents of contextual integrity have argued that when people use Google, they are in a social context that resembles researchers visiting a public library.[89] Under the transmission norms of that latter context, patrons' search/reading history is confidential. It follows under contextual integrity that Google presumptively violates privacy when it shares search history with third parties. That is the result that proponents of contextual integrity favor. That is where their analysis ends.

But public libraries are governed by a far richer set of informational norms. Coincidentally, I recently took my son to get a library card, a necessary first step to accessing our local library's services. As part of the registration process, I had to hand over my driver's license.[90] If I gave the clerk a false ID, I would have committed a felony.[91] In the terminology of contextual integrity, before research information flows from libraries to patrons (i.e. they check out books), transmission norms require identification information to flow from patrons to libraries. Patrons who acquire library books without providing truthful information about themselves violate contextual integrity.

Consider the implications of this contextual analysis for Google search.[92] If Google is like a public library, then it would be well within its rights to require each of us to provide verifiable personal identification information—photo, date of birth, ID number, home address, weight, height, eye color (all the information that is on a

[87] Martin, *supra* note 69, at 553 ("Individuals, employees, users, and consumers make judgments about privacy expectations and violations regardless of the notice and choice policy in many situations.").

[88] *See* Ari Ezra Waldman, *Privacy's Rights Trap*, 117 NW. U. L. REV. ONLINE 88, 90–91 (2022) ("Individual rights of control require an infrastructure to make them meaningful, and that infrastructure does not exist in the law of informational capitalism.")

[89] Nissenbaum, *supra* note 5, at 40–43.

[90] Iowa City Public Library, *Library Cards: Getting a Card*, https://www.icpl.org/about/cards (last visited Sept. 8, 2025) (on file with author).

[91] Iowa Code § 718.5 Falsifying Public Documents ("A person who … makes or alters any public document, or any instrument which purports to be a public document … commits a class 'D' felony.")

[92] Nissenbaum, *supra* note 5, at 41 ("Just as with the off-line environment, we would expect the same standards to prevail online.").

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press

driver's license)—before we run a search. Indeed, if Google *really* is like a public library, then the company may even have an argument under contextual integrity that any of us who use its services without truthfully identifying ourselves violate *its* privacy. Surely that is a result every friend of privacy wants to avoid.

The general point is this. A theory that grounds itself in the nuances of complex social contexts opens a lot of space for unintended consequences. Under an open-ended and heavily layered approach like contextual integrity, results that may initially seem like victories for individual privacy can quickly turn to losses once teams of high-paid corporate attorneys apply their legal judo.

3.6. A Frog in Hot Water

The analysis so far has focused on isolated judges making decisions in single cases. If contextual integrity were adopted as a general rule of decision, it would play out in many cases over many years. Over the long run, contextual integrity provides corporations with a reliable strategy to continuously chip away at privacy protections.

Contextual integrity recognizes that social contexts are "evolving structures and the activities, actors, norms, values, and attributes comprising them evolve simultaneously."[93] When a change to information flow is abrupt, we notice, resist, and jump to action to oppose injustice.[94] In these situations, contextual integrity offers its most robust privacy protections. But change does not have to be abrupt. "Practices [may also] shift almost imperceptibly [and], over time … bring about shifts in conventional expectations."[95] If change happens gradually and norms shift against privacy, contextual integrity offers no recourse. Without a noticeable departure between actual data flows and expected contextual information norms, no plaintiff will surface to register a problem. And once the norms have shifted, contextual integrity cements them as the new benchmark for privacy.

Corporations can leverage this aspect of contextual integrity into a winning legal strategy.[96] By incrementally shifting from presently acceptable data practices toward presently unacceptable practices that firms prefer, firms can assure themselves of contextual integrity's endorsement at every step.[97] Proponents of

[93] NISSENBAUM, *supra* note 2, at 145; *see* Austin, *supra* note 52, at 132 ("[S]ocial conventions can change and we could become used to the various forms of public surveillance.").

[94] Nissenbaum, *supra* note 6, at 145 ("[W]e resist, suspicious that [the change] occasion[s] injustice or even tyranny."); Nissenbaum, *supra* note 5, at 33 ("[W]hen the flow of information adheres to entrenched norms, all is well; violations of these norms, however, often result in protest and complaint.").

[95] Nissenbaum, *supra* note 6, at 144.

[96] Oskar J. Gstrein & Anne Beaulieu, *How to Protect Privacy in a Datafied Society? A Presentation of Multiple Legal and Conceptual Approaches*, 35 PHIL. & TECH. 3, 27 (2022) ("[A]n uncritical adoption of [contextual integrity] might allow such powerful actors to promote one-size-fits-all solutions that lower existing protection standards in some areas of the world."); Ibo van de Poel, *Socially Disruptive Technologies, Contextual Integrity, and Conservatism About Moral Change*, 35 PHIL. & TECH. 82, 3 (2022) ("[W]hat about cases in which technology reinforces existing power imbalances and injustices without violating entrenched norms? It would seem that such cases remain under the radar in [contextual integrity].").

[97] Benthall, Gürses, & Nissenbaum, *supra* note 11, at 47 ("[Contextual integrity] theorizes that norms are the result of a process of social adaptation."); SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM:

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press

contextual integrity are aware of this problem,[98] but have yet to provide a response.[99] They hope that "the robustness of the social structure of contexts and the efficacy of their respective informational norms will stop the slide down the slope and prevent a society from throwing away privacy in tiny bits."[100] But "[e]ven entrenched norms can change over time."[101] If firms implement changes to data flow patiently, gradually, and imperceptibly, contextual integrity will not stand in their way. Worse, contextual integrity would give a legal stamp of approval to the new normal they create. Some other privacy frameworks offer fixed standards, like whether data collection was consensual, that are less vulnerable to shifting social sentiment. As argued above, these alternative frameworks can identify at least some clear-cut violations for rooting their privacy jurisprudence. The nuances, complexities, and indeterminacies of contextual integrity leave it particularly vulnerable to corporate efforts at social engineering.

3.7. A One-Way Ratchet

Even judges doing their best to implement contextual integrity in an unbiased way will sometimes make errors. Errors that disfavor privacy will tend toward permanence under contextual integrity while, errors that favor privacy will not. Consider a series of norms for information flow, ranging from very restrictive to very permissive. Suppose the norm that reflects the status quo in a social context is somewhere in the middle. This is the norm that contextual integrity will tend to favor.

Suppose now that a firm has implemented a data flow that is more permissive than the status quo norm would ordinarily sanction. Some adversely affected individual brings suit.[102] There are two ways that a judge applying contextual integrity in the scenario could get things wrong:

1. The judge may prohibit the data flow, even though a correct application of contextual integrity would find that the information flow is legitimate (despite being more permissive than the status quo).
2. Or the judge may permit the data flow, even though a correct application of contextual integrity would determine that the information flow is illegitimate.

THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 15 (2019) ("This conflict produces a psychic numbing that inures us to the realities of being tracked, parsed, mined, and modified."); McDonald & Forte, *supra* note 17, at 3 ("[P]ower can be used to normalize privacy violations.").

[98] NISSENBAUM, *supra* note 2, at 161.

[99] *Id.* at 160 ("[T]he framework of contextual integrity appears to provide no buffer against insidious shifts in practice that ultimately gain acceptance as 'normal.'").

[100] *Id.* at 243.

[101] Nissenbaum, *supra* note 6, at 144; NISSENBAUM, *supra* note 2, at 15 ("[H]istorical … variation … is directly predicted by the model."); NISSENBAUM, *supra* note 2, at 3 ("[I]nformational norms evolve over time.").

[102] Legally, this scenario is a bit farfetched since most privacy statutes do not provide a private right of action. *See* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 944 (2009) ("In an absence of private rights of action, however, there is likely to be significant underenforcement of privacy interests."). Adding this true-to-life detail would only serve to further amplify the systematic pro-corporate bias I am about to describe.

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press

In the first scenario, the privacy status quo would be protected, but only temporarily. The same firm, or a similarly situated firm, could try again, perhaps with some slight variation to the flow parameters.[103] The burden would be on some future individual litigant to bring a new case, hoping the next judge will make the same mistake as the first.

In the second scenario, the scope of privacy protections would have shrunk with little chance of reversal. As victims, individuals are differently situated from offender firms. They cannot as easily force relitigation of the same issue since, unlike firms, they cannot tweak the nature of the violation in ways that demand a new hearing. Furthermore, once data flows receive legal sanction, social norms will slowly adapt to anticipate them.[104] Unlike other theories that offer a fixed normative baseline to which judges can always return, contextual integrity provides no pathway for rewinding information norms back to their earlier state.

3.8. Persistent Particularism[105]

Proponents of contextual approaches could argue that the above concerns just represent hypothetical growing pains of the sort that any new law would face. Perhaps, through repeated application in courts, a robust jurisprudence would eventually supplement the framework.[106] Precedential guidance might make a law premised on contextual integrity more predictable, thereby halting the parade of horribles described above.

Unfortunately, contextual integrity is quite clear that, unlike decisions in law interpreting whether someone consented to a privacy policy[107] or whether some exchange occurred in public, decisions about flows of information in one social context will have little precedential value for other social contexts. Judges applying contextual integrity would have to approach each context anew, rendering decisions "on a case-by-case basis."[108] This is because social contexts are highly variable,[109] and so are the privacy norms embedded in them.[110] Because

[103] RICHARDS, *supra* note 10, at 83–85 (describing how Facebook uses A/B testing to constantly tweak data use practices).

[104] Solove, *supra* note 57, at 1026 ("[T]he law does not simply reflect social values; it also shapes them, and over time it can help build some degree of social consensus.").

[105] Particularism is a familiar view in moral philosophy with recognized shortcomings. Jonathan Dancy, *Moral Particularism*, THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Edward N. Zalta ed., 2017), https://plato.stanford.edu/archives/win2017/entries/moral-particularism/.

[106] Solove, *supra* note 57, at 1027 ("[T]here are benefits to allowing judges and juries to decide cases in a contextual manner. Through precedent, which serves to limit the degree of variation and inconsistency in cases, judicial involvement enables the growth and development of standards for weighing conflicting and contested values.").

[107] Admittedly, there are different interpretations of judicial precedent on privacy policies. *See generally* Gregory Klass, *Empiricism and Privacy Policies in the Restatement of Consumer Contract Law*, 36 YALE J. ON REGUL. 45 (2019).

[108] NISSENBAUM, *supra* note 2, at 165; *id.* at 239 ("I can think of no other way to deal with [conflicts between or among contexts] except case-by-case.").

[109] Nissenbaum, *supra* note 5, at 39 ("[Social contexts] include combinations and permutations (mash-ups) constrained only by human creativity and the technological limits of the moment.").

[110] Martin, *supra* note 69, at 554 ("The rules used to develop privacy norms vary across [all these] contexts.").

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press

"contextual integrity … recognizes an indefinite array of possibilities,"[111] it "does not [even] support substantive prescriptions for general families of technologies … [T]he most fruitful assessments take place *within particular contexts*."[112]

Some proponents of contextual integrity have implied that the theory would not even support general substantive prescriptions across individuals within the same context. Empirical studies demonstrate "significant relationships between individual factors and contextual privacy expectations."[113] These individual factors include people's idiosyncratic histories and policy preferences,[114] as well as demographic characteristics like age and gender.[115] This has led some researchers to recommend "tak[ing] into account both contextual variables and individual-level attitudes, concerns, and beliefs."[116] If that is right, not only would judicial decisions applying contextual integrity in one context have little precedential value for another context, the decisions may not even carry weight between different individuals in the same context.

4. CONCLUSION

They say it takes a theory to beat a theory.[117] While I have argued that a legal doctrine framed around contextual integrity would ultimately undermine privacy protections, I have not argued that any alternative theory would do a better job overall. Indeed, contextual integrity's leading competitors already hold sway in the law, and their privacy-diminishing impact is playing out before our eyes. For all I have said, contextual integrity may still be the best theory available. Even if it would eventually undermine individual privacy when applied by real world judges, it may do so more slowly than rival theories of privacy.

There are possible refinements to contextual integrity that might mitigate some of its dangers. First, in characterizing social contexts and their purposes, contextual integrity might commit to prioritizing the perspective of one of the three involved parties: data subject, sender, or recipient. Contextual integrity's advocates seem most concerned for consumers, who tend to be subjects and/or senders, so focusing

[111] NISSENBAUM, *supra* note 2, at 143.

[112] *Id.*, at 200 (emphasis added); *id.*, at 137 ("There may be no general solutions to these general types of conflicts and it may be that some are simply intractable.").

[113] Kirsten Martin & Katie Shilton, *Why Experience Matters to Privacy: How Context-Based Experience Moderates Consumer Privacy Expectations for Mobile Applications*, 67 J. ASSOC. INF. SCI. & TECH. 1871, 1872 (2016); *see also* NISSENBAUM, *supra* note 2, at 119 ("[E]xpectations of privacy remain complex and contested at present."); McDonald & Forte, *supra* note 17, at 10 ("[Contextual integrity] tend[s] to overlook especially the fact that vulnerable individuals do not have a voice in what is agreed upon to be appropriate levels of privacy.").

[114] Martin & Shilton, *supra* note 112, at 1872.

[115] Martin & Nissenbaum, *supra* note 34, at 117 ("Younger respondents (under 35 years old) were more critical of seeking access to data from data brokers and online government records than of seeking access by asking data subjects directly (the null condition). Women were more opposed than men to the use of marital status in job applications.").

[116] Martin & Shilton, *supra* note 112, at 1880.

[117] I hope to offer my own soon enough!

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press

on their point of view (e.g., that Facebook is a platform for friends to meet) would center their interests. This would not totally resolve indeterminacies in characterizing social contexts, since people visit Facebook for a range of reasons. Some visitors want to meet friends, but many want to buy/sell goods or organize for social/political causes.[118] Despite this natural variation in motive, favoring one of the three participants within contextual integrity's framework would narrow the range of characterizations social contexts will bear.

A second refinement would be to pick which values to prioritize in contextual integrity's evaluative step.[119] "General moral and political considerations"[120] encompass *a lot.* A willful, confused, or uncertain judge could reach any conclusion in any case just by choosing the values they bring to bear. It would help if contextual integrity's advocates could circumscribe the values that matter, or at least come up with some hierarchy of values. They might say, for example, that individual dignity matters most, except when the stakes for efficiency or security are very high. As with the first refinement, this would still leave huge indeterminacies (what does dignity mean?; when does an efficiency become significant?), but it would narrow the range of possibilities that a conscientious judge must countenance (because maybe other important values like equality and democracy are best protected through regimes outside of privacy law).[121]

Finally, contextual integrity might moderate its unwavering commitment to social context. "Whereas other accounts offer interpretations of privacy in terms of universal prescriptions, contextual integrity couches its prescriptions always within the bounds of a given context."[122] But perhaps some universal prescriptions, or rather *pro*scriptions, are not such a bad idea. Perhaps there are some data practices (e.g., deploying facial recognition systems in public spaces)[123] that, no matter how inured or complacent society becomes,[124] should be deemed beyond the pale. As to these practices, such a refinement would remove all indeterminacy. Federal regulators already seem to be tending in this direction.[125] Integrating some similarly

[118] *See Facebook, Marketplace*, https://www.facebook.com/help/1713241952104830/ (last visited Sept. 8, 2025) (on file with author) ("You can use Marketplace to buy and sell items with people in your community on Facebook."); Meta Transparency Center, *About Ads About Social Issues, Elections or Politics*, https://transparency.meta.com/policies/ad-standards/SIEP-advertising/SIEP (last visited Sept. 8, 2025) (on file with author) ("Learn how ads about social issues, elections or politics are defined on Facebook and Instagram.").

[119] *See* Gstrein & Beaulieu, *supra* note 95, at 31 (recommending the adoption of "essential criteria for the protection of fundamental rights" concerning data).

[120] NISSENBAUM, *supra* note 2, at 165.

[121] *See generally* Austin, *supra* note 52 (distinguishing between privacy and other important social values).

[122] Nissenbaum, *supra* note 6, at 154.

[123] *See* Rachel Metz, *Portland Passes Broadest Facial Recognition Ban in the US*, CNN (September 9, 2020, 8:06 PM), https://www.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html.

[124] Woodrow Hartzog, Evan Selinger, & Johanna Gunawan, *Privacy Nicks: How the Law Normalizes Surveillance*, 101 WASH. U.L. REV. 717, 788 (2024).

[125] Bradley, *supra* note 5, at 133 ("[Regulators] have sought to establish substantive baseline norms"). Though the Federal Trade Commission still gives primacy of place to privacy policies to which consumers consent, they have also identified data practices that it considers presumptively deceptive or unfair. HOOFNAGLE, *supra* note 5, at 146 ("It is no longer the case that companies can simply point to a privacy

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press

universal and uncompromising basic information norms might assuage the most worrying arguments against contextual integrity by backstopping just how far privacy-corrosive evolution of contextual norms could go.

While any of these refinements would help, one might wonder whether the resulting view would still be recognizable as contextual integrity. The first refinement might be seen as removing contextual integrity's core concern—social context—and replacing it with something meaningfully different—one party's perception of social context. The second refinement risks converting contextual integrity's evaluative angle—integrity to context—into some single moral or political consideration. And the third refinement would require contextual integrity to abandon some of its prized mercurial relativism. Only contextual integrity's advocates can say whether the view would survive such reforms. It may also be that we all need to move beyond integrity to context if we aim to prevent privacy's demise.

Acknowledgements

For helpful discussions and comments on earlier drafts, I am grateful to Biagio Andò, Ignacio Cofone, Andrew Jordan, Kirstin Martin, Rishab Nithyanand, participants at the Privacy Law Scholar's Conference in 2024, and two insightful anonymous reviewers.

. . .

MIHAILIS E. DIAMANTIS (mihailis-diamantis@uiowa.edu) is the Ben V. Willie Professor in Excellence at the University of Iowa College of Law, with courtesy appointments in the Department of Philosophy and the College of Business. He co-edits the Technology Section of the *Journal of Business Ethics.* He holds a JD from Yale Law School and a PhD in Philosophy from New York University.

policy and justify any kind of data practice."); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 628, 638–40, 667–69 (2014) ("The FTC has brought actions against companies for 'deceptive' or 'unfair' practices based on consumer expectations, industry standards, and public policy.").

https://doi.org/10.1017/beq.2025.10085 Published online by Cambridge University Press