The 7^{th} PrivaCI report

May 19 - 21, 2025 in Brussels, Belgium, Vrije Universiteit Brussel & Brussels Privacy Hub.

Editors: Severin Engelmann and Yan Shvartzshnaider
Notetakers: Kyra Milan Abrams, Isabela Bertolini Coelho, Matthew Franchi, Margot Hanley, Ketevani Kukavam, Jae June Lee, Sunayana Rane, Kat Roemmich

Special thanks to our sponsors: SolidLab Flanders, CPDP.ai, Hasselt University, Digital Life Initiative (DLI) Cornell Tech, Research Foundation – Flanders (FWO)

Table of contents

Executive summary

In May 2025, the Contextual Integrity (CI) community gathered for the 7th annual PrivaCI Symposium—the first to take place in Europe—hosted by Vrije Universiteit Brussel and the Brussels Privacy Hub in Belgium. The symposium brought together over 70 researchers, practitioners, and policymakers to advance the application, critique, and extension of CI across diverse domains. Across eight sessions and community feedback discussions, participants explored how CI can inform theory, practice, governance, and standards in a rapidly evolving digital landscape shaped by artificial intelligence, generative technologies, and platform infrastructures.

The symposium opened with a session on CI and Theory, where presenters explored how group privacy, power asymmetries, and infrastructural dependencies intersect with CI and how the framework might respond to these complex dynamics. Papers proposed integrating CI with frameworks such as the capabilities approach and vulnerability theory, and debated whether CI should evolve toward greater contextual flexibility to accommodate fluid socio-technical realities.

Subsequent sessions applied CI to topics including synthetic data, online community harms, responsible AI in education, regulatory reforms, biometrics, surveillance, and standards-setting. Highlights included studies of privacy norms in queer communities on Reddit, critiques of synthetic data's normative neutrality, and proposals for integrating CI into data protection reforms and fiduciary governance models. The symposium also examined CI's role in addressing challenges posed by neuroprivacy, genomic data ethics, dense street imagery, and online tracking.

A dedicated session focused on CI and generative AI (GenAI), where researchers explored how CI can be operationalized to audit the privacy norms encoded in large language models and to elicit user expectations of privacy in interactions with GenAI systems. Discussions highlighted the importance of empirical and normative alignment in AI design and governance.

Session 1: CI and Theory

Notetakers: Kat Roemmich and Isabela Bertolini Coelho

This session brought together a series of forward-looking papers that collectively highlighted emerging theoretical challenges to Contextual Integrity (CI) posed by AI, especially large language models (LLM), data intermediaries, platform infrastructures, and group-level data dynamics. While CI remains a robust framework for describing and prescribing information norms within defined contexts, each paper highlighted distinct ways in which current sociotechnical and legal developments are testing the limits of the framework, and proposed extensions to CI through operationalization in new domains (e.g., group privacy) and integration with normative theories (e.g., power / vulnerability, human capabilities) to better address power asymmetries, normative pluralism, and infrastructural dependence.

Common themes across talks. Across all four papers, there was a shared recognition that many digital environments—especially those shaped by AI and platform governance—destabilize the very notion of context. Whether through system-driven context-switching, infrastructural collapse, or metaversal reconfiguration of social space, the papers underscored the fragility of context in an age where background conditions are increasingly engineered, opaque, and contested. They emphasized the need for normative analysis at group, institutional, and infrastructural levels.

Additionally, there was significant discussion about the difficulty of assessing the internal logic of these systems due to proprietary training data and inconsistent behaviors. Several speakers pointed to a broader failure in tech ethics, paralleling mistakes from the Big Data era, where new technologies are introduced without sufficient understanding of their normative consequences.

Accordingly, these papers—either explicitly or implicitly—addressed the under-theorized role of *power* in contextual integrity. Whether in the form of platform control, normative divergence across user groups, or emergent vulnerabilities in data economies, the talks converged on the idea that making power analytically central to CI's application is essential to diagnosing and prescribing appropriate informational norms within and across contexts.

Promising directions for future work. Future research should position CI not only as an evaluation tool but also as a generative framework for shaping ethical AI design. Key directions could develop context-sensitive parameters to guide the negotiation of normative boundaries—particularly in balancing individual and group interests under conditions of vulnerability and structural power asymmetry. Promising paths include embedding minimum moral thresholds into CI, exploring how fiduciary-like roles can be incorporated into its parameters, and formalizing CI into multi-scalar data governance models capable of operating at individual, domain, and societal levels.

Another promising path involves formalizing CI into multi-scalar data governance models capable of operating at individual, institutional, and societal levels. There is also a need to extend CI to account for

non-human ”agents” such as LLMs that influence social processes despite lacking subjectivity.

From contextual integrity to contextual flexibility? (full paper)

Armen Khatchatourov (Universit´e Gustave Eiffel)

Problem Statement: This paper discusses divergent conceptualizations of “context” between CI theory and its use in computer science (CS) and human-computer interaction (HCI), with CS/HCI treating context as a dynamic, implicit environmental or interactional layer. The paper traces how this view emerged historically and examines the limitations of current AI/HCI systems in handling context transitions, raising questions about autonomy, normativity, and system control in contemporary ubiquitous computing environments.

Application of CI: CI is employed as a normative lens to contrast against the interaction-level and system-defined conceptualizations of context in CS/HCI. While CI sees contexts as semi-stable, socially constructed spheres with intelligible norms governing information flows, CS/HCI systems treat context as a set of measurable features to be inferred and acted upon by the system, generally without user knowledge or participation. The authors use CI to highlight the tension between system-controlled versus socially negotiated boundaries: while they highlight CI’s potential to better safeguard self-determination (e.g., through participation in norm-setting), they also raise concerns about static views of contextual boundaries. They suggest a move toward contextual *flexibility* may be needed to reflect the fluidity of norms in modern socio-technical contexts.

Current Progress and Results: This is a theoretical provocation rather than an empirical study. The authors presented a historical analysis of AI’s evolution—from rule-based GOFAI to domain-specific expert systems to context-aware ML systems—to argue that each wave has tried and failed to model context meaning fully. They show how the move to software-layer policies that dynamically switch between contexts risks bypassing user autonomy and socially legitimate transitions, where the result is often a loss of both contextual intelligibility and social accountability.

Challenges and Lessons Learned: The paper highlights challenges in (1) AI/HCI systems imposing context rather than respecting socially co-constructed ones; (2) boundaries between contexts that are often unstable and negotiable, yet systems rely on fixed or inferred boundaries; (3) risk of systems reifying neoliberal governance logics through invisible definition and enforcement of context switching rules. It suggests mutual lessons learned between CI’s understanding of context and that of CS/HCI: while CS/HCI can learn from the social negotiation of boundaries highlighted in CI, CI could more formally accommodate contextual flexibility to account for the fluidity of real-world social contexts.

Future Work and Research Directions: More research is needed to examine the theoretical limits and normative risks where software systems determine and enforce contextual transitions without user participation or social consideration.

Minimally Just Framework for Digital Dignity: Unifying Contextual Integrity and the Capabilities Approach (full paper)

Kat Roemmich (University of Michigan), Florian Schaub (University of Michigan) and Kirsten Martin (University of Notre Dame)

Problem Statement: This paper addresses the question left unanswered—when a data flow is unjust—by CI's normative relativism, which evaluates privacy based on whether information flows adhere to context-relative norms and local standards of justice. The central question is how to evaluate the justice of a data flow when context-relative norms diverge, for example when a data flow is judged to both promote the social ends of a context and risk dignity harm to vulnerable people and groups.

Application of CI: CI provides the foundational normative framework in this work, particularly its parameters that co-constitute an informational norm and its values-pluralist commitments. The authors suggest that formalizing a minimum moral standards, i.e., shared norm, of respect for human dignity across contexts can resolve divergent norm conflicts that remain after application of CI's normative heuristic.

Current Progress and Results: The authors propose operationalizing Sen and Nussbaum's Capabilities Approach (CA) by setting minimal justice thresholds based on the essential requirements to uphold human dignity as a transmission principle in CI. This extension would enable the evaluation of data flows against a shared moral minimum—respect for human dignity (through CA) and social context (through CI)—based on its human impact. Where a data flow may violate a person's dignity by reducing any of the ten core capabilities (e.g., bodily health, affiliation, emotions, practical reason) below their minimum thresholds, it would be considered unjust. The empirical case presented illustrated how a flow supporting bodily health may simultaneously erode affiliation in the U.S. employment context marked by structural inequality. Under CA, capabilities are non-fungible; thus, enhancing one at the cost of another—particularly for populations already near threshold—is unacceptable. The model offers a principled basis for resolving norm conflicts, identifying unacceptable trade-offs, and making visible the power laden consequences of "appropriate" data flows without consideration of shared moral minimums.

Challenges and Lessons Learned: Introducing a universal evaluative layer introduces questions about maintaining internal consistency within CI. The authors aimed to resolve this by drawing upon later writings of Michael Walzer acknowledging the need for minimum moral standards (e.g., human rights), suggesting CI's Walazerian foundations are compatible with this move, but seek input from the broader CI community.

Future Work and Research Directions: This is an ongoing research program. Future directions include theoretical development with the CI community and empirical validation of the CA+CI model through further studies. To make it explicitly compatible with rights-based data and AI governance, the framework would also require future work to formalize a capability impact assessment methodology.

Q&A Summary: Comments included observations on the alignment between normative privacy judgments (with and without consideration of core capabilities) and CI's normative heuristic. Questions concerned how this framework could inform the design of top-down regulation and data governance with

values sensitivity.

– Q1: The heuristic element of CI (how people intuitively evaluate appropriateness) is crucial and aligns well with capabilities theory. It helps elevate CI beyond individualistic preferences to entitlements and human functioning. Answer: Agreed, and emphasized that the capabilities approach provides a consistent, legally and culturally grounded basis for shared norms.

– Q2. Another participant asked about thresholds for ethical inferences, particularly in emotion AI. Answer: Speaker explained Nussbaum's emotional capability: the ability to experience, understand, and develop emotions in relation to one's values. Author also highlighted how emotions connect with cognition, reasoning, and identity, and how degrading them affects practical autonomy.

Data Intermediaries and Emerging Data Economies: Exploring the Need for Evolving the CI Framework

Michiel Fierens (ULeuven Centre for IT & IP Law), August Bourgeus Vrije Universiteit Brussel) and Ruben D'Hauwers (Vrije Universiteit Brussel)

Problem Statement: This paper explores questions raised when applying CI to address the rise of group-based data practices within emerging data economies: how can privacy frameworks balance individual and group interests when data is shared, aggregated, and acted upon at systemic levels? The paper addresses this question by examining the role of data intermediaries (i.e., entities that mediate between individuals and data controllers) and the challenges in accounting for the collective dimensions of data governance within CI, for example in contexts where group benefits or harms emerge only after data flows are initiated.

Application of CI: The authors apply CI as a foundational framework to assess the appropriateness of data flows, and raise the question of how well CI can accommodate settings where data is pooled for public goods.

Current Progress and Results: The work is primarily conceptual. The authors highlight practical dilemmas such as those posed by the EU Data Governance Act, which envisions data intermediaries as neutral actors with fiduciary responsibilities, without prescribing a definitive solution. They underscore the need to formalize how intermediaries relate to both individuals and groups, and question whether groups can be treated as autonomous entities within privacy theory. The authors suggest that CI's application to data economies mediated by public utility-like intermediaries may require theoretical expansion. They propose extending CI with systemic principles that operate at individual, group, domain, and societal levels.

Challenges and Lessons Learned: A key challenge is ontological: what is a group in the context of group privacy? The instability and retroactivity of group identification in data practices, as the authors note, complicates efforts to define governance or protection mechanisms in advance. Another challenge is conceptual: intermediaries are situated between users and institutions, but there is no clear parallel

intermediary for groups unless one reconceives the governance structure entirely. The authors note the inadequacy of ad hoc definitions of group, especially when harms materialize through post hoc inference.

Future Work and Research Directions: The main focus of future work is in defining concepts: defining appropriate systemic principles that simultaneously operate across levels, defining appropriate normative anchor points for group privacy, and even defining groups themselves—particularly when groups are emergent, inferred, or retroactively recognized.

Q&A Summary: The interactions focused on emerging empirical work on group privacy in CI and emphasized the importance of sustaining attention to the challenges raised by group privacy at both empirical and normative dimensions.

– Q1: How to define a group? Answer: Speaker notes that groups are often formed by the data flows themselves, emerging after-the-fact. Suggests leveraging the idea of ad hoc group formation and dual interest theory (individual and super-individual).

– Q2: Why protect group interests if individual rights exist? Answer: Traditional view: Group rights emerge from individual autonomy. Speaker argues: In data spaces, groups may have autonomous interests, especially when data is aggregated and used in ways not visible to individuals.

– Q3: What qualifies as a data intermediary? Answer: According to the EU Data Governance Act, intermediaries are neutral entities that facilitate trusted data flows. They are envisioned with strict obligations and possible fiduciary duties, distinguishing them from firms like ISPs.

Contextual Vulnerability: Bridging Contextual Integrity with Power Theories (extended abstract)

Gianclaudio Malgieri (Leiden University)

Problem Statement: This paper questions the extent to which CI can account for vulnerability and power asymmetries in contemporary data environments, particularly within platformized social contexts like social media and the metaverse where the opportunity for users to engage in norm-setting is increasingly challenging. The authors invoke EU regulatory terms to highlight how, in practice, the “average user” model breaks down in the face of *layered vulnerability*, where users face compounded risks due to structural, relational, and technological dependencies.

Application of CI: The authors position CI as a promising framework for interpreting data subject risks because of its attention to context-relative informational norms, which current vulnerability/power theories lack. At the same time, they highlight how CI lacks an explicit vocabulary or analytic structure to assess degrees of vulnerability, particularly in contexts that are themselves fragile or collapsed due to infrastructural dependence on Big Tech platforms. They propose extending CI’s diagnostic apparatus to reveal layered power imbalances (relational, structural, legal) and suggest expanding CI with parameters for vulnerability to assess harm and risk severity in digital environments increasingly dominated by platform control.

Current Progress and Results: Drawing on insights from their ReSocial project, the author synthesizes theoretical developments in power/vulnerability studies with legal and technological contexts. While the authors did not present formal empirical results, they emphasized a conceptual reframing: moving from a binary of average vs. vulnerable users toward a layered vulnerability model that captures structural and contextual dependencies to foreground the contextual conditions under which power asymmetries are intensified—particularly in digital environments where both individuals and social contexts are mediated by and dependent upon private platforms.

Challenges and Lessons Learned: A major challenge identified is definitional: if everyone is vulnerable, vulnerability loses normative force. The authors adopt a minimum layer of vulnerability view that recognizes universal interdependence while distinguishing higher-risk situations through layered analysis. Another challenge is that existing legal and design paradigms often fail to account for the contextual collapse introduced by platform infrastructure—a concern that raises questions about whether CI's traditional context-centric parameters are sufficient. The author concludes that without a framework for contextualized power and vulnerability, privacy theory and law will remain inadequate in addressing harms to digital dignity and resilience.

Future Work and Research Directions: The author advocates for a formal integration of vulnerability-sensitive parameters into CI to assess the severity of informational risks. This could take the form of a risk-indexing system tied to context fragility, user dependence, and resilience factors. Future work may also operationalize layered vulnerability in empirical studies (e.g., mapping how relational or infrastructure dependencies affect resilience and rights-exercising capacity on social platforms).

Q&A Summary: Questions concerned how to operationalize CI to account for rising vulnerabilities and what vulnerability-assessment parameters could be applied systematically to address contexts of structural dependence.

– Q1: What should we do about context collapse and systemic risk in platforms? Answer: We shouldn't only try to "de-collapse" contexts, but instead, adjust enforcement thresholds. The greater the power imbalance, the lower the bar should be to consider someone vulnerable.

– Q2: How do we assess power imbalance legally? Answer: While legal history shows removal of key protections (e.g., around consent and power imbalance), courts and regulators (like DPAs) still act on this logic. More consistent structural recognition is needed.

Comments: Discussion on how consent mechanisms have been weakened by regulatory interpretation, undermining power-sensitive privacy protections.

Session 2: CI and Sociotechnical lens

Notetakers: Kyra Milan Abrams and Severin Engelmann

The three talks in this session examined the relationship between CI and the Sociotechnical lens within different contexts. Paula Helm, Benjamin Lipp and Roser Puja presented their work “Synthetic Data and Privacy: generating reality, silencing controversy.” This work explores the relationship between synthetic data and contextual integrity, specifically through a project that used synthetic data as a solution. Helm discussed the Centaur project, which uses multimodal data (visual, audio) to track organized crime patterns in Germany. The project highlights conflicts between stakeholder priorities: public institutions wanted behavioral detection models trained on camera footage, while citizens resisted contributing real data. To resolve this, a tech company proposed synthetic data as a privacy-preserving workaround. They collaborated with investigators to script and produce fictional crime scenes as training data—essentially generating data from the imagination of stakeholders. Helm, as the project’s ethicist, raised concerns about the narrative that synthetic data is neutral or detached from real people, emphasizing that synthetic data remains a highly curated, norm-laden artifact.

In their presentation, Kyle Beadle, Mark Warner, and Marie Vasek introduced their study, *“Intracommunity Online Harms as Contextual Integrity in LGBTQ+ Communities,”* which examines how norms surrounding information sharing and data use manifest in online queer communities on Reddit. Drawing on the framework of contextual integrity, the authors analyze how platform users navigate the expectations of information flow and privacy within community interactions. Their findings reveal instances of context collapse, norm conflict, and intracommunity privacy harms, particularly where moderation practices are employed by users against one another. While Reddit markets itself as an inclusive platform, its underlying monetization strategies incentivize high-frequency posting, creating normative tensions with queer communities’ efforts to govern their own data and maintain contextual boundaries.

Lastly, Marco Houben, Jo Pierson and Rob Heyman presented their work “Assessing contextual integrity through a socio-technological ethical approach in the context of responsible AI in public education.” This work explores the relationship between CI, sphere transgressions and technological mediation. Focusing on the guidance ethics approach, the authors apply this to meso and macro challenges introduced in Edtech. Each talk presented challenges concerning how different groups have different priorities for data use and how we as researchers can explore these challenges.

Future directions include using synthetic data as a way to protect privacy, using CI to study subcommunities that have additional nuances and privacy contexts which may also contradict a broader, societal context, mapping the iterative process of developing norms within a static context or "group", pulling apart informational privacy norms within online platforms, building on the idea 'guiding' technologies with the help of contextual integrity and the framework of sphere transgressions to repair societal challenges, and promotion of Edtech and education to cooperatively work on these questions.

Synthetic Data and Privacy: generating reality, silencing controversy (extended abstract)

Paula Helm (University of Amsterdam), Benjamin Lipp (Technical University Denmark) and Roser Puja (University College London)

Problem Statement: This work explores the relationship between synthetic data and contextual integrity, specifically through a project that used synthetic data as a solution. Helm discussed the Centaur project, which uses multimodal data (visual, audio) to track organized crime patterns in Germany. The project highlights conflicts between stakeholder priorities: public institutions wanted behavioral detection models trained on camera footage, while citizens resisted contributing real data. To resolve this, a tech company proposed synthetic data as a privacy-preserving workaround. They collaborated with investigators to script and produce fictional crime scenes as training data—essentially generating data from the imagination of stakeholders. Helm, as the project's ethicist, raised concerns about the narrative that synthetic data is neutral or detached from real people, emphasizing that synthetic data remains a highly curated, norm-laden artifact.

Application of CI: Although CI wasn't deeply integrated in the analysis, CI is mentioned as a possible framework to address potential privacy violations that could arise from synthetic data. However, this exploration is left for future research.

Current Progress and Results: Helm discussed the Centaur project, which uses multimodal data (visual, audio) to track organized crime patterns in Germany. The project highlights conflicts between stakeholder priorities: public institutions wanted behavioral detection models trained on camera footage, while citizens resisted contributing real data. To resolve this, a tech company proposed synthetic data as a privacy-preserving workaround. They collaborated with investigators to script and produce fictional crime scenes as training data—essentially generating data from the imagination of stakeholders.

Challenges and Lessons Learned: This work-in-progress proposes synthetic data as a novel challenge of data justice making initial connections to privacy and bias. However, the talk centered on documenting the justification behind initiating and developing the Centaur project's use of synthetic data as a way to mitigate privacy concerns of collecting "real" data from public places such as train stations in Germany.

Future Work and Research Directions: This work calls for further scrutiny of calls for applying synthetic data as a justified privacy protection and data protection framework.

Q&A Summary

– Q1: Could you tell me something more about you as an embedded ethicist in the context of working together with the company that developed Centaur? Answer: I was not employed by the company, I was working for an ethical company. I supervised a PhD student that worked on this project.

– Q2: What did they expect from that specific role? Answer: In Centaur, they wanted to work with a specific company and I said we are out if you do this you will lose your ethics partner. You need to

implement provenance methods.

– Q3: What we could expect normatively from synthetic data? Reminds me of the motivation for differential privacy whereby noise is injected into a dataset so as to strike a "good" balance between privacy as noise and utility as accuracy. There seems to be a similar narrative behind the justification of generating synthetic data for the Centaur project. Answer: Yes, these narratives are nearly the same and we need to keep a close eye on the kind of normative work synthetic data are doing here. In particular, synthetic data might be used as an attempt to avoid algorithmic discrimination.

Intracommunity Online Harms as Contextual Integrity in LGBTQ+ Communities

Kyle Beadle (University College London), Mark Warner (University College London) and Marie Vasek (University College London)

Problem Statement: The authors observe a concerning takedown of LGBTQ+ content on social media by content moderation schemes. This work explores the privacy norms along which LGTBQ+ users share information on social media. Through online queer communities on Reddit, the authors find context collapse, norm conflicts, and privacy consequences of moderation between users. While the platform Reddit promotes inclusivity, it also has platform monetization dynamics that promote their users to post all the time. Simultaneously, queer communities make choices to govern their data that are in conflict with the norms of the platform.

Application of CI: The authors ask whether and how contextual integrity could be applied to understand and study the additional nuances and privacy contexts of LGTBQ+ communities. Authors raise several important questions in this regard such as how to map the iterative process of developing norms within a static context or "group" on social media? Their empirical work on sharing norms within LGTBQ+ communities is based on a recently published article at CSCW.

Current Progress and Results: Their empirical work suggests ways for platform designers to better use implicit norms to support governance in identity-based communities. This study examines online queer communities on Reddit, focusing on how specific subcommunities engage in self-moderation. The researchers identify instances of *norm conflict* occurring within a single community context, distinguishing this from *context collapse*, which typically refers to conflicts arising from overlapping audiences. In this case, group members weaponize other users' posts—removing them from their original context and using them within the same community to silence dissent. While Reddit promotes an ethos of inclusivity, its platform design and monetization strategies encourage constant user engagement. As a result, queer communities are left navigating the tensions between Reddit's incentive structures and their own efforts to govern content and maintain community standards.

Challenges and Lessons Learned: This work illustrates tensions in sharing information online within LGTBQ+ communities. Online spaces can offer safe spaces fostering inclusivity through sharing

identity-based information, which, in turn, can lead to identity-based discrimination and hate speech. Thus, the work shows that within specific communities that have specific informational needs, the experience of content moderation is perceived as censorship. This censorship can be self-censoring when Queer users take down identity-based information in response to hate speech against them. Is this form of silencing a form of inappropriate flow of information? The authors argue that for specific communities, contextual norms might be "multi-layered" and dynamic. This work-in-progress raises questions as to how CI could address the following key questions:

Future Work and Research Directions: How can we, with CI, study subcommunities that have additional nuances and privacy contexts which may also contradict a broader, societal context? How do we map the iterative process of developing norms within a static context or "group"? How can we pull apart informational/privacy norms within online platforms?

Q&A Summary:

– Q1: Are we conflating context with role? Example: coffee drinkers of the world unite as a type of role. Not because we've created a context of coffee drinkers but more so because of their role (previous work by Madiha Choski mentioned). Answer: This is an important question that we hope to address using CI but that we have not found an answer for yet.

– Q2: Do you see any specific harms that target queer individuals specifically since groups can disclose? Do you see a need for stricter privacy protection? Answer: Yes, there is lots to chew on here. We've seen people get doxed and outed, their identity exposed on Reddit and they end up on Facebook. Doxing and outing are the two biggest ones.

Assessing contextual integrity through a socio-technological ethical approach in the context of responsible AI in public education

Marco Houben (UHasselt), Jo Pierson (UHasselt) and Rob Heyman (VUB)

Problem Statement: This presentation examined the intersection of Contextual Integrity (CI), technological mediation (as conceptualized by Verbeek), and the ethics of guidance in the context of public education and educational technology (EdTech). Focusing on a smart school initiative designed to predict early dropout risk, the authors illustrated how ethical tensions arise when algorithmic systems are introduced into traditionally human-centered educational environments. They juxtaposed CI with *sphere transgression theory* from political theory and *guidance ethics*, a design-oriented ethical framework, highlighting the conceptual misalignments among these approaches. The presenters questioned whether CI alone is adequate for addressing the deeper institutional harms and structural power asymmetries that emerge with the deployment of predictive technologies in education.

Application of CI: This presentation explored CI, technological mediation (Verbeek), and the ethics of guidance within the domain of public education and EdTech. Drawing on a smart school project aimed at predicting early dropout risk, the authors showed how ethical frictions emerge when technology enters

traditionally human-centered educational spaces.

Current Progress and Results: The work examines the relationship between guidance ethics, CI, and sphere transgression to find that the theoretical underpinnings do not align.

Challenges and Lessons Learned: see “current progress and results”. The presenter also alluded to concerns about whether existing CI tools are sufficient for addressing deeper institutional harms and power asymmetries.

Future Work and Research Directions: The presenter raised a series of core questions: How can we further build on the idea of 'guiding' technologies with the help of contextual integrity and the framework of sphere transgressions to repair our societal challenge? How can we seduce Edtech and education to cooperatively work on these questions? (sustainably) What design and governance capabilities are needed for this?

Q&A Summary:

– Q1: Could you expand on the concept of *repair*? How does it manifest in practice? I was thinking of care ethics as a potential framework for guiding repair work. Are there any concrete examples? And how is this form of guidance normatively grounded? Answer: The concept of repair in this context is not primarily normative, but ontological—it is about how individuals express meaning within their specific school environments. The form repair takes depends heavily on local context and lived experience.

– Q2: I see a lack of normative force in these workshops. If a workshop participant transgresses a norm, how can you, as a researcher, identify or articulate that transgression? Is there something within the workshop structure itself that enables you to make such a determination? Answer: The workshop methodology is designed to allow stakeholders to express their own meanings and understandings. It’s not intended to impose external normative judgments, so it may not be well-suited to identifying norm transgressions in a systematic or prescriptive way.

CI Community Feedback session # 1

Note-taker: Ketevani Kukava, University College Dublin

CI Community Feedback session # 1 covered the following topics: 1) Integration of Contextual Human Rights-Based Approach and Data Autonomy; 2) The Legal Effects of Risk to Rights and Freedoms in the EU: The Case of the GDPR; 3) Putting OSINT in Context: How to Regulate Privacy in Public.

Integration of Contextual Human Rights-Based Approach and Data Autonomy

Kyra Abrams (University of Illinois at Urbana-Champaign)

Kyra Milan Abrams introduced the concept of data autonomy, meaning that people should have complete control over the flow of their personal information. She framed autonomy as a condition of appropriateness. She focused on the Human Rights-Based Approach (HRBA) by Design, which implies embedding human rights into the design of technology. She also discussed the notion of HRBA by cities, which involves city governance frameworks that extend beyond existing human rights protections.

Kyra Abrams highlighted how context influences data autonomy, with a particular focus on HRBA in cities and public transportation systems. She presented case studies from Champaign County and Marion County to illustrate these dynamics. With regard to Champaign-Urbana, she cited a news report where the Champaign-Urbana Mass Transit District declined a payment proposal from Marketplace Mall to use their space. Besides, she referenced concerns raised by local civil rights activists regarding Indianapolis' public transit agency for its lack of diversity among the businesses it works with.

Kyra Abrams invited feedback on several aspects, including:

- Advice on application for U.S. context for dissertation;
- Suggestions for future cities and case studies;
- Appropriate audience for contextual data autonomy and human rights.

During the discussion, an audience member asked Kyra Abrams to elaborate on the extent to which complete control corresponds to appropriateness, noting the significant distinction between the two concepts. He also asked her to expand on what it means to be "fully informed," particularly in the context of technology assessment, where it is often difficult for individuals to be fully informed of the consequences.

Kyra Abrams responded by acknowledging that the idea of "control" might seem misaligned but clarified that her perspective on control is based on indigenous data sovereignty. For her, control means the ability to govern data about oneself in ways that are not Western or colonial. This includes the power to say "no" or redirect certain flows of information. She emphasized that as data moves across contexts, it becomes increasingly difficult for individuals to remain fully informed. She argued that people cannot truly give full

consent, because full consent requires full understanding. Her point was that data autonomy should highlight this misalignment.

The Legal Effects of Risk to Rights and Freedoms in the EU: The Case of the GDPR

Tatiana Duarte (KU Leuven)

In the talk, **Tatiana Duarte** examined the legal effects of risk to rights and freedoms in the EU. She emphasized that in science, risk is typically defined as a relation between a set of outcomes and their corresponding likelihood – usually a causal relationship. However, when causality is either absent or complex, it becomes difficult to determine the outcomes (i.e., threats) and to assess their likelihood.

When it comes to risks to rights, this formula – the relationship between outcomes and their likelihood - is not always possible to use. Duarte asks, how do we measure risks to rights? She suggests that data controllers must construe the meaning of risk in context. This is where the legal effects of risk to rights intersect with the concept of contextual integrity. She further explained that controllers must construe the risk in context, but resort to diverse knowledge bases, including expert advice from data protection officers and input from stakeholders. A second effect of risk, as pointed out in data protection scholarship, is that risk functions as a calibrator of obligations: The higher the risk, the more stringent and protective the required measures. The third legal effect is that data controllers must prove that the rules of data processing are appropriate to contextual data protection needs. These three legal effects – 1) construing the meaning of risk in a specific context, 2) risk as an obligation calibrator, and 3) risk as a way of reversing the burden of proof – oblige controllers to develop appropriate rules and ensure that information flows comply with contextual data protection needs.

During the discussion, an audience member addressed Tatiana Duarte, noting that her points appeared to reflect a realist idea of risk by saying that risk can be quantified. He suggested considering a more constructivist approach to risk, which aligns with some of the points she had already made. He referenced the concept of reflexive realism, which acknowledges the need to measure risk. However, how do we agree on how we even measure the risk? He stressed that risks are always subject to contestation and signify political conditions. He then asked to what extent she has been thinking of risk governance as a process of looking at stakeholders and how norm construction happens.

Tatiana Duarte responded by clarifying that she did not intend to suggest that it can be calculated as a one-way calculation. Rather, she views the concept of risk and how it is framed as normative. She explained that her reference to the classical formula for risk was meant to show what is in law. Duarte noted that she omitted the precautionary principle which is recognising uncertainty that underpins any formulation of risk. She emphasized that her idea was constructivist or conventionalist. In her view, controllers are the companies interested in pursuing the activity of measuring risk, but this is an arena of dialogue. Ultimately, the legal subjects, such as controllers are responsible for conducting the risk assessment, and they have the final say.

Her point is that because risk framing is normative, it is open to contestation and more perspectives should come into play.

Putting OSINT in Context: how to regulate privacy in public

Amir Cahane (Hebrew University of Jerusalem)

In his talk, **Amir Cahane** focused on SOCMINT and the problem of privacy in public. He emphasized that governments increasingly use social media for intelligence gathering, particularly, for national security and law enforcement purposes. The shift from mass media to social media has introduced new challenges around secrecy and privacy. Social media content is often publicly accessible, but much of it is shared voluntarily by users for specific audiences and purposes.

Cahane highlighted the following issues: decontextualization and context collapse, effects of AI-based processing, enhanced state power, and "nontargets" contributing to predictive models.

With regard to the framework to regulate government-led SOCMINT, he emphasized the following principles:

- Publicly available personal data remains personal data.
- Social media openness is a continuum.
- Enhanced safeguards against the superior power of the state.
- Actionable data should be contextualized.

Additionally, Cahane highlighted the following CI elements:

- 6-level classification of "openness."
- Context-sensitive authorization regime.
- Purpose limitation enforcement.
- Mandatory context preservation.
- Platform-aware processing.
- Documentation requirements.
- Human-in-the-loop for contextualization.
- Analyst competency standards.

During the discussion, an audience member posed a question to Amir Cahane regarding Article 40(12) of the Digital Services Act (DSA), which permits various actors, including NGOs, to access so-called public data for the purpose of systemic risk research, such as analyzing negative consequences for public safety. He referenced an upcoming paper on the reasonable expectations of publicness, which explores what types of data can be analyzed and gathered. He suggested that there may be an interesting overlap that merits further discussion.

In response, Amir Cahane noted that the entire spectrum of activities undertaken by national security and law enforcement agencies with open-source intelligence on social media should be considered. These activities include targeted investigations, mass collection, etc. He emphasized that these practices involve varying modalities, some of which fall under the domain of mass surveillance jurisprudence of the European Court of Human Rights (ECtHR).

As a follow-up, the same audience member pointed out that Cahane has studied oversight mechanisms in the context of surveillance and questioned how realistic it is to expect law enforcement and national security agencies to change the way they grab public data. He highlighted the role of commercial companies that provide solutions to them. There is the entire industry that feeds security agencies with publicly available data, social media data, and so forth. He asked about the implementation of those principles, how realistic it is, and how it can be made more implementable.

Amir Cahane replied that he was not in a position to speak about the political feasibility. With regard to context-preserving data retention, he highlighted that context also needs to be documented as part of the collection effort. Counterintuitively, this may require collecting more data to be able to preserve privacy. He underscored the importance of law enforcement practitioners thoroughly documenting their activities in order to enable future oversight.

Session 3: CI and Regulation reforms

Notetakers: Sunayana Rane (Princeton University/ Chicago University), Jae June Lee (Cornell tech)

In Session 3, speakers explored ways in which CI can inform regulatory approaches. In the first session, the speaker advocated for ways to encourage corporate responsibility. The second speaker examined how CI's inductive, context-sensitive approach can harmonize with the deductive, legalistic traditions of European data protection law. It illustrated practical tensions around categories such as "personal data" and "legitimate interests."

Across both talks, participants suggested ongoing investigation into the operationalization of CI within existing regulatory frameworks to better align corporate actions with societal privacy norms. Speakers highlighted market-driven compliance mechanisms that included incentive-based regulatory approaches (such as large fines) and leveraging financial risk management mechanisms (such as increased insurance costs associated with potential noncompliance). Another presentation underscored how integrating CI into GDPR interpretations could mitigate the rigidity of existing legal definitions, offering nuanced privacy protections aligned with societal contexts.

Future research will focus on empirically mapping privacy norms and institutional design innovations that embed CI principles into market structures and legal frameworks alike.

Fostering a Market for Responsible Data Practices

Noah Apthorpe (Colgate University), Eleanor Birrell (Pomona College), Travis Breaux (Carnegie Mellon University), Kirsten Martin (Notre Dame University), Rishab Nithyanand (University of Iowa), Sarah Radway (Harvard University), Yan Shvartzshnaider and Maximiliane Windl (LMU Munich)

Problem Statement: Why should the consumer bear the burden of consent documents, etc.? This system does not work. What can the company do (they are currently getting away with a lot of stuff), can we make them do more? Would it be possible to enforce responsible data practices (which we define as those that are consistent both with legal standards and societal values) without new legislation?

Application of CI: In the social context of largest fines levied for GDPR violations, will the companies change their behavior to proactively try to mitigate risk (without new legislation)?

Current Progress and Results: They take examples from other industries to show how this might be possible to achieve without additional legislation.

Challenges and Lessons Learned: Consumers are often burdened with changing their behavior, whereas companies can be made to change behavior too by setting up incentives correctly.

Future Work and Research Directions: A combination of better enforcement and insurance against financial risk of getting caught might help achieve this outcome without new laws.

Q&A Summary:

– Q1: Is better enforcement (and then insurance against the fines for enforcement) the solution?

– Q2: In the cyber world, insurance against financial risk of getting caught did not work to change behavior.

Answer: Yes, but the fines just weren't big enough to shape behavior.

Answer: Insurance companies will only insure if you meet some basic criteria. So we turn the insurance company into a watchdog. Also creates an obligation to explain to your stockholders what your actual risks are (to the SEC). If there is a big financial risk, there is an obligation to disclose (the fact that they are insured also indicates a big financial risk).

– Q3:You should supplement this theory with a new theory of who should get the money from the fines. That piece is missing here.

Bridging the transatlantic divide: combining the inductive contextual privacy approach with the deductive data protection approach

Max von Grafenstein (Einstein Center Digital Future, Alexander von Humboldt (Institute for Internet and Society)

Problem Statement: Combining the inductive contextual privacy approach with the deductive data protection approach

Application of Contextual Integrity: In this project, CI is reconciled with the deductive data protection approach. Whether an IP address is personal data, for example, depends on how it is being used and whether it is needed.

Current Progress and Results: Several examples reconciled with the two systems. Flood zones, for example, relate to a specific homeowner and their house, so it counts as personal data, but it doesn't make any CI sense. Reconciling these two ideas involves improving outcomes for such cases, where the deductive approach might be too broad. So in the CI inductive approach, it depends on the ultimate value of the context. Combining the approaches means we can protect the fundamental rights from the processing risks. It is protecting effectiveness.

Challenges and Lessons Learned

Deductive data protection approach (typical for continental-European law traditions) fails each time we look at specific cases like flood zones or IP address.

Future Work and Research Directions

These ideas dovetail with “personal data” and “legitimate interest” ideas in CI, and we can expand this work to engage with those definitions. This in its current form would also be useful to practicing lawyers currently. Art 25 sec 1 of GDPR does data protection by design, which does in effect combine these approaches, and we should also have more like that.

Q&A Summary

Question about empirical work toward understanding norms (legal/social). Authors ran surveys and collected data about this general frame of questions. They asked people what someone could be done with their data, and grouped them by their concerns. The categories of their concerns actually reproduced the categories of fundamental rights. Contextual layer may reveal gaps in that higher level as well, and these two layers should be in conversation.

CI Community Feedback session #2

Rapporteurs: Matt Franchi & Margot Hanley

Privacy as Demarcation: In Search of a Common Concept from Private Sphere to Data Protection

Nora Becker, TU Dortmund University

Problem Statement: Privacy debates are split: "private-sphere" cases such as overhearing through a wall, and data-protection cases such as database misuse, are usually analyzed with different lenses. Becker asks whether a single analytic frame—demarcation—can unite them. Her claim: privacy is present whenever an intentional boundary separates X (the party withholding something) from non-X (the party kept out), regardless of whether that boundary is a wall's thickness, a turned back, or a closed browser permission.

Application of CI: CI supplies the scaffolding for this boundary test. Roles map to X/non-X, information types identify what is being shielded, and CI's transmission principles appear in a second decision layer that checks whether permission overrides or modifies the boundary.

Current Progress and Results: Becker unveiled a two-stage decision tree plus an evaluation matrix:

- **Stage A – Demarcation?** Record whether a boundary exists, from whom, toward whom, and about what.
- **Stage B – Permission?** If a boundary exists, verify whether an authorized transmission principle legitimizes crossing it.

Demonstrations showed how small technical or physical changes (thin vs. thick wall, handheld parabolic mic vs. unaided hearing) alter the tree's path and the resulting privacy verdict, suggesting the model can compare divergent scenarios—ranging from drywall eavesdropping to cross-database re-identification—on a common footing.

Challenges and Lessons Learned: Two open issues surfaced:

- Choosing a baseline comparison case—without a clear analogue, the tree stalls.
- Normative weight—does the tree itself encode values such as autonomy or data protection, or remain a neutral diagnostic?

Both challenges point to the need for curated case libraries and domain-specific glossaries.

Future Work and Research Directions:

- **Build a comparison-case library.** Document dozens of concrete scenarios already referenced—wall thickness, turning away, closed-window eavesdropping, use of technical advantage, cross-database linkage—so users can choose a baseline and observe how different decision paths resolve.
- **Translation study.** Drawing on Nissenbaum's and Solove's prior "translation" work, test whether the demarcation tree can reconcile autonomy-focused private-sphere doctrines with rule-based data-protection law, and identify where new CI-style parameters may be required.
- **Chain-flow alignment.** Collaborate with CI scholars to map the decision tree onto multi-hop or "chain computerization" data flows, treating each hop as a fresh demarcation check and refining the CI tuple if needed.
- **Practical tooling.** Develop an interactive visualizer that walks regulators or engineers through each branch of the tree, records their answers, and exports an auditable report—turning the framework into a usable compliance aid.

Q&A Summary:

– Q1: Does a "partial" demarcation equal a CI norm breach or a full violation? Answer: "Partial" triggers Stage B: evaluate permission and contextual expectations before labeling a breach.
– Q2: Can the framework cope with multi-hop data chains? Answer: Conceptually, each hop is a new demarcation check; tooling to automate this is on the roadmap.

Data Protection in Chains: Position Paper (Work in Progress)

Maria-José Bonthuis, University Medical Center Groningen

Problem Statement: The premise of this work was to enrich the core framework of contextual integrity with the idea of 'chain governance', drawing from the idea of chain computerization.

Application of CI: In this work, CI is extended to include additional hypothetical parameters in the traditional CI tuple of (data subject, data sender, data receiver, information transferred, and transmission principle).

Current Progress and Results: The proposed work is in progress. It discusses specific considerations around 'big' data, including how big data introduces complexity that makes transparency hard to qualify. Complex big data streams often have loosely-defined 'chains of command', originating at societal or collective interests.

Challenges and Lessons Learned: There remain challenges to define the suitability of merging contextual integrity and chain computerization. The author noted that this line of work had come from difficulties in decomposing information flows involving big data, and, indeed, this can be a highly challenging task in today's complex data landscapes.

Future Work and Research Directions: Proposed future work included more collaboration with scholars of contextual integrity expertise.

Q&A Summary:

There was sustained discussion around the author's call to establish a third actor (subject), i.e., an 'infectious disease' in a data flow that involved tracking who had contracted said disease. There was also limited ability for audience members to draw effective comparisons between contextual integrity and chain computerization, due to their limited familiarity with the latter concept (this includes us, the rapporteurs).

Session 4: CI and Biometrics

Rapporteurs: Sunayana Rane (Princeton University/ Chicago University), Jae June Lee (Cornell tech)

Session 4 focused on applying CI to the domains of health and related fields. This session encompassed three diverse studies: health data reuse at the municipal level, neurotechnology governance, genomic ethics. The session illustrated CI's potential for addressing these complexities.

Several common themes surfaced across presentations. Each speaker stressed limitations of current consent-driven models, noting that consent alone inadequately captures privacy concerns, especially when data can be repurposed unpredictably or affect non-consenting third parties. For example, this was apparent in Hanley's critique of neuro-privacy legislation, and de Groot's analysis of genomic data practices. Collectively, the session reinforced the urgency of developing finer-grained, CI-informed rules to govern relational, procedural, and normative dimensions of information flows. Future research directions emphasized empirical studies to better understand context-specific privacy norms and inform policy innovation.

Re-use of personal health data by local authorities for public interest purposes (use case)

Dorine Van Zeeland (Hasselt University - VUB-SMIT), Sofie Hennau (Hasselt University - VUB-SMIT) and Jo Pierson (Hasselt University - VUB-SMIT)

Problem Statement: Can we use public interest as the basis for the re-use of health data?

Application of CI: This project is an exploratory study. The GDPR already includes exceptions for such data reuse "for substantial public interest" under certain conditions. There are different kinds of legitimacy that need to be considered, and different laws/different community values apply in each case. There are a lot of reservations in health data sharing between authorities.

Current Progress and Results: Interviews of local politicians, asking them what would you intend to do with personal health data of citizens, and what kind of capacities do you need. Five mid-size cities, b/c larger cities have larger departments to answer these questions.

Challenges and Lessons Learned: There are reservations about health data sharing between authorities, in addition to financial constraints and interoperability issues. Political vision is often lacking in depth, but the administrative staff have better ideas. But the administrative staff is understaffed, and they still don't have sufficient knowledge of how they could use this data. More support is needed for vulnerable groups (which are vulnerable because of digital technologies… if using paper, they would not be vulnerable).

Future Work and Research Directions: Larger studies in health and lifestyle data reuse (smartphone apps, smart watches) to see if they can be used in responsible ways by municipalities. Want to see if robust policies could contribute to health policy preparedness. Improving vaccination levels, optimal monitoring, etc.

Q&A Summary:

– Q1: Look into the points emerging in the EU health data space as new laws emerge
– Q2: There are unexpected challenges that emerge, and differences between local authorities' vision in different cities. Answer: Yes, they are observing this too.
– Q3: Use different vignettes to fix CI parameters. Look into citizens' perspectives, not just authorities. Answer: yes, that is a future direction.

Rethinking Regulatory Approaches to Neuroprivacy: A Contextual Integrity Perspective (extend abstract)

Margot Hanley (Duke University)

Problem Statement: Explore how CI gives a lens to navigate critical privacy lens that is developing and examine neuro-privacy debates. Influx of money into the Neurotech space. Right now, it's mostly medical. But it's increasingly a broader consumer technology and education. AI is an accelerant.

Application of CI: Mental privacy is a debated space, leading to competing policy decisions on what exactly should be regulated and why. CI can help us think about what to prioritize in making those decisions. Treating CI as a descriptive and normative framework.

Current Progress and Results: In the neuro community, there is disagreement on what should be regulated. There is the neural privacy camp – focus on neural signals themselves, and mental privacy camp – focus on mental states (including any data that can be used to infer mental states). Two US state laws (CO and CA) have already passed legislation (HB 24-1058, CCPA) that add neural data to laws. CI would critique sensitivity as not being intrinsic to information type. Impossible to evaluate whether privacy is preserved. CI

does not reject sensitivity as a whole, but we need more fine-grained, context-driven rules. In applying CI parameters, it is clear that the laws only highlight one of the five: focuses on information type but leaves others unchecked. Laws flatten crucial distinctions. And it's impossible to evaluate whether privacy is preserved.

Challenges and Lessons Learned: Keystrokes and eye tracking can also reveal sensitive info about mental state, and this is not neural data. But perhaps CI can help us distill this space, focusing on information flows in a fine-grained manner based on existing informational norms.

Future Work and Research Directions: Can we translate CI principles into practical guidance for policy? Projects in-progress to do this, incorporating a deeper understanding of norms and expectations.

Q&A Summary:

– Q1: What about different categories of people impacted by this (for example, sports athletes and how their neural privacy is different/their experience with neural technologies is different). Answer: Reading different scalp, skin, etc. measurements affects different groups differently based on these characteristics. You have to account for individual differences. In this space, we are still trying to understand what neurotypical is, and what that looks like from a data perspective.
– Q2: There are consumer products coming out that suggest that you can infer people's stress levels, mental state etc. from noninvasive techniques. Would that emphasize the importance of these ideas?
– Q3: In the mental state framework, does the focus lie on the algorithm or the inference or both? Those seem different things. Answer: Focus, sleep, etc are all mental states that you almost have to induce in order to observe a measurable difference. So it involves the full range of the process.

A Contextual Integrity Approach to Genomic Information: What Bioethics can learn from Big Data Ethics (extended abstract)

Nina de Groot (VU University Amsterdam)

Problem Statement: Bioethical debate on genomics information is focused on medical space, whereas it should be better integrated with CI

Application of CI: Different contexts apply in different genomics data use cases

Current Progress and Results: Ideas on sensitivity of genetic information (STR vs SNP, for example), and on identifying distant relatives. There have also been many hacks of commercial genetic databases. Consent is often not informed (can be changed at a moment's notice, at any time), people don't read terms of service, etc. Only 2% of the population need to be in a DNA database in order to identify everyone. Consent has its limits.

Debate is similar to online privacy and big data debates (Nissenbaum said there is a need for change but not for revolution). Tyranny of the minority: if only 2% decide to share, then the whole population is included in these DNA databases.

Challenges and Lessons Learned: There are ethical issues beyond these critiques. Many of these problems have existing information norms in medicine, so maybe we can bring those into the CI framework. But we need norms outside medicine too, because this data is valuable outside of medicine (law enforcement uses, for example).

Future Work and Research Directions: How to develop CI-based norms that could govern the use, collection etc. of genomics data. How to put this into bioethics research debates, and into practice.

Q&A Summary:

Nina and Margot should write something together about using CI for different types of data
There was a debate about privacy exceptionalism for genomic data (and the same is going on for neurotech). Is there really anything problematic or exceptional about these two different kinds of data.

Session 5: CI and Standards

Rapporteurs: Matt Franchi & Margot Hanley

Session Summary

The three submissions in the CI and Standards session highlight the ample room that data stakeholders (i.e., data senders, data receivers, and regulators) still have to uphold the privacy of their data subjects. Whether it be autonomous driving companies, advertisers, standard-setting bodies, or academic research groups, there exists a need to establish contextual standards, and, more importantly, adhere to them in an auditable way. The importance of this work appears plainly before today's technological landscape, where the volume of identifiable data is exploding, and the ability to parse through said data is proliferating with advances in artificial intelligence.

The first two papers in this session ground their standard-setting recommendations in empirical experiments, showing real privacy harms in dense street imagery and in the tracking-enabled internet. Then, they provide recommendations specific to the context of their problems; notably, the first paper levies recommendations upon data receivers like academics, as academics are more flexible to amending their behavior than data senders and other industrial stakeholders. The third paper is more analytical, establishing a clear need for standard-setting bodies to consider metadata, or data about content data like how, where, and when it was created.

Privacy in Dense Street Imagery: From Face Blurring to Appropriate Flow of Spatio-Temporal Information (Use Case)

Hauke Sandhaus, Matt Franchi, Madiha Zahrah Chokshi, Severin Engelmann, Wendy Ju, and Helen Nissenbaum; Cornell University

Problem Statement: The problem addressed in this paper is a lack of consideration towards the privacy of groups when applying privacy-preserving processing methods to images of public street scenes.

Application of CI: CI is employed in this work as the privacy framework of choice for demarcating appropriate and inappropriate flows of information in the data landscape of dense street imagery (DSI). The authors map out specific flows that would arise from DSI's depiction of two groups in New York City: mobile food vendors and bike-based food delivery workers.

Current Progress and Results: The authors presented a penetration test showing just how easy it is to generate distributions of inferred group membership, addressing mobile food vendors and bike-based food delivery workers. Further, they use CI to demarcate appropriate and inappropriate flows that involve these groups. Tangibly, they call for specific recommendations levied upon the academic community, including establishing ethics review boards (beyond IRBs for overseeing human subjects research), adhering to a new CI transmission principle when working with DSI, developing contextual obfuscation tools, and studying emerging societal norms around DSI-producing technologies like CCTV cameras, dashboard cameras (dashcams), and smart glasses. Finally, this work presents two formative challenges. First, the authors challenge, and demonstrate clear evidence against, the assumption that anonymizing individuals within street imagery sufficiently protects privacy. Second, the authors call attention to DSI's status as a threat to the very nature and value of public space; turning venues for entrepreneurship into sites of vulnerability, morphing opportunities for spontaneity into fear of computational conjecture, and disaggregating the societal affordances of being a 'pedestrian'. Summatively, the authors utilize a sentiment from *The Smart Enough City*, surmising that unfettered DSI can move society towards a state where to avoid being tracked, you would have to take the functionally impossible step of opting out of public space.

Challenges and Lessons Learned: The authors work within the bounds called for by contextual integrity, meaning that relevant norms involving DSI must be known in order to make a definitive call on any information flow's appropriateness. The authors state this challenge might be overcome via vignette studies, as shown by many other works in the CI literature.

Future Work and Research Directions: Future work for this paper involves developing a contextual obfuscation tool, concrete evaluations of vision language models (VLMs) on capabilities involving the de-identifying and clustering of groups, and academic reform over the handling of large-scale empirical datasets that depict traces of real people.

Q&A Summary:

The presenter received specific questions and commentary about the perception of the project, and the general legality of collecting moats of DSI, from the European privacy perspective (notably, all of the authors of this work are situated at an American institution.) The consensus is that the societal norms involving DSI are highly sensitive to culture.

Web Privacy Based on Contextual Integrity: Measuring the Collapse of Online Contexts

Ido Sivan-Sevilla and Parthav Poudel; University of Maryland

Problem Statement: This work highlights the problem of multiple context collapse that occurs when web trackers persistently identify users across more than one context. Further, the authors argue that existing work is not considerate of who is violating the context and which context on the web.

Application ofvCI: This work operationalizes CI to empirically study single context collapse and multiple context collapse in different web contexts.

Current Progress and Results: The authors developed an impressive data collection pipeline that crawled the top 700 popular websites across distinct contexts (e.g., Adult, eCommerce, Education, LGBTQ, etc.) for 27 days, and parsed out identifying 'cookies' and JavaScript fingerprinting scripts.

The authors were able to generate a comprehensive, data-driven picture of context collapse across several online contexts, computing the average number of unique third-parties, the average number of cookies, the average number of persistent identifiers, and the percentage of in-context websites participating in context collapse. The authors find that context collapse is incurred via identifying cookies much more often than via JavaScript fingerprinting scripts.

Challenges and Lessons Learned: The authors note limitations in their data collection pipeline that limit their ability to collect rich pictures of user behavior.

Future Work and Research Directions: The authors call for the assigning of different groups to first-party websites that prevents trackers from causing context collapse, à la the functionality offered by Mozilla Firefox's 'Total Protection' feature.

Q&A Summary:

– Q1: Is context collapse merely a CI norm breach, or does it amount to a full privacy violation because clear context differentiation is a pre-condition for privacy? Answer: Ido maintained that collapse is best described as a norm breach in CI terms, yet acknowledged that if context differentiation itself is viewed as foundational, repeated breaches effectively become violations.

– Q2: How can the sharp separation of contexts in the physical world (e.g., visiting a doctor vs. searching for a job) be translated to the far more fluid online space, where browsing "follows" the user? Answer: He

emphasized the contrast between distinct offline contexts and the fluid online environment where trackers mix information flows, creating the collapse in question.

– Q3: Can processing data "on the edge"—drawing inferences locally for tasks such as managing bus lanes—provide enough data minimization and purpose limitation to prevent context collapse? Answer: He suggested edge processing as a technical remedy: running inferences locally minimizes raw data transfer, aligns with purpose limitation, and can therefore curb context collapse.

Metadata Standards: Contextual Enforcement of Personal Data Protection in an Automated World

Louise de Bethune; KU Leuven, CITIP, and State Archives Belgium

Problem Statement: In this work, the author examines metadata, asserting that (1) metadata is not inherently different from other mediums of data; (2) metadata can leak privacy just as content data can; and (3) data subjects are generally unaware of how metadata about them is processed.

Application of CI: This work applies CI when analyzing metadata standard-setting bodies, dissecting relevant norms into CI tuples (including information type, transmission principles, and 'roles'). The work calls special attention to the context in which data is created and processed, defining this information as 'metadata'.

Current Progress and Results: This work is more analytical, and forgoes any empirical measurement as presented in the former two papers of the session. And so, results are primarily recommendations. The author proposed inclusive metadata standards: to incorporate diversity within metadata standard-setting bodies, advocate for inclusive organizational values, and base standards on the concepts of fundamental rights and contextual integrity; establishing such standards might lead to positive impact on data governance.

Challenges and Lessons Learned: The primary challenge posited by this work is the actual adoption of the aforementioned recommendations by metadata standard-setting bodies.

Future Work and Research Directions: Future work might include a more thorough comparison of 'content' data and metadata, with respect to contextual norms and potential for privacy harms.

Session 6: CI and Surveillance

Note-taker: Ketevani Kukava, University College Dublin

The session covered the following topics: 1) Contextual Integrity Use Case: Dense Street Imagery; 2) Trawling Publicly Available Personal Data as a Case of Public Surveillance – and the Lessons Unlearned.

Contextual Integrity Use Case: Dense Street Imagery

Matthew Franchi (Cornell University) and Hauke Sandhaus (Cornell University)

Matthew Franchi discussed that dashcams make dense (spatially and temporally) street imagery. He highlighted the ways of obfuscation: blurring PII and trimming the start/end of trips. Among the receivers are academics, customers, corporations, and government. Dashcams lie in between sensors and robots, in a meaningful way. They assume the movement profile of their parent object. A large part of DSI's current threat comes from the adoption by highly used ride-sharing vehicles. Accurate, specific characterization of DSI-producing technologies helps to identify corresponding informational norms.

Matthew Franchi touched upon Jane Jacobs' "eyes on the street" theory: neighborhood vitality and safety are anchored under the watchful eyes of local community members. DSI-producing technologies inherit in part from eyes on the street. He discussed the following examples: a news report about two students creating face recognition glasses, sidewalk robots, and drones.

Franchi highlighted the importance of CI for DSI: CI captures and demarcates the highly contextual and specific information flows involving DSI, cleanly decomposing an event into a data sender, data receiver, data subject, information transferred, and transmission principle.

He discussed open questions around DSI, including how to obfuscate, cloud storage vs. on-edge processing, defining informational norms, and whether there are other ways to restrict the privacy risks of DSI, aside from visual processing techniques.

During the discussion, an audience member pointed out that, from a data protection perspective, making inferences on the edge is preferable to central storage. This approach aligns with the principles of data minimization and purpose limitation and limits the processing to a single context and prevents a collapse of context. Matthew Franchi agreed to this point.

Trawling publicly available personal data as a case of public surveillance – and the lessons unlearned

Bilgesu Sumer (KU Leuven), Isabela Maria Rosal (KU Leuven) and Ezgi Eren (KU Leuven)

At the beginning of her presentation, **Bilgesu Sumer** discussed the differences between web scraping, crawling, and trawling. Web scraping involves extracting specific data, such as text, images, etc. from web pages. Web crawling is broader, referring to the automated navigation of multiple web pages to harvest data. Trawling is even broader, focused on detecting patterns to feed into AI models.

In the legal context, she examined the legal basis of legitimate interest under Article 6(f)(1) of the GDPR and the case law – Meta v. Bundeskartellamt. Drawing on EDPB guidelines, Sumer noted that legitimate interest

can be relied on for AI model development and deployment, but it is not a “default” justification. Moreover, sensitive data should not be involved, and a balancing test should be conducted.

She also addressed the problem of reasonable expectation, arguing that people are often influenced and manipulated by big tech companies. As a result, they expect their privacy to be violated and get used to the idea of their data being processed by tech giants. Sumer further discussed context collapse, emphasizing the risk of training AI models on misunderstandings.

Bilgesu Sumer concluded that GDPR remains insufficient, almost inapplicable to data trawling. She highlighted that data that is not sensitive at the beginning may become sensitive as a result of the trawling activity and data enrichment. Additionally, data not initially personal may become personal data later. Under the GDPR, there must be a risk of actual harm towards a specific individual. Theoretical risk is not sufficient. If the risk of actual harm towards an individual is small, the legitimate interest could be a valid legal basis, even if larger groups may be significantly harmed. She pointed out that CI can also protect group privacy, as opposed to the GDPR.

In closing, she posed the following questions: Do we need completely different parameters/additional parameters to identify the context in trawling and GenAI training? Or do we need more limitations and safeguards on trawling practices?

During the discussion, an audience member asked about the term “public surveillance”, and why they call it so, does it refer to surveillance in public or surveillance conducted by public bodies? In response, Sumer explained that trawling typically involves data that is publicly available, often shared voluntarily by individuals on social media. While users may intentionally make their data public, they do not expect it to be used for training AI. Anything that is made public is in the public sphere. This is the reason they call it “public surveillance.”

Session 7: CI and GenAI

Notetakers: Kat Roemmich and Isabela Bertolini Coelho

This session explored how CI can be applied, extended, and operationalized in the era of Generative AI (Gen AI), particularly in relation to user-facing large language models (LLMs). As these technologies rapidly integrate into domains such as education, healthcare, and social interaction, traditional assumptions about user control, contextual boundaries, and transparency are increasingly challenged. The two papers presented in this session demonstrate complementary approaches: one uses CI to *audit* the normative assumptions encoded in LLMs themselves, while the other aims to *elicit* evolving privacy norms from end users interacting with GenAI tools. Together, they illustrate the methodological rigor and practical importance of CI as a foundation for empirical and normative governance in the age of AI.

Common themes across talks. Both papers demonstrate how CI's structured framework can be used to guide the design, evaluation, and regulation of LLMs by defining socially appropriate privacy norms and highlighting divergences between system behaviors/practices and user expectations. They debated how LLMs may inadvertently produce misleading or inaccurate personal data, potentially breaching privacy norms. Another recurring point was the displacement of trust and expertise, as AI agents begin to replace professionals in sensitive domains such as healthcare and HR. The black-box nature of these models and their inconsistent outputs across prompts highlighted difficulties in assessing their normative alignment. Throughout, the necessity of proactive ethical evaluation rather than reactive fixes was stressed.

Promising directions for future work. The first paper's framework for surveying LLMs lays the groundwork for a standardized CI-based audit tool that regulators, developers, and third-party evaluators could use to measure and compare normative privacy assumptions across models. The second paper's approach to eliciting privacy expectations from LLM users offers a valuable empirical foundation for informing data policy design and platform practices. Together, these contributions highlight the potential for integrating CI's normative assessments with technical efforts to align LLM behavior and data-sharing practices with the human value of privacy. Finally, the session called for interdisciplinary efforts combining technical, social, and normative perspectives to ensure responsible AI adoption grounded in a deep understanding of contextual integrity.

LLM on the wall, who *now*, is the appropriate one of all?: Contextual Integrity Evaluation of LLMs

Yan Shvartzshnaider (York University) and Vasisht Duddu (University of Waterloo)

Problem Statement: As generative AI systems are increasingly deployed, misalignment between encoded norms and social norms can result in privacy violations including inappropriate disclosures, reinforcement of biased practices, and extraction of sensitive training data. The paper foregrounds an orthogonal chal lenge: beyond studying outputs that leak sensitive information and reinforce bi ases, how can we

rigorously assess the normative privacy assumptions built into LLM behavior?

Application of CI: The paper leverages CI as the theoretical and methodological foundation to answer this question. By using factorial vignette designs from prior CI-based survey work (IoT and COPPA contexts), the authors treat LLMs as normative agents capable of revealing "encoded" assumptions about what information flows are acceptable. The authors administered vignettes to a variety of LLMs, each rated on a Likert scale of acceptability, and compared with original study results with human subjects.

Current Progress and Results: Key findings included variation in privacy norm judgments across LLMs, especially regarding transmission principles (e.g., consent) with model-specific tendencies, prompt sensitivity across models, and systematic patterns of norm clusters by actor, purpose, device, and transmission principle that suggest LLMs exhibit structured—if opaque—normative behavior.

Challenges and Lessons Learned: Black-box opacity remains a major barrier, making it difficult to account for differences in training data and fine-tuning with out greater transparency. Prompt sensitivity also threatens reproducibility and interpretability. That said, the authors suggest an approach to isolate consistently encoded norms.

Future Work and Research Directions: The authors propose refining their framework into a standardized CI-alignment audit tool for privacy norms in LLMs, which could evaluate models for alignment with privacy norms, aid in benchmark ing normative LLM behavior by regulators and developers, and even serving as a proxy for data transparency when direct access to normative assumptions is unavailable. Further directions include expanding to other contextual domains and across cultures.

Q&A Summary: The author was asked about the difference between the datasets used in the work.

Contextual Privacy Perspectives of Generative AI Users

Alisa Frik (ICSI) , Mada Alhaidary (King Abdulaziz City for Science and Technology), Julia Bernd (ICSI), Basel Alomair (King Abdulaziz City for Science and Technology) and Serge Egelman (University of California, Berkeley)

Problem Statement: This paper presents a study design-in-progress aimed at eliciting contextual privacy norms among users of generative AI systems (e.g., LLM-based chatbots). With increasing adoption of GenAI tools across domains such as education, health, and creative work, it remains unclear how users perceive the privacy implications of their interactions, particularly regarding data collection, sharing, and secondary use. The authors seek to explore how users' expectations align or diverge from actual data sharing practices.

Application of CI: The authors use CI to guide their investigation, structuring the measurement of privacy expectations by decomposing data flows into CI's five standard parameters. Vignettes are designed to

simulate realistic interactions between users and GenAI tools, with variations introduced across CI parameters to assess acceptability. The authors aim to surface patterns in perceived appropriateness across different purposes and contexts of use to provide a richer picture of emerging privacy norms among users of generative AI systems.

Current Progress and Results: At the time of presentation, the study was in the design and feedback phase. The authors shared a draft methodology for a factorial vignette survey that would present users with hypothetical scenarios involving data flows from GenAI tools and collect Likert-scale responses on acceptability.

Future Work and Research Directions: The finalized study is expected to contribute empirical insights into evolving privacy norms around GenAI systems, especially user sensitivity to different transmission principles and third party data sharing practices. Future work could involve comparing normative expectations around contexts of use, analyzing differences in perceived appropriateness based on user experience and system familiarity, and informing privacy guidance grounded in empirical norms.

Q&A Summary: The audience discussion focused on study design considerations, including clarifying system contexts so that participants are aware of which specific genAI system they are evaluating, refining the purpose parameter to assess purpose of data sharing practices alongside contexts of tool use, and leveraging pre-screeners to segment participants based on actual genAI usage experience.

– Q1: What makes GenAI privacy concerns unique relative to other tech? Answer: Novel data flows, ambiguity around data sources/subjects (user vs. AI output), evolving societal role of agents.

– Q2: Are we missing key stakeholders or data sources?

– Answer: Training data sources (public vs. private) and copyright were acknowledged as important but logistically challenging to include fully.

– Q3: How should the ”sender” (Prodigy Hub) be conceptualized in CI terms? Answer: Actively debated. Challenge is whether simply naming the tool suffices, or if its societal role/ontology needs definition for meaningful norm extraction. No clear resolution yet.

– Q4: Should ”purpose of sharing” be a distinct parameter? Answer: Suggested as important (e.g., sharing for marketing vs. security). Team is considering adding it to better capture nuanced concerns.

– Q5: Should marketing be included as a recipient despite initial exclusion? Answer: Strong argument made for inclusion due to unique GenAI profiling risks (e.g., inferring medical info).

Session 8: CI and User perceptions

Notetakers: Kyra Milan Abrams and Severin Engelmann

The two talks in this session focused on CI and User Perceptions. Isabela Coelho and Frederic Gerdon presented their work "Transatlantic Privacy Perceptions in the Age of AI and Digital Technologies Through the Lens of Contextual Integrity." They capture expectations of privacy to help policymakers, companies and the public learn more about current and future AI and digital privacy concerns.

Transatlantic Privacy Perceptions in the Age of AI and Digital Technologies Through the Lens of Contextual Integrity

Isabela Coelho (University of Maryland) and Frederic Gerdon (University of Mannheim)

Problem Statement: To help policymakers, companies, and the public learn more about current and future AI and digital privacy concerns.

Application of CI: Emphasis on social norms connects the survey with CI. The interpretations can help us understand real life groups and how we think about CI and the normative ground.

Current Progress and Results: 78 respondents for the survey. The survey has two main parts: a rotating part that measures change over time and a core part that measures emerging privacy issues and the current state and future of privacy laws. European experts view their privacy laws as more favorable compared to US experts. European experts have grown more pessimistic, US increased optimism but still more pessimistic than their EU counterparts. Risk of social engineering/ deepfakes, high in the EU. The US is more concerned with transparency and mass data collection and aggregation in comparison to EU.

Challenges and Lessons Learned: Challenges include small sample size, and they have an expectation of shifts in the digital privacy landscape due to generative AI.

Future Work and Research Directions: Adding more context specific measurements of perceptions by directly using CI parameters. Legal frameworks lag behind tech innovations, but expert insights reveal where gaps are forming. Exploring these gaps is a future direction. Exploring the business centered framework in the US vs user centered framework in Europe.

Q&A Summary

– Q1: Who are your experts in your sample? Answer: The sample was collected through the professional

networks of the principal investigators (PIs). These networks consist of individuals recognized for their expertise and substantial experience in the field of privacy and data protection.
– Q2: What about social networks? Answer: Privacy experts were recruited using snowball sampling initiated from an initial panel of identified experts. We also sought to expand the sample through outreach via the International Association of Privacy Professionals (IAPP) and LinkedIn, which contributed modestly to extending our pool of participants.
– Q3: Do you have the same person living in Europe? U.S. experts in Europe? Answer: It is possible for someone to be an American living in Europe. Our survey includes a specific question asking respondents to indicate the jurisdiction or region in which they are considered an expert, allowing us to capture such cases accurately.
– Q4: Why did you exclude governments in the question surrounding businesses and individual users? Answer: We addressed government actors separately through a dedicated question focused specifically on government roles, rather than combining them with businesses and individual users in that particular item.

Integrating Contextual Integrity into Cross-Country Comparative Research on Acceptance of Data Uses (extended abstract)

Frederic Gerdon (University of Mannheim)

Frederic Gerdon presented their study *"Integrating Contextual Integrity into Cross-Country Comparative Research on Acceptance of Data Uses."* This work employs a cross-national survey incorporating a vignette-based experimental design to examine individuals' acceptance of data use for public benefit, systematically varying key CI parameters such as actors, information types, and transmission principles. Both this presentation and the preceding talk engaged with the complexities of user perceptions of privacy across national contexts, offering insights into how CI can be meaningfully applied in comparative research on data governance and public attitudes toward data use.

Problem Statement: While cross-country comparisons and comparative research on data use and privacy are well established, such studies often fail to adequately account for context. In particular, they tend to overlook how variations in social norms, legal frameworks, and cultural expectations shape perceptions of data practices across different national settings.

Application of CI: Integration of CI in broader micro macro uses. Their survey is designed using CI parameters and they integrate CI and the Comparative Privacy Research Framework. Social contexts are placed at the meso level with this integration. Data types they use are health, location, energy use, and social media. Data recipients include university researchers, researchers at an internet company, and public agencies. Transmission principles include opt-in, opt-out, and ethics boards.

Current Progress and Results: The study conducted an online survey in Germany, Spain, and the United Kingdom, employing a vignette-based experimental design to explore public acceptance of data use for public

benefit. The vignettes systematically varied key parameters of Contextual Integrity (CI), such as actors, data types, and transmission principles. The survey gathered responses from 1,682 participants, with approximately 500 respondents from each country. The findings revealed notable cross-national differences: respondents in Germany showed a marked reluctance to share data, particularly concerning certain transmission principles, while participants in the UK expressed predominantly negative views, driven by a strong preference for greater individual control over their personal data.

Challenges and Lessons Learned: The study uncovered substantial variation in responses across the different CI parameters, with this variation largely shaped by country-specific factors. This highlighted the complex interplay between national context and privacy norms, underscoring the challenge of designing vignettes that are both contextually meaningful and methodologically comparable across countries. The findings emphasize the importance of integrating cultural, legal, and institutional factors when applying CI in cross-country research on data practices.

Future Work and Research Directions: The findings suggest that CI offers valuable tools for uncovering context-specific differences in privacy perceptions both within and across countries. Future research should further develop comparative approaches that account for the *meso* level—capturing the role of institutions, communities, and organizations that shape data practices and expectations. A key direction will be the integration of CI with analyses at the *micro* level (individual attitudes and behaviors), the *meso* level (social structures and intermediaries), and the *macro* level (broader legal, cultural, and political frameworks). This multi-level integration will enable a more comprehensive understanding of how privacy norms are formed, contested, and negotiated in different national and institutional contexts.

Q&A Summary

– Q1: Interested in the meso level — where can we situate social marginalization within these levels? Answer: Social marginalization can occur at all levels of analysis. For example, it may arise at the macro level through institutional structures and national policies, at the meso level through organizational and community practices, and at the micro level through interpersonal relationships and individual interactions. These levels interact in shaping experiences of marginalization.

– Q2: The relationship between macro, meso, and micro levels seems hierarchical. Do you see any way to map between those levels? Answer: While these levels can appear hierarchical, they are in fact interdependent. For example, the doctor–patient relationship illustrates how macro-level healthcare policies influence meso-level organizational practices and, in turn, shape micro-level individual interactions. Some phenomena may pertain mainly to a single level, but there are clear correlations and dynamic connections across levels.

– Q3: You used a non-probability sample — can you speak to potential biases this introduces? Answer: Since the sample was recruited online through a German commercial provider, quotas were applied to enhance representativeness. Nevertheless, the sample may be biased toward individuals who are more

technologically literate than the general population. Given the experimental design, the thresholds for drawing inferences are somewhat lower, but we recognize that a probability-based sample would provide stronger external validity.

– Q4: In terms of your approach, given different demographics, are respondents in different countries surveyed in English or their native language? How do linguistic differences relate to privacy perceptions, and what challenges did you face in formulating questions? Answer (Paper 1 Speaker): We chose to administer the survey in English across most countries because managing translations into numerous languages would have been impractical. However, for Latin America we plan to provide versions in Spanish and Portuguese, as we anticipate low response rates for English-only surveys in that region. Answer (Paper 2 Speaker): In our study, we deliberately avoided referencing specific institutions, such as the NHS, and instead used generic language to enhance cross-country comparability.

– Q5: Given the appeal of cross-country comparisons, how can we move beyond viewing privacy as merely a matter of individual preference, especially when consent mechanisms are justified by national differences? Answer: Contextual Integrity provides a useful framework here, as it highlights how individual preferences are shaped by the organization of social contexts, which differ across countries. For instance, family structures and expectations vary internationally, influencing the purposes, norms, and expectations that underpin privacy preferences.

– Q6: Your methodology demonstrates the statistical power to identify patterns. Is it possible to focus on a specific social domain, such as education or family, to explore the reasoning behind cross-national differences in norms — perhaps even drawing on historical sources, like ancient Japanese texts? Answer (Paper 2 Speaker): This type of inquiry could certainly be pursued through either qualitative or quantitative methods. Answer (Paper 1 Speaker): My work is grounded in statistical methods, but collaboration with qualitative researchers has already proven valuable in enriching the analysis through deeper contextual insights.

SYMPOSIUM CHAIRS

Gianclaudio Malgieri (eLaw, Leiden University; Brussels Privacy Hub)
Jo Pierson (imec-SMIT, Vrije Universiteit Brussel & Universiteit Hasselt)
August Bourgeus (imec-SMIT, Vrije Universiteit Brussel)

PROGRAM COMMITTEE

Noah Apthorpe (Colgate University)
Borja De Balle Pigem(Google)
Rachel Cummings (Columbia University)
Cathy Dwyer (Pace University)
Laura Drechsler (CITIP, KU Leuven)
Ralf De Wolf (imec-MICT-UGent)
Beatriz Esteves (Ugent-imec)
Seda Gürses (TU Delft)
Max Von Grafenstein (Alexander von Humboldt Institute for Internet and Society)
Johanna Gunawan (Maastricht University)
Emiram Kablo (Universität Paderborn)
Irith Kist (Data Protection Officer at the Netherlands Cancer Institute)
Frauke Kreuter (LMU Munich, Germany and at the University of Maryland, USA)
Priya Kumar (Pennsylvania State University)
Mainack Mondal (IIT Kharagpur)
Elisa Orrù (The Centre for Security and Society)
Madelyn Sanfilippo (University of Illinois at Urbana-Champaign)
Luke Stark (Western University)
Katherine J. Strandburg (New York University School of Law)
Vincent Toubiana (CNIL)
Andrew Trask (OpenMined)
Kirsten Martin (University of Notre Dame)
Joris van Hoboken (Vrije Universiteit Brussel, Belgium)
Laurens Vandercruysse (Vrije Universiteit Brussel)
Ine Van Zeeland (imec-SMIT-VUB, Universiteit Hasselt)
Primal Wijesekera (ICSI)
Ben Zevenbergen (Google)
Yixin Zou (Max Planck Institute for Security and Privacy in Bochum)

STEERING COMMITTEE

Marshini Chetty (University of Chicago)
Helen Nissenbaum (Cornell Tech)
Yan Shvartzshnaider (York University)

The Symposium Program

Monday	
9:00 AM	**Registration, Coffee and Refreshments**
9:45 AM	**Welcome**
10:00 AM	**Opening Panel**
Session 1: CI and Theory ***Chair: Ine van Zeeland (imec-SMIT)***	
11:00 AM	**From contextual integrity to contextual flexibility?** (full paper) Armen Khatchatourov (Université Gustave Eiffel)
11:15 AM	**A Minimally Just Framework for Digital Dignity: Unifying Contextual Integrity and the Capabilities Approach (**full paper) Kat Roemmich (University of Michigan), Florian Schaub (University of Michigan) and Kirsten Martin (University of Notre Dame)
11:30 AM	**Data Intermediaries and Emerging Data Economies: Exploring the Need for Evolving the CI Framework** Michiel Fierens (ULeuven Centre for IT & IP Law), August Bourgeus Vrije Universiteit Brussel) and Ruben D'Hauwers (Vrije Universiteit Brussel)
11:45 AM	**Contextual Vulnerability: Bridging Contextual Integrity with Power Theories (extended abstract)** Gianclaudio Malgieri (Leiden University)
11:55 AM	**Discussion (10 mins)**
12:10 PM	**Lunch**
Session 2: CI and Sociotechnical lens ***Chair: Ido Sivan-Sevilla (University of Maryland)***	

1:45 PM	**Synthetic Data and Privacy: generating reality, silencing controversy (extended abstract)** Paula Helm (University of Amsterdam), Benjamin Lipp (Technical University Denmark) and Roser Puja (University College London)
2:00 PM	**Intracommunity Online Harms as Contextual Integrity in LGBTQ+ Communities** Kyle Beadle (University College London), Mark Warner (University College London) and Marie Vasek (University College London)
2:15 PM	**Assessing contextual integrity through a socio-technological ethical approach in the context of responsible AI in public education** Marco Houben (UHasselt), Jo Pierson (UHasselt) and Rob Heyman (VUB)
2:30 PM	**Discussion (10 mins)**
	Setup buffer
CI Community Feedback session # 1 ***Chair: August Bourgeus Vrije Universiteit Brussel)***	
2:45 PM	**Integration of Contextual Human Rights-Based Approach and Data Autonomy** **Kyra Abrams (University of Illinois at Urbana-Champaign)**
	The Legal Effects of Risk to Rights and Freedoms in the EU: The Case of the GDPR **Tatiana Duarte (KU Leuven)**
	Putting OSINT in Context: how to regulate privacy in public **Amir Cahane (Hebrew University of Jerusalem)**
3:00 PM	**Feedback (10 mins)**
3:10 PM	**Break (20 min)**
Session 3: CI and Regulation reforms ***Chair: Pierre-Luc Déziel (Unviversité Laval)***	
3:30 PM	**Fostering a Market For Responsible Data Practices (use case)** **Noah Apthorpe (Colgate University), Eleanor Birrell (Pomona College), Travis Breaux (Carnegie Mellon University), Kirsten Martin (Notre Dame University), Rishab Nithyanand (University of Iowa), Sarah Radway (Harvard University), Yan Shvartzshnaider and Maximiliane Windl (LMU Munich)**

3:45 PM	**Bridging the transatlantic divide: combining the inductive contextual privacy approach with the deductive data protection approach (extended abstract)** Max von Grafenstein (Einstein Center Digital Future, Alexander von Humboldt (Institute for Internet and Society)
4:00 PM	**Discussion (10 mins)**
	Setup buffer
CI Community Feedback session #2 ***Chair: Elisa Orrù (Max Planck Institute CSL)***	
4:15 PM	**Privacy as Demarcation. In Search for a Common Concept from Private Sphere to Data Protection** **Nora Becker (TU Dortmund University)**
4:20 PM	**Position paper work in progress Dataprotection in chains** **Marie-José Bonthuis (University Medical Center Groningen)**
4:25 PM	**Discussion (10 mins)**
4:35 PM	**Panel: Reflections of the day**
5:00 PM	**Predinner break**
7:00 PM	**Dinner**

Tuesday	
9:30 AM	**Registration, Coffee and Refreshments**
Session 4: CI and Biometrics ***Chair: Jo Pierson (imec-SMIT, Vrije Universiteit Brussel & Universiteit Hasselt)***	
10:15 AM	**Re-use of personal health data by local authorities for public interest purposes (use case)** **Dorine Van Zeeland (Hasselt University - VUB-SMIT), Sofie Hennau (Hasselt University - VUB-SMIT) and Jo Pierson (Hasselt University - VUB-SMIT)**
10:25 AM	**Rethinking Regulatory Approaches to Neuroprivacy: A Contextual Integrity Perspective (extend abstract)** Margot Hanley (Duke University)
10:40 AM	**A Contextual Integrity Approach to Genomic Information: What Bioethics can learn from Big Data Ethics (extended abstract)** Nina de Groot (VU University Amsterdam)
10:55 AM	**Discussion (10 mins)**
	Setup buffer
Session 5: CI and Standards ***Chair: Kirsten Martin (University of Notre Dame)***	
11:10 AM	**Privacy in Dense Street Imagery: From Face Blurring to Appropriate Flow of Spatio-Temporal Information (use case)** **Hauke Sandhaus (Cornell University), Matt Franchi (Cornell University), Madiha Zahrah Choksi (Cornell University), Severin Engelmann (Cornell University), Wendy Ju (Cornell University) and Helen Nissenbaum (Cornell University)**
11:20 AM	**Web Privacy based on Contextual Integrity: Measuring the Collapse of Online Contexts (extended abstract)** Ido Sivan-Sevilla (University of Maryland) and Parthav Poudel (University of Maryland)
11:35 AM	**Metadata standards: contextual enforcement of personal data protection in an automated world (full paper)** Louise de Bethune (KULeuven, CITIP and State Archives Belgium)

11:50 AM	**Discussion (10 mins)**
12:00 PM	**Lunch**
Session 6: CI and Surveillance ***Chair: Ralf De Wolf (imec-mict-Ugent)***	
1:30 PM	**Contextual Integrity Use Case: Dense Street Imagery (use case)** **Matthew Franchi (Cornell University) and Hauke Sandhaus (Cornell University)**
1:40 PM	**Trawling publicly available personal data as a case of public surveillance – and the lessons unlearned (full paper)** Bilgesu Sumer (KU Leuven), Isabela Maria Rosal (KU Leuven) and Ezgi Eren (KU Leuven)
1:55 PM	**Discussion (10 mins)**
	Setup buffer
Session 7: CI and GenAI ***Chair: Severin Engelmann (Cornell Tech)***	
2:10 PM	**LLM on the wall, who *now*, is the appropriate one of all?": Contextual Integrity Evaluation of LLMs (extended abstract)** **Yan Shvartzshnaider (York University) and Vasisht Duddu (University of Waterloo)**
2:25 PM	**Contextual Privacy Perspectives of Generative AI Users (full paper)** Alisa Frik (ICSI) , Mada Alhaidary (King Abdulaziz City for Science and Technology), Julia Bernd (ICSI), Basel Alomair (King Abdulaziz City for Science and Technology) and Serge Egelman (University of California, Berkeley)
2:40 PM	**Discussion (10 mins)**
2:50 PM	**Break (30 min)**
Session 8: CI and User perceptions ***Chair: Gianclaudio Malgieri (eLaw, Leiden University; Brussels Privacy Hub)***	

3:20 PM	**Transatlantic Privacy Perceptions in the Age of AI and Digital Technologies Through the Lens of Contextual Integrity** Isabela Coelho and Frederic Gerdon
3:35 PM	**Integrating Contextual Integrity into Cross-Country Comparative Research on Acceptance of Data Uses (extended abstract)** Frederic Gerdon
3:50 PM	**Discussion (10 mins)**
4:00 PM	**Symposium Wrap Up**
	CPDP Openning Night
6:00 PM	**Keynote: Mireille Hildebrandt (Emeritus Professor, VUB) on the race towards Artificial General Intelligence (AGI), the Brussels Effect of the GDPR and AI Act, and the importance of privacy for constitutional democracy.** **Panel discussion** ***moderated by Gianclaudio Malgieri (eLaw, Leiden University; Brussels Privacy Hub)*** **Helen Nissembaum, Cornell Tech** **Bart Jacobs, Radboud University** **Cornelia Kutterer, Considerati**