Philosophy & Technology (2025) 38:6
https://doi.org/10.1007/s13347-025-00838-z

RESEARCH ARTICLE

Why you Should not use CI to Evaluate Socially Disruptive Technology

Alexandra Prégent[1]

Received: 9 July 2024 / Accepted: 11 December 2024

Abstract

Contextual Integrity (CI) is built to assess potential privacy violations of new sociotechnical systems and practices. It does so by evaluating their respect for the context-relative informational norms at play in a given context. But can CI evaluate new sociotechnical systems that severely disrupt established social practices? In this paper, I argue that, while CI claims to be able to assess privacy violations of *all* sociotechnical systems and practices, it cannot assess the ones that cause severe changes and disruptions in the norms and values of a given context. These types of technology are known as socially disruptive technologies (SDTs) and this paper argues that they are beyond CI's scope. It follows that at best, a privacy assessment of those technologies by CI would be useless and, at worst, lead to potential harm, including failure to identify privacy violations and unwarranted legitimisation of privacy-threatening technology. Government actors, policymakers, and academics should refrain from relying on CI to assess this type of technology.

Keywords Informational Privacy · Contextual Integrity · Emerging Technologies · Value Change · Social Norms

1 Introduction

The rise of ICTs (Information and Communication Technologies) and other sociotechnical systems and practices has impacted our lives by enmeshing people and technology in webs of information, reshaping social dynamics and expectations (Floridi, 2014). Expectations of privacy are among the most challenged by these sociotechnical changes, pushing philosophical inquiry in information ethics into a seemingly never-ending quest for informational privacy (Lavazza & Farina, 2023). Explaining and justifying people's privacy interests and rights in terms of control or access over their personal information appeared to be a much more challenging task

✉ Alexandra Prégent
a.pregent@phil.leidenuniv.nl

[1] Leiden University, Institute of Philosophy, Leiden, The Netherlands

Published online: 14 January 2025

than it looked at first sight. In informational privacy, the control- and access-based accounts of privacy have dominated the debate so far. However, these accounts have faced numerous challenges that have weakened their claims over people's privacy interests and rights. The problem of privacy in public (Ryberg, 2007), the feminist critique of privacy rights (Allen, 2003), and the moral hollowness of privacy rights (Thomson, 1975) are just the tip of the iceberg. Against the backdrop of this decade-long conundrum, the contextual integrity (CI) framework developed by Helen Nissenbaum (2010, 2018, 2004, 1998) proposed a novel approach that considers informational privacy in terms of the appropriate flow of information in a given context. Presented as a tool to assess privacy violations of sociotechnical systems and practices, CI stands out by its capacity to provide a coherent answer to the challenges that other accounts are unable to resolve. Rather than focusing on individual's interests and rights, Nissenbaum proposes to investigate the structure of normative standards that guide the flow of information as a way to justify (or reject) the use of personal information by different parties (Rule, 2019).

Attractive by its clear methodology and simple step-by-step framework, CI has seen its popularity grow steadily over the years with interdisciplinary scholars, political actors, and governmental institutions relying on its model (Wisniewski & Page, 2022). The Federal Trade Commission has followed the CI heuristic in its report on "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers" (FTC, 2012). In 2014, the report on "Big Data and Privacy" by the U.S. Executive Office of the President's Council of Advisors on Science and Technology referred to CI as a helpful guide in its advice on privacy regulations (Executive Office of the President's Council of Advisors on Science and Technology, 2014, 41). CI has been used for assessing smart technologies (Apthorpe et al., 2018; Shaffer, 2020; Winter, 2012), technological change (O'Neill, 2022, 2023), to explore the long-term risks of COVID-19 surveillance technologies (Vitak & Zimmer, 2020) and more recently, to tackle the new threat posed by neurotechnology (Susser & Cabrera, 2023). These and other examples demonstrate the increasing use of CI to conduct privacy assessments of new technologies; but is the CI heuristic capable of assessing *all* sociotechnical systems and practices?

In this paper, I argue that while CI is presented as a tool that can help assess privacy violations of *all* sociotechnical systems and practices, it cannot help assess some emerging ones, that is, in particular, those that cause severe changes, disrupting the norms and values of a given context. These types of technology are known as socially disruptive technologies (SDTs) and this paper argues that they are beyond CI's scope.[1] By critically revisiting the CI heuristic (Sect. 2), the paper shows that CI is facing two major problems which threaten the legitimacy of its evaluation results (Sect. 3). The two problems are 1) the problem of invalid comparison, and 2) the problem of the prevailing norm. These two problems are identified as breaking points in the CI heuristic and can both lead to a failure to identify privacy violations and a legitimisation of privacy-threatening technology. Finally, in Sect. 4, the paper

[1] See Sect. 4 for examples of SDTs.

focuses on SDTs and the reasons why *new* SDTs cannot be evaluated by CI. I argue that CI can only evaluate SDTs retrospectively.

2 The Framework

Sociotechnical systems and practices may sometimes interfere with people's expectations of privacy. In contrast to previous accounts that could not provide reasonable justifications for why people's privacy would be diminished in some cases but not in others (i.e., public settings), the CI framework provides a solution (Nissenbaum, 2004, 2010). It can explain why "ten different people observing the contents of your shopping cart on ten different occasions is *not* the same, from a privacy perspective, as one party recording and storing it" (Nissenbaum, 2019, 237, italics in the original). It also answers Ryberg's famous question about why a street CCTV camera is not the same as an old lady peeping on the street through her apartment window (Ryberg, 2007).[2] Indeed, unlike the CI, the access and control accounts of privacy seem unable to articulate why, from a privacy perspective, being watched by a person is different from being watched by a surveillance camera. According to Nissenbaum, the reason other privacy theories struggled to answer these sorts of questions was because "[they] were ignoring parameters whose values varied across the different cases" (Nissenbaum, 2019, 238). CI therefore proposes to unveil these salient parameters.

CI starts by considering privacy as appropriate flow of information. Hence, violations of *privacy* are done by *inappropriate* flow of information (Nissenbaum, 2010, 2018, 2004). To be able to trace back the information flow, CI focuses on the informational norms at play in a context. These informational norms are characterised by key parameters that are present in every context: the actors (senders, data subject, recipients), the transmission principles, and the attributes. These parameters respectively define the parties who are the subjects of the information as well as those who are sending and receiving it, the principles under which this information is transmitted, and the types of information at stake (Nissenbaum, 2010, 142–143). Hence, flows of information are shaped by key parameters, and embedded in specific contexts. Libraries, health care system, voting stations, schools, airport security, etc., are all contexts. Contexts are considered social domains in a Walzerian sense, with their own teleological values and purposes (Nissenbaum, 2010, 134). Hence, social contexts have entrenched social norms embedded in them (Nissenbaum, 2010, 132–134, 146). These social norms help achieve the context's values, which take the form of goals, purposes, or ends. Prevailing values in the U.S. health care system, for instance, include alleviating physical suffering, curing illness, and promoting the health of individuals as well as collectives (Nissenbaum, 2010, 134). Hence, informational norms and values are both in a co-constitutive relationship with their context, shaping it and being shaped by it (Nissenbaum, 2010, 141, 180).

[2] For an interesting discussion on public privacy, see Ryberg (2007), Lever (2008), Goold (2008), and Ryberg (2008).

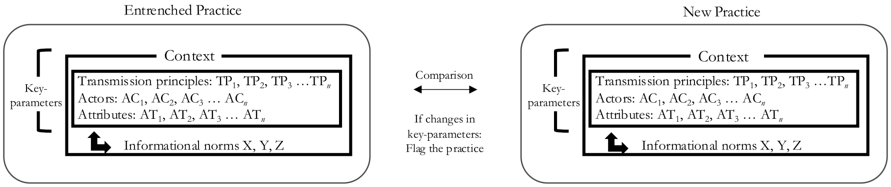

Entrenched Practice
Key-parameters
Context
Transmission principles: TP_1, TP_2, TP_3 ...TP_n
Actors: AC_1, AC_2, AC_3 ... AC_n
Attributes: AT_1, AT_2, AT_3 ... AT_n
Informational norms X, Y, Z
Comparison
If changes in key-parameters: Flag the practice
New Practice
Key-parameters
Context
Transmission principles: TP_1, TP_2, TP_3 ...TP_n
Actors: AC_1, AC_2, AC_3 ... AC_n
Attributes: AT_1, AT_2, AT_3 ... AT_n
Informational norms X, Y, Z

Fig. 1 Scheme of CI decision heuristic before moral augmentation

If the new technology provokes a change in the flow of information, the practice is “flagged as violating entrenched informational norms, which constitute a prima facie violation of contextual integrity” (Nissenbaum, 2010, 150). This departure from the entrenched context-relative informational norms at play in the context is assessed by drawing a “comparison […] between [the] entrenched practice and the novel practice” (Nissenbaum, 2010, 148–149). Figure 1. below schematises this process.

Once the practice is flagged, it is not rejected *ipso facto* but needs to be assessed normatively. The normative assessment can be seen as the second part of the evaluation and mainly relies on the values of the context. CI uses the values as evaluative tools to analyse the new technology. The values of a context are the result of a collective judgment that is, similar to the context-relative informational norms, also historically, culturally, and geographically shaped. Hence, a new technology that induces a departure from these entrenched norms is thus seen as an a priori threat, but can nonetheless be upheld against the entrenched practice if it can show that it respects and promotes the values of the context; thus maintaining the integrity of the context (Nissenbaum, 2010, 186). In sum, CI is a hermeneutic tool that helps us interpret complex situations, shape our analysis, and guide our thinking along clear social and normative lines to find salient structural social settings and patterns.[3]

3 Two Major Problems in the CI Heuristic

Although CI has been the tool of choice in recent years for identifying potential privacy violations by new and emerging technologies, it has also been subject to a number of criticisms. The normative fragility that results from relying on social norms (Austin, 2003; Birnhack, 2011), the low probability of agreeing on the norms that deserve to prevail (Rule, 2019), the inherent conservatism of CI making it possible to justify problematic technologies that follow established norms (van de Poel, 2022a), and the impossibility of preserving individual rights – such as autonomy and individual choice – are the main ones (Gstrein & Beaulieu, 2022). Nissenbaum herself conceded that it is sometimes “impossible to locate the relevant entrenched

[3] Nissenbaum draws her theory mostly from social theorists (Schatzki (2001), Bourdieu (1984), and Walzer (1984)) and implements these ideas in her pragmatic and normative account, which heavily rely on common values and norms.

norms against which to compare the novel flows" (Nissenbaum, 2019, 247). However, in these cases, she argues that CI still stands on an equal footing with the other accounts of privacy, as in those cases the other accounts also cannot provide a reasonable justification for a potential loss of privacy (Nissenbaum, 2019, 247).

In what follows, I will build on the previous criticisms[4] of CI to identify two breaking points in the CI heuristic that make the evaluation vulnerable to misuse. I will then identify two potential harms that can result from those breaking points. Finally, I will show why new SDTs are outside CI's scope.

The first breaking point in the CI heuristic is identified as the *problem of invalid comparison* and targets cases where the CI heuristic compares the new practice against the informational norms of the entrenched one, while the two practices belong to two different contexts.[5] The second breaking point is identified as the *problem of the prevailing norm*, which shows that identifying the norm that deserves to prevail in a given context is problematic as it stems from a subjective judgment of what should be the normative standard.

3.1 The Problem of Invalid Comparison

The comparison requirement is presented as a first step in the heuristic to evaluate the new practice against an already accepted normative benchmark which is the entrenched practice. As van de Poel (2022a) highlights, entrenched contextual norms serve society in a functional way, in the sense that they enable the realisation of shared ends.[6] As such, they are used as a benchmark to flag a new practice when the new practice departs from those entrenched norms. As prescribed by the framework, proponents of CI first look at the context-related informational norms that were at play *before* the introduction of the new practice to trace back the flow of information. This means that, for instance, if new virtual agents were to enter the health care context as personal assistants to practitioners,[7] the CI framework would

[4] I have no space here to cover in detail those previous criticisms, but it should be noted that Austin (2003) and Birnhack (2011), both coming from a legal perspective, have expressed worries over the reliance of CI on social norms. Austin pointed out that, by relying on social norms, CI lack the normative strength of other independent normative justifications. For instance, she argues that CI cannot demonstrate that an entrenched practice involves a loss of privacy. Hence, once a society becomes used to public surveillance, for instance, CI cannot articulate *why public surveillance is wrong from a privacy perspective* as it takes the entrenched informational norms as the *benchmark* for privacy (see Austin 2003). van de Poel (2022a) added to Austin and Birnhack's worries, by stipulating that the inherent conservatism of CI might be problematic in cases where "technology reinforces historically grown injustices" (van de Poel (2022a), 1).

[5] I am putting aside the more general problem of "framing" in social theory, which includes the problem of contexts within contexts as well as the related never-ending efforts at defining what a context is. As my goal is to pinpoint what is problematic with the CI heuristic specifically, I do not have the space to discuss this more general problem.

[6] As van de Poel points out, sometimes entrenched norms may "hinder rather than advance important share ends" (van de Poel (2022a), 2).

[7] See the case of SUKI (2021) "Using an AI Assistant to Reduce Documentation Burden in Family Medicine: Evaluating the Suki assistant", *American Academy of Family Physicians Innovation Labs Report (AAFP)*.

evaluate the new technology based on the informational norms at play *before* these virtual agents integrate into the health care context. This is not problematic.

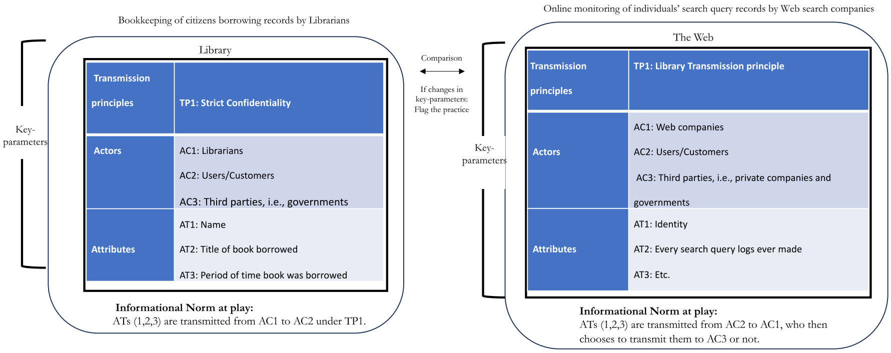
However, some new practices are sometimes in new, rather undefined contexts, where norms are flaky, or absent,[8] which prompts a CI evaluation to assess the new practice based on the informational norms of an established, similar context. This is what I will refer to as the *problem of invalid comparison*. This change of context, I argue, severely weakened the analysis by failing to respect the original justification that legitimated the comparison as a relevant technique in the first place. Let me explain this assertion. CI's foundational thesis is that every context is culturally and historically based, with its own teleology, which includes specific and uniquely shaped informational norms that guide the flow of information in accordance with the context's goals, purposes, and ends (Nissenbaum, 2010, 3, 134). These norms have been finely tuned over time and respect the customs, beliefs, values, and ideologies of a population. Informational norms are therefore context-dependant, and they preserve the integrity of the context in which they are embedded because they are the *product* of its particular structured social setting (Nissenbaum, 2010, 141). Hence, relying on the informational norms of a different context to evaluate a new practice is problematic as those norms are *not part of the teleological structure* of the context in which the new practice is evaluated. A change in context thus violates the coherence of the ensemble (rationale) on which CI grounds the legitimacy of its evaluation (Nissenbaum, 2004, 217). I will now illustrate this violation by using one of the case study discussed by Nissenbaum (2010).

3.1.1 Illustration of the Problem of Invalid Comparison with a Case Study

Nissenbaum uses many different examples to demonstrate how CI can function as a tool. One of them was using CI to investigate the practice of monitoring and tracking individual's search query logs by web browser companies. Using CI, she situates the practice "in the context of the Web" (Nissenbaum, 2010, 198), and evaluates it against the informational norms at play in the context of the library. Highlighting the similarities between the two contexts, she asserts that the Web as a context is a "complete comparison point" to libraries for the analysis of this new practice (Nissenbaum, 2010, 195–196). Following CI's steps, Nissenbaum goes on to compare the web searches (new practice) to its entrenched version, which is in her view the individuals' search of library catalogues and library's reference books of borrowing records.

As CI asks, the informational norms pertaining to the 'entrenched' context (i.e., the library) are identified and applied to the practice of individuals' online search queries. The informational norms governing the practices of librarians to which she refers relate mainly to the rules of conduct for librarians as stated in the Library Bill of Rights (Zimmer, 2007). These rules determine the transmission principles of the flow of information. Following them, library information transmissions regarding

[8] Some new practices also *create* a new context, which is often the case of SDTs. I will put these cases aside for now but will address them in Sect. 4.


Bookkeeping of citizens borrowing records by Librarians
Library
Key-parameters
Comparison
If changes in key-parameters: Flag the practice
Online monitoring of individuals' search query records by Web search companies
The Web
Key-parameters

Transmission principles	TP1: Strict Confidentiality
Actors	AC1: Librarians AC2: Users/Customers AC3: Third parties, i.e., governments
Attributes	AT1: Name AT2: Title of book borrowed AT3: Period of time book was borrowed

Informational Norm at play:
ATs (1,2,3) are transmitted from AC1 to AC2 under TP1.

Transmission principles	TP1: Library Transmission principle
Actors	AC1: Web companies AC2: Users/Customers AC3: Third parties, i.e., private companies and governments
Attributes	AT1: Identity AT2: Every search query logs ever made AT3: Etc.

Informational Norm at play:
ATs (1,2,3) are transmitted from AC2 to AC1, who then chooses to transmit them to AC3 or not.

Fig. 2 Overview of the identified key parameters of CI for both contexts

individual's searches are done under *strict confidentiality* principles, which leads Nissenbaum to argue that individuals' web searches should be governed by similar strict confidentiality principles. This means that information should flow in a similar way in the context of the Web as it does in the context of the library. In Fig. 2**.** below we can see an overview of this comparison, where the key parameters are used to undertake the evaluation.

3.1.2 Deviation from the CI Rationale: the Interplay Between Norms and Their Respective Context

The reliance on the informational norms at play in the context of the library to evaluate the actions carried out by web search companies on the Web is problematic because it goes against CI's rationale,[9] grounded in the uniqueness of every context.[10]

Informational norms are the products of a finely-tuned and uniquely structured social setting – shaped by the historical, cultural and geographical contingencies of a particular population at a particular time (i.e., respect customs, beliefs, values, and ideologies). They are described as "elements of a context-based system of informational norms as well as context-based normative systems, generally" (Nissenbaum, 2010, 141) and as part of a "co-constitutive relationship" with their context (Nissenbaum, 2010, 141). As such informational norms are the guardians of the integrity of the context, ensuring that the values are respected. Therefore, it is legitimate to

[9] Moreover, it justifies the process of identifying similarities between two contexts through a method of cherry-picking which is done by disregarding existing differences and focusing only on perceived similarities.

[10] "Because contexts are essentially rooted in specific times and places, their concrete character in a given society, reflected in roles, practices, norms, and values, is likely to be shaped uniquely by that society in relation to the arrangement of other contexts in that society as well as to its culture, history, politics, and economics, and even to physical and natural contingencies (e.g., war, famine, and earthquakes)." (Nissenbaum 2010, 134–135).

ask the question: what would legitimise the use of informational norms – considered context-dependant – in a different context than the one they are in a co-constitutive relationship with? If we argue that they can be used to legitimise the flow of information in a different context, then they are at odds with the justification of their own legitimacy, which is that they have been shaped by this particular context. Doing so would violate the internal logic in which their legitimacy is rooted. Therefore, I would argue that CI's rationale holds *only* in cases where the actions *x* of a new technology are evaluated in the *same* context as the actions *x* of the entrenched practice. For instance, in the library context, informational norms related to book records on paper (i.e., entrenched practice) can be used to evaluate the new practice of digital book records on a standalone computer. Cases where two contexts are needed should not be evaluated using the CI heuristic.

3.2 The Problem of the Prevailing Norm

CI is confronted with a second breaking point in its heuristic which I will refer to as *the problem of the prevailing norm*. The problem of the prevailing norm should be seen as superimposed on the problem of the invalid comparison. The problem of the prevailing norm refers to the task of identifying the norm that *deserves* to prevail in a context.

The CI heuristic can only be pursued once the informational norms of a context have been established because it is based on these norms that the information flow is evaluated. The problem of the prevailing norm thus points to this breaking point in the evaluation. It is a problem because the 'prevailing norm' refers to the norm that *deserves* to prevail (Nissenbaum, 2010, 149, 197) and this choice is not always as forward as it might seem. Indeed, the choice is complexified by at least two factors. Firstly, the number of norms available as potential candidates for the 'prevailing' one in a given context is generally multiple. Second, whoever makes the evaluation will make their choice of which norm deserves to prevail based on their political worldview, ethics and personal history. As Rule argues, even in the position of "reasonable observers", the chances of people agreeing on the norm that deserves to prevail are seemingly next to zero (Rule, 2019, 270). CI simply does not offer the necessary tools to conduct the evaluation in a way that would lead reasonable observers to the same and unique outcome on the prevailing norm in a given context. I will illustrate this problem in what follows.

3.2.1 Illustration of the Problem of the Prevailing Norm with a Case Study

For the sake of the illustration, let's put aside the first problem viz., the problem of invalid comparison. Let's take the context of the library once more. Taking the context of the library as a starting point, the CI requires the evaluator to find the prevailing transmission principle which is embedded in the dominant norms at play.

In this case scenario, the author endorses and recognises the Library Bill of Rights' (hereafter *LBR*) transmission principle of 'strict confidentiality' as the *prevailing* norm in the context (Nissenbaum, 2010, 196–197). However, as is often the case, other entrenched norms besides the principle of 'strict confidentiality' could have been seen as prevailing in this context. For example, the transmission principles drawn from the USA Patriot Act (hereafter *UPA*) were also used to regulate access to library catalogues after 9/11 (Zimmer, 2007, 203–204). Thus, one alternative choice would have been to recognise the transmission principles derived from the *UPA* as the prevailing ones instead of the one from the *LBR*.[11] While the principle of strict confidentiality states that information about individuals – relating to their borrowing records – should only be shared between individuals and librarians, the transmission principles guided by the *UPA* state that such information can also be transmitted from the librarian to the government.

The prevailing norm should be the one that best serves the context's values and goals. On Nissenbaum's interpretation, public repositories of information, such as the libraries, have always upheld privacy-directed values that support diverse freedoms and interests associated with inquiry, education, and expression (Nissenbaum, 2010, 196). However, although these are certainly important, it would be understandable if, in a context such as the post-9/11 era, these values were seen as less important than those that are security-related, which, as the author notes, can, for example, enable better monitoring of security threats and help to reduce child pornography (Nissenbaum, 2010, 196). The divergence existing both in the interpretation and in the contextual judgment of every evaluator might have led someone else to argue differently than Nissenbaum (Rule, 2019).

3.3 Two Potential Harms

In the previous section, I identify two breaking points in the CI heuristic, mentioning that these problems should be taken seriously as they can lead to potential harm. These harms are 1) a failure to identify privacy violations and 2) unwarranted legitimisation of privacy-threatening technology.

First, it might lead impartial evaluators to reach different judgments about the entrenched context to be used as a point of comparison and the norm that deserves to prevail, which is problematic. Second, it allows an ill-intentioned person to *manipulate* the evaluation, by choosing both the entrenched context and the prevailing norm[12] to arrive at the outcome that is the *most advantageous* for them rather than the one that preserves the integrity of the context. It should be kept in mind that the impartial evaluators and the ill-intentioned person may both cause harm.

Returning to our case study, where CI is used to evaluate whether or not the actions of web search companies that monitor individual search query logs respect the integrity of context. In this example, the change in context means that the evaluator can identify the entrenched context of their choice. In the case study, the

[11] This follows Rule (2019), arguing that agreeing on the norms that shall prevail can sometimes be impossible or at least extremely difficult.

[12] In cases where there is no comparison done across two contexts, the problem of the prevailing norm remains, and may lead to the potential harm without the need for the problem of invalid comparison to occur.

library and the Web could be compared as they were both seen as “public repositories of knowledge and information” (Nissenbaum, 2010, 195). Based on that definition, equal candidates to the library as an ‘entrenched’ context of the Web could also be the newspapers, radio broadcasting, TV news, Yellow Pages, magazines, etc. Hence, while the library context allowed her to evaluate the web search companies’ practices against the principle of ‘strict confidentiality’, another context—also seen as a ‘public repository of knowledge and information’—could allow an evaluator to evaluate practices against the principles of ‘open access and public domain’, which are the principles guiding the information norms of all the other contexts mentioned above. Had the evaluator chosen an entrenched context where the prevailing norm allows open access and public domain, the evaluation would have been much more lenient towards the web search companies’ practices, since against the backdrop of “open access and public domain”, the web search companies’ practices do not appear to depart from the entrenched norms. Thus the practice of web search companies could have been legitimised by a CI analysis that would have relied on another entrenched context such as the magazines or the TV news context. This is how the CI could have been manipulated, by legitimising the technology based on a wrongful comparison.

With the problem of the prevailing norm discussed in Sect. 3.2.1, if we had upheld the *UPA* principles against the *LBR* principle, CI could have been used to legitimise State access to individual searches and borrowing records in accordance with the *UPA* principles, which is what the author’s evaluation identifies as problematic (Nissenbaum, 2010, 196–197). The choice of the prevailing norm is therefore problematic because it can be manipulated to legitimise opposite outcomes, in this case potentially preventing ordinary citizens from making a privacy claim about their searches when accessing information.

Hence, these two breaking points may lead CI to be manipulated and harm people by denying that their privacy has been violated. The change of contexts and the subjective choice of the prevailing norm severely undermine the strengths and benefits of the CI reliance on the structure of contexts and leaves the door open to misuse of the framework, which could lead to the justification and legitimisation of wrongdoings (e.g., monitoring of citizen’s search query logs by the State) and the implementation of privacy-threatening technologies (e.g., web browser trackers).

4 Contextual Integrity and New SDTs

In this section, I argue against the use of CI to evaluate new SDTs. In Sect. 2, I have explained the framework and mentioned that CI’s main claim is that it can help identify (informational) privacy violations by tracing back the flow of information following the structured setting of contexts. The justification relies on a conception of contexts as teleological structures, where norms *and* values shape the context and are shaped by it. This section looks in more detail at the values and their limitations in identifying privacy-intrusive technologies.

4.1 Socially Disruptive Technology

New and emerging technologies that rapidly change the fabric of social life have been studied for some time (Wiegel et al., 2005; Rip & Kemp, 1998; Nissenbaum, 1998; Henderson & Clark, 1990) but in the last decade, particular attention has been devoted to technologies that provoke 'technological changes' (Carlsen et al., 2010; Volti, 2009) and 'technomoral changes' (Farina et al., 2022; Nickel et al., 2022; Swierstra et al., 2009; Wright et al., 2014).

Technologies that provoke social disruption are now grouped under the umbrella term of 'socially disruptive technology' (hereafter SDTs) (van de Poel et al. (2023); Hopster & Löhr, 2023; Hopster, 2021). These technologies share the particularity of disrupting human life at a "fundamental level" (Hopster, 2021). They severely disrupt the set of norms and values at play in the context in which they take place, changing social practices and the ways in which humans communicate and interact (Carlsen et al., 2010). Technology that disrupts social life also generally encompasses a high level of uncertainty (Carlsen et al., 2010; Nickel, 2020). The advent of civil aviation in the first half of the twentieth century, the launch of the World Wide Web in the public domain in 1993, the creation of the atomic bomb in the Second World War, the introduction of the oral contraceptive pill in the 1960, and the introduction of firearms to the First Nations in North America in the seventeenth century are all context-based technologies that can be analysed in terms of their social disruptions.

Contexts and technologies share a relationship of *interdependence.* As Hopster points out, social disruption is not intrinsic to the technology but rather is dependent on the "complex interplay between a technology and a given social context" (Hopster, 2021, 4). The ability to get from one place to another by plane rather than by car or train was socially disruptive for people in the U.S. in the early years of the twentieth century, but this disruption did not affect other societies for the simple reason that civil aviation did not exist in their countries yet. This relation to contexts explains why CI seems the de facto choice when assessing privacy-threatening technologies.

4.2 Moral Augmentation and SDTs

At this point in the analysis, defenders of the CI framework might argue that the moral evaluation would nonetheless save the evaluation from the pitfalls identified above. This potential counterargument would be legitimate, as my analysis so far has focused primarily on the descriptive part of the heuristic. I will respond to this potential claim in a twofold manner. First, I will make two short, more general arguments that apply to almost all technologies. Second, I will develop a targeted, longer argument focusing on SDTs as falling outside the scope of CI, which will also serve to explain why the normative part of CI cannot save the evaluation.

Defenders of CI might say that even if we agree 1) that carrying the CI evaluation across two contexts and 2) that the choice of the prevailing norm (influenced by individual contingencies on the evaluators' part, i.e., political worldviews, ethical principles, etc.) might be problematic, the evaluation can still be salvaged by the moral part of the heuristic, where the new practice needs to be evaluated *on its own merits*, viz., in terms of its capacity to respect the context's values. In other words, even if the comparison was done against the wrong entrenched practice, and the wrong prevailing norm was chosen, the new practice, ultimately, needs to pass the moral evaluation to be upheld, which is not based on the comparison at stake in the descriptive part. Because the second part of the analysis does not take into consideration the entrenched practice but only focuses on the new practice in its own context, it seems that the two problems could potentially be overcome.

Let me explain this further. Following Nissenbaum, the descriptive part of the heuristic concludes with a *prima facie* violation of contextual integrity (Nissenbaum, 2010, 150). Once the prima facie violation is established, the moral evaluation can proceed and from it, a *genuine* violation can be established.[13] Hence, the *prima facie* violation – that is the result of a departure by the new practice from at least one of the key parameters (see Sect. 2) – can be *overturned* by the moral evaluation if the latter proves that the new practice promotes the values of the context (Nissenbaum, 2010, 239). This is why it seems that the moral part might rescue the whole evaluation.

4.2.1 Argument 1. The Threats Enabled by the two Breaking Points Remain

Even if CI can in some cases overcome these problems in the second part of the evaluation, this does not mean that the CI heuristic is safe from the *threats* posed by it. Proponents of CI who argue that the moral evaluation can rescue the whole evaluation forget a pivotal step in the CI heuristic. As I mentioned earlier in this paper, to access the moral evaluation, the practice needs first to be *flagged*. A new practice is flagged when it disrupts the flow of information and departs from the entrenched practice. However, the threat present in both problems is that the new practice may not depart from the entrenched flow of the old practice if the old practice can be chosen from another context.[14] This may lead to the practice not being flagged in the first place, thus not undergoing the moral evaluation. This would lead directly to the first harm, the failure to identify privacy violations, and thereby enable the second harm, the unwarranted legitimisation of privacy-threatening technology.

4.2.2 Argument 2. Value Manipulation in the "Moral Augmentation" of CI

As was argued elsewhere (Rule, 2019), the CI's moral evaluation is also facing important problems. As described by Nissenbaum, the core of the moral augmentation is set around the values of a context. While Nissenbaum asserts that these values are identifiable, Rule argues that this is rarely the case. For instance, Nissenbaum states that the prevailing values of the U.S. health care system include

[13] I borrowed the term 'genuine' violation from van de Poel (2022a).

[14] This argument is also valid for the problem of the prevailing norm.

alleviating physical suffering, curing illness, and promoting the health of individuals as well as collectives (Nissenbaum, 2010, 134). However, especially in the U.S. where the health care system is based for the most part on a free market model, one could look at the way the health care system is structured and argue that the dominant values are capitalist ones, such as the efficiency of diagnosis, acceleration of the speed at which various drugs and treatments reach the market, and promotion of communication between different branches such as pharmacists and doctors. One could make a compelling argument around the claim that these values are the ones dominating and structuring the U.S. health care context rather than the ones identified by Nissenbaum. Hence, because the moral evaluation is grounded on the *interpretation* of thick concepts such as the values of a given context, the chances of arriving at a consensual outcome are very low, almost impossible (Rule, 2019, 270). As Rule states, the authoritative guidance presupposed by the moral augmentation of the CI heuristic implies a "transition from empirical knowledge of social conditions as they are, to normative directions for social practice as it ought to be" (Rule, 2019, 263).[15] This transition is difficult and subject to being the victim of a multiplicity of conflicting interpretations and judgments. Thus, Rule concludes that the normative evaluation based on the prevailing values of a context is "more likely to come in the form of gambits for "friendly persuasion", than revelations of unique "right answers"" (Rule, 2019, 277). This means that the normative evaluation is as much susceptible to manipulation as the choice of the entrenched context and the choice of the prevailing norm. Rule therefore stresses the normative fragility of the methodology of evaluation, which, when scrutinized, is revealed to be ultimately guided by the moral and political worldviews of individuals rather than by an objective 'Truth' that would be collectively endorsed (Rule, 2019).

4.3 Technology-Induced Value Change

Putting the first two arguments aside, I will now focus on the reasons that prevent CI from analysing SDTs. The core of the argument is that SDTs force a value change that provokes the emergence of a new state of affairs, which falls beyond CI's scope.

CI's Walzerian rationale is grounded in the idea that contexts are teleological, with norms and values both in a *co-constitutive relationship* with their respective context (Nissenbaum, 2010, 134, 141, 180). This is crucial for CI as it makes it possible to base the integrity of the context (and violations of informational privacy) on the respect of the information flow along the prevailing norm and in accordance with the dominant values of a given context. The prevailing norms and values' legitimacy is rooted in the way social norms and collective values are created. They are the product of cultural, historical and geographical evolutions that best serve the interests of the context in terms of its goals, purposes and ends (Nissenbaum, 2010, 3,

[15] It should also be noted that, in general, Nissenbaum seems to be identifying the values of a context "as it ought to be" rather than the values of a context "as it is", but it is not clear from the CI heuristic alone how we should choose the values of a context – i.e., values that *are* prevailing in the context or values that *should* prevail.

141, 180).For instance, in the U.S. educational context, they are defined by Nissenbaum as “transmitting knowledge”, “know-how”, and “imparting training”, in the health care context, they are defined as “alleviating physical suffering”, “curing illness”, “promoting the health of individuals as well as collectives”, and in the library context, they are defined as the “edification of citizens through untrammelled access to books” and “unconstrained intellectual exploration”.[16] Thus, the use of contextual values as an evaluative tool to analyse a new technology is superimposed on the prima facie evaluation by context-relative informational norms but is not independent of it.[17] Informational norms and values are interrelated because informational norms represent the dominating values of a given context.[18]

Hence, in theory, a new technology is evaluated against (1) the prevailing informational norms and (2) the values that are at play in a given context. If the new technology departs from the entrenched norms, it is flagged as a prima facie violation, but can still be rescued by the normative part of the analysis if it shows that it respects and promotes the values of the context: thus respecting its integrity.

However, some technology, such as SDTs fall beyond CI’s evaluation scope. They fall beyond because CI can only evaluate technologies based on entrenched norms and values in a context, which is what SDTs disrupt. SDTs severely and fundamentally disrupt norms, values, expectations, and beliefs (Hopster, 2021), inducing a profound change in the entrenched norms and values of a given context. By bringing new opportunities but also new threats, they conflict and mix the hierarchy of already-established norms and values, overturning the entrenched guiding ones. By doing so, they provoke “indeterminate situations” in Dewey’s sense (Dewey, 1938, 105–107); situations that are “somehow unsettling, incomplete, or felt as unpleasant” (van de Poel & Kudina, 2022, 5). The change in the state of affairs from pre-SDT to post-SDT creates an indeterminate situation that is induced by the technology (van de Poel & Kudina, 2022). It is indeterminate because the entrenched guiding norms and values of a context are changed by the technology, while the ‘new’ ones are still in the making.[19] Social norms and values usually take time to develop solid roots in a social context (van de Poel, 2022b; Bicchieri et al., 2018; Bicchieri et al., 2004). Hence, at the emergence stage, norms and values are fragile, ill-defined, and usually subject to a high level of uncertainty with practices, expectations and beliefs not corresponding to one another. The social change provoked by SDTs profoundly alters existing norms and values and creates new ones. In this

[16] See Nissenbaum 2010, specifically pp.134 and 183.

[17] Nissenbaum also mentioned some moral and political values, that seem to be overarching, more general values, such as “justice”, “fairness”, “autonomy”, “freedom”, “equality”, etc. From my understanding, these values can help us guide the normative analysis in terms of the *salience* of potential problems posed by the new technology, but they always need to be adapted and modified to be relevant in the context under evaluation.

[18] “Understanding the ways that norms of information flows relate to values, ends, and purposes of social contexts is crucial to judgments of whether novel flows are acceptable, and if not, constitute reasons for resisting change and weighing in favor of entrenched norms” (Nissenbaum, 2010, 228).

[19] See van de Poel & Kudina (2022) for a detailed explanation of technology-induced value change based on Dewey’s understanding of values.

newly created context (i.e., context post-disruption of SDTs), the norms and values are at the emergence stage, meaning that they are far from well-known and collectively endorsed. In this disruption of the status quo, where the prevailing norms and values have not yet been determined, the ‘new’ context (i.e., post-SDT context) has been without *entrenched* norms and values for some time. In this stage (i.e., before or at the initial moment of application of the technology), neither the changes nor the ‘final’ outcome can be determined using CI. This annihilates the possibility of grounding any normative appeal on the entrenched norms and values in the post-SDT context, at least for a while, given that it takes some time for new norms and values to establish themselves.

Only retrospective CI analysis might be able to analyse SDTs. This is so because the framework requires the technology to be evaluated against the backdrop of a robust, structured social setting (i.e., context). This state of affairs is not attainable with SDTs – otherwise, the technology would not cause a ‘social disruption’ in the sense established above. As seen in Sect. 3, CI can also not rely on another, similar context for its analysis either, as this would force it to go against its own justification of its rationale. Without entrenched norms and values to rely on in the new context, and without the possibility of relying on the entrenched norms and values of a similar context, CI is left with no tools to assess the privacy impact of SDTs before or at the time of their application.

In sum, in the case of SDTs, the informational norms at play in the ‘new’ context (context post-disruption) are new and ill-defined. For this reason, they do not have the same legitimacy as the “entrenched” norms and should not be used for the CI evaluation. Thus, the comparison requirement is impossible to fulfil in those types of cases because no practice preceded the SDT in the new context, as the new context was induced by the technology itself. The disruption has also caused serious changes in the set of dominant values. Hence, the established hierarchy of values in the context is shaken and the values to be respected and promoted are changed, rendering the moral analysis null. Therefore, the emergence of a new state of affairs – provoked by the SDTs – falls beyond CI’s scope of evaluation. Pursuing the evaluation as it is would, in the case of SDTs, lead to an abusive use of CI, where the analysis would be illegitimately based on two different contexts and where no entrenched norms from the context of the new practice would be used. In my view, this would be a misuse of the framework, with serious implications, including the possible failure to identify privacy violations and the use of the framework as a tool to justify and legitimise privacy-threatening technologies.

4.3.1 Implications for Defenders of CI

This has some implications for the future use of CI. First, it seems that a change in the heuristic is necessary, namely the incorporation of an extra criterion prohibiting the possibility of using two different contexts to evaluate a new technology. This would by itself narrow down the types of technology that CI can evaluate and would thus make sure that the new technology is evaluated by the norms pertaining to the context at play. To include this new criterion, proponents of CI could add the *identification* of context as an overarching parameter in the analysis. As an overarching parameter, the context could not change itself, leaving the changes only possible for the three remaining key parameters (i.e., attribute, transmission principle, and actor). This would compel a comparison of ‘established’ and ‘new’ practices in the same context and would narrow the scope of CI while not affecting the decision heuristic process for other types of technology. In that sense, it may be that sometimes, it is not possible to use CI to evaluate a new technology. Moreover, this would also help to avoid potential harm created by the change in context (i.e., the problem of invalid comparison). However, these harms would still be attainable through the choice of the prevailing norm in a given context (i.e., the problem of the prevailing norm).

Another important point for the future use of CI relates to a potential limitation of the critique I propose in this paper, and more specifically to the identification of a technology as an SDT. Indeed, it may prove to be a hasty task to determine whether or not an emergent technology is an SDT. Although some frameworks have been developed to categorise new technologies as SDTs, they remain rather vague in terms of their identification criteria (see Hopster, 2021). As there is no clear ‘threshold’ proposed in this paper as to when values and norms should or should not be considered sufficiently disrupted by a technology for it to be considered an SDT, this may lead to situations where it is unclear whether CI can be used or not.

5 Conclusion

CI is presented as a tool that can help evaluate sociotechnical devices and systems, and in particular those that provoke radical or disruptive changes in the fabric of social life as they are the most susceptible to cause protest and indignation (Nissenbaum, 2010, 5). Hence, CI seems to be an ideal choice to evaluate the privacy issues of SDTs. However, closer inspection demonstrated that this is not the case. I have argued that CI cannot evaluate technologies that severely disrupt the social norms and values of a given context, putting at risk individuals’ privacy claims when doing so. I made the case that SDTs cause such disruption and, therefore, should be considered beyond CI’s reach.

As the two breaking points in the descriptive part of the CI heuristic and the problem of values in the normative part have shown, CI is subject to important pitfalls that should be kept in mind when using it. Moreover, in the case of SDTs, the predictive capability of CI is severely undermined by the induced change in norms and values that these kinds of technology provoke.[20] Thus, CI cannot guide us in resolving the new trade-offs created by this shift in norms and values because this change does not immediately lead to a stable and clear situation but rather to an indeterminate situation (i.e., high uncertainty).

Even though I believe that proponents of CI (as well as many philosophers of technology) are right to pressure us to acknowledge the importance of contexts when assessing the use of new technology – as social settings can provide us with

[20] This is not to say that the influence is one-sided, as technology and societal values are mutually influenced by one another (van de Poel, 2020; Swierstra, 2013).

reasonable justifications on whether we want to disclose personal information – I think they would be wrong to present CI as the optimal choice to assess privacy violations of *any* sociotechnical devices or systems. Government regulations, private companies' privacy policies, and developers of new technology resting their privacy violation assessments on this framework should be aware that its foundation allows only for an adequate evaluation of a limited number of technologies. As its scope is limited, I conclude that the theoretical promises of CI do not align with real-world scenarios in which SDTs exist. SDTs must be subject to a privacy assessment that provides an adequate method for measuring the extent of the social disruption they cause. Finally, I urge for a more informed use of CI to avoid potentially harmful analysis. Users of CI that do not account for these pitfalls will fail to acknowledge that the framework allows for carrying out deceptive and misleading analyses that may lead to harmful conclusions. The broader aim of this paper is to contribute to the advancement of methodological tools for assessing potential privacy violations caused by the use of new and emerging technologies, particularly those with sociotechnical dimensions. Future privacy frameworks should aim to meet the challenge posed by SDTs, perhaps by integrating insights from social privacy with those from technosocial change.

Author Contributions Not applicable.

Funding This work was supported by the SSHRC Canadian grant (#752–2021-1281).

Declarations

Ethics Approval Not applicable

Consent to Participate Not applicable

Consent to Publish Not applicable

Competing Interests The author has no relevant financial or non-financial interests to disclose.

References

Allen, A. L. (2003). *Why privacy isn't everything: Feminist reflections on personal accountability*. Oxford: Rowman & Littlefield.

Apthorpe, N., Shvartzshnaider, Y., Mathur, A., Reisman, D., & Feamster, N. (2018). Discovering smart home internet of things privacy norms using contextual integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2*(2), 1–23. 59.

Austin, L. (2003). Privacy and the question of technology. *Law and Philosophy, 22*, 119–166. Springer.

Bicchieri, C., Duffy, J., & Tolle, G. (2004). Trust among strangers. *Philosophy of Science, 71*(3), 286–319.

Bicchieri, C., Muldoon, R., & Sontuoso, A. (2018). *Social Norms. The Stanford encyclopedia of philosophy*. In Edward N. Zalta & Uri Nodelman (Eds.), (Winter 2023 Edition) https://plato.stanford.edu/archives/win2023/entries/social-norms/

Birnhack, M. D. (2011). "A quest for a theory of privacy: Context and control" [Review of Privacy in Context: Technology, Policy, and the Integrity of Social Life, by Helen Nissenbaum]. *Jurimetrics, 51*(4), 447–479.

Bourdieu, P. (1984) Distinction: A social critique of the judgement of taste. Richard Nice, trans. Cambridge, MA: Harvard University Press.

Carlsen, H., Dreborg, K. H., Godman, M., Hansson, S. O., Johansson, L., & Wikman-Svahn, P. (2010). Assessing socially disruptive technological change. *Technology in Society, 32*(3), 209–218.

Dewey, J. (1938). *Logic, the theory of inquiry.* Henry Holt.

Executive Office of the President's Council of Advisors on Science and Technology. (2014). *Big Data and Privacy: A Technological Perspective*. Washington D.C.: The White House. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf. (Retrieved on 30th of June, 2024).

Farina, M., Karimov, A., Zhdanov, P., Lavazza, A. (2022). AI and society: A virtue ethics approach. *AI & Society*. https://doi.org/10.1007/s00146-022-01545-5

Floridi, L. (2014) *The fourth revolution: how the infosphere is reshaping human reality*. Oxford: Oxford University Press.

FTC. (2012). Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers. Privacy report of the Federal Trade Commission. https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers. (Retrieved on May 6th, 2024).

Goold, B. (2008). The difference between lonely old ladies and CCTV cameras: A response to Ryberg. *Res Publica, 14*(1), 43–47.

Gstrein, O., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy & Technology, 35*, 3. https://doi.org/10.1007/s13347-022-00497-4

Henderson, R. M., & Clark, K. B. (1990). Architectural innovation: The reconfiguration of existing product technologies and the failure of established firms. *Administrative Science Quarterly, 35*(1), 9–30.

Hopster, J. (2021) The ethics of disruptive technologies: Towards a general framework. In J.F. de Paz Santana & D.H. de la Iglesia (Eds.), *Advances in Intelligent Systems and Computing*. Cham: Springer. https://doi.org/10.2139/ssrn.3903839

Hopster, J., Löhr, G. (2023). Conceptual engineering and philosophy of technology: Amelioration or adaptation?. *Philosophy & Technology*, *36*(70). https://doi.org/10.1007/s13347-023-00670-3

Lavazza, A., & Farina, M. (2023). Infosphere, datafication, and decision-making processes in the AI era. *Topoi, 42*, 843–856.

Lever, A. (2008) Mrs. Aremac and the camera: A response to Ryberg (On Privacy in Public Places). *Res Publica, 14*, 35–42. https://ssrn.com/abstract=2507480

Nickel, P. J. (2020). Disruptive innovation and moral uncertainty. *NanoEthics, 14*, 259–269. https://doi.org/10.1007/s11569-020-00375-3

Nickel, P. J., Kudina, O., & van de Poel, I. (2022). Moral uncertainty in technomoral change: Bridging the explanatory gap. *Perspectives on Science, 30*(2), 260–283. https://doi.org/10.1162/posc_a_00414

Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy, 17*, 559–596.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79(1)*, 119–157.

Nissenbaum, H. (2010) Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

Nissenbaum, H. (2018). Respecting context to protect privacy: Why meaning matters. *Science and Engineering Ethics, 24*(3), 831–852.

Nissenbaum, H. (2019). Contextual integrity up and down the data food chain. *Theoretical Inquiries in Law, 20*(1), 221–256.

O'Neill, E. (2022). Contextual integrity as a general conceptual tool for evaluating technological change. *Philosophy & Technology, 35*, 79. https://doi.org/10.1007/s13347-022-00574-8

O'Neill, E. (2023). Balancing caution and the need for change: The general contextual integrity approach. *Philosophy & Technology, 36*, 68. https://doi.org/10.1007/s13347-023-00671-2

Rip, A., & Kemp, R. (1998) Technological change. In S. Rayner, & E. L. Malone (Eds.), *Human choice and climate change: Vol. II, Resources and Technology* (pp 327–399). Battelle Press.

Rule, J. B. (2019). Contextual integrity and its discontents: A critique of Helen Nissenbaum's normative arguments. *Policy & Internet, 11*(3), 260–279.

Ryberg, J. (2007). Privacy rights, crime prevention, CCTV, and the life of Mrs Aremac. *Res Publica, 13*, 127–143.https://doi.org/10.1007/s11158-007-9035-x

Ryberg, J. (2008) Moral rights and the problem of privacy in public: A reply to lever and goold. *Res Publica, 14*(1), 49–56. https://doi.org/10.1007/s11158-008-9048-0

Schatzki, T. (2001). Practice Minded Orders. In T. R. Schatzki, K. K. Cetina, & E. von Savingny (Eds.), *The Practice Turn in Contemporary Theory* (pp. 42–5). London: Routledge.

Shaffer, G. (2021). Applying a contextual integrity framework to privacy policies for smart technologies. *Journal of Information Policy, 11*, 222–265. https://doi.org/10.5325/jinfopoli.11.2021.0222

SUKI. (2021) Using an AI assistant to reduce documentation burden in family medicine: Evaluating the Suki assistant. *American Academy of Family Physicians Innovation Labs Report (AAFP)*. https://www.aafp.org/dam/AAFP/documents/practice_management/innovation_lab/repor-suki-assistant-documentationburden.pdf.

Susser, D., & Cabrera, L. Y. (2023). Brain data in context: Are new rights the way to mental and brain privacy?. *AJOB Neuroscience*. https://doi.org/10.1080/21507740.2023.2188275

Swierstra, T. (2013). Nanotechnology and technomoral change. *Etica & Politica, 15*(1), 200–219.

Swierstra, T., Stemerding, D., Boenink, M. (2009) Exploring techno-moral change: The case of the obesity pill. In Sollie, P., & Düwell, M. (Eds.), *Evaluating New Technologies*. The International Library of Ethics, Law and Technology, vol 3. Springer. https://doi.org/10.1007/978-90-481-2229-5_9

Thomson, J. J. (1975). The right to privacy. *Philosophy and Public Affairs, 4*(4), 295–314.

van de Poel, I. (2020) Three philosophical perspectives on the relation between technology and society, and how they affect the current debate about artificial intelligence. *Human Affairs, 30*(4), 499–511. https://doi.org/10.1515/humaff-2020-0042

van de Poel, I. (2022a). Socially disruptive technologies, contextual integrity, and conservatism about moral change. *Philosophy & Technology, 35*(3). https://doi.org/10.1007/s13347-022-00578-4

van de Poel, I. (2022b). Understanding value change. *Prometheus, 38*(1), 7–24.

van de Poel, I., & Kudina, O. (2022). Understanding technology-induced value change: A pragmatist proposal. *Philosophy & Technology*, 35(40). https://doi.org/10.1007/s13347-022-00520-8

van de Poel, I., Hermann J., Hopster J., Lenzi D., Nyholm S., Taebi B., & Ziliotti E. (2023). *Ethics of socially disruptive technologies: An introduction*. Cambridge: Open Book. Publishers

Vitak, J., & Zimmer, M. (2020). More than just privacy: Using contextual integrity to evaluate the long-term risks from COVID-19 surveillance technologies. *Social Media + Society, 6*(3). https://doi.org/10.1177/2056305120948250

Volti, R. (2009). *Society and technological change* (6th ed.). Worth Publisher.

Walzer, M. (1984). *Spheres of justice: A Defense of Pluralism and Equality*. Basic Books.

Wiegel, V., van den Hoven, J., & Lokhorst, G. J. C. (2005). Privacy, deontic epistemic action logic and software agents: An executable approach to modeling moral constraints in complex informational relationships. *Ethics and Information Technology, 7*(4), 251–264.

Winter, J.S. (2012). Privacy and the emerging internet of things: using the framework of contextual integrity to inform policy. Pacific telecommunication council conference proceedings 2012. https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/5545fd56-fa8f-49369adf-7084cb00a25a/content

Wisniewski, P.J., Page, X. (2022). Privacy theories and frameworks. In: Knijnenburg, B.P., Page, X., Wisniewski, P., Lipford, H.R., Proferes, N., Romano, J. (Eds.), *Modern Socio-Technical Perspectives on Privacy*. Springer, Cham. https://doi.org/10.1007/978-3-030-82786-1_2

Wright, D., Finn, R., Gellert, R., Gutwirth, S., Schütz, P., Friedewald, M., et al. (2014). Ethical dilemma scenarios and emerging technologies. *Technological Forecasting and Social Change, 87*, 325–336.

Zimmer, M. (2007). *The quest for the perfect search engine: Values, technical design, and the flow of personal information in spheres of mobility*. PhD diss.: New York University.