Pam Dixon*

Group Privacy, Data and AI: Collective Forms of Privacy and Its Relationship to Technology and Policy Frameworks

Collective privacy refers to the privacy interests of a group of people. As AI systems have advanced in capacity to analyze and segment people into groups with predictable behaviors, collective privacy has become increasingly relevant. However, there is a governance gap: while some indigenous governance frameworks such as those of the Māori acknowledge a right to collective privacy, the majority of privacy laws effectuate privacy primarily at an individual level, not a collective level. Europe's GDPR, adopted in some form in most regions of the world, exemplifies an individual privacy approach. This paper defines group privacy and analyzes the complex socio-technical environments underlying the collective privacy gap. The paper examines key case studies highlighting diverse aspects of collective privacy: the Māori algorithm charter with the New Zealand government, the All of US genetic data biobank policies, and the European Court of Human Rights case Lewit v. Austria.

Keywords: *Collective privacy, group privacy, GDPR, Artificial Intelligence, genetic privacy, indigenous governance, Māori algorithm charter, Lewit v. Austria.*

* Founder and Executive Director, World Privacy Forum.

1. Introduction

This paper explores concepts and applications of privacy in the context of groups and proposes a definition of the term *collective privacy* or *group privacy* as "those privacy interests that are held by or applicable to a definable group of people." Collective privacy is emerging as an issue of note for several reasons, one of them being that gaps in protections for group interests in privacy are becoming more visible as technology advances. Specifically, the dominant global privacy norms that focus on individual privacy rights, when contextualized in a world increasingly suffused with high volumes of data, AI, and machine learning analysis which can create, impact, and predict groups [1] in many ways, is exhibiting systemic gaps regarding the protection of collective privacy interests.

Privacy as a theory and doctrinal matter regarding individuals and privacy-related rights ascribed to individuals has been written about extensively.[2] However, collective privacy has been underrepresented in the dominant scholarly literature both about privacy and about collectivity. [3] A critically important body of scholarly, legal, and other work on collective or group privacy does exist. The clearest affirmative articulations of collective privacy at this time may be found in work relating to indigenous groups globally, and within the national and subnational tribal frameworks across a range of jurisdictions. Important examples include the U.S. Indigenous Data

[1] The concept of a group has been studied in multiple disciplines, including mathematics, physics, and social science, among others. This paper utilizes Campbell's postulation of *entitativity* (1958), later validated and refined by Lickel et al (2001) as a primary theoretical basis for determining the quality of cohesiveness of a group. When a cohesive group is formed, Campbell found that it will exhibit a range of quantifiable characteristics that determine its proximate level of entitativity, or "groupiness." Entitativity and its contribution to this analysis of collective privacy is discussed in more detail in this paper. See text and footnotes 11-15.

[2] There is an abundant and excellent literature on the complex topic of the definition of privacy. See: *DeCew J.,* Privacy, Stanford Encyclopedia of Philosophy, 2018; *Gellman R.,* Fair Information Practices: A Basic History, 2025, <http://dx.doi.org/10.2139/ssrn.5348107> [12.11.2025]; *Bamburger K. A., Mulligan D.,* Privacy on the Ground: Driving Corporate Behavior in the United States and Europe, Cambridge: MIT Press, 2016; *Solove D.,* Understanding Privacy, Cambridge: Harvard University Press, 2008; *Solove D.,* Against Privacy Essentialism, GWU Law School Public Law Research Paper, 2025-19; *Allen A. L.,* Presidential Address, The Philosophy of Privacy and Digital Life, 93 Proceedings of the American Philosophical Association, 2019, 21-38.

[3] Collectivity is a broad topic with multiple branches of inquiry. Collective judicial action is analyzed, for example, in the large body of scholarship regarding Rwanda's Gacaca Court, which in the period from 2001 to 2012 processed almost 2 million cases related to the 1994 Rwandan genocide. See: *Megwalu A., Loizides N.,* Dilemmas of Justice and Reconciliation: Rwandans and the Gacaca Courts, African Journal of International and Comparative Law, 2010, <https://ssrn.com/abstract=1406863> [12.11.2025]. Collective bargaining is another large branch of inquiry; see: *Court de le A.,* Stabilising Collective Agreements in Continental Europe: How Contract Law Principles Reinforce the Right to Collective Bargaining, Oñati Socio-Legal Series, Vol. 9, No. 1, 2019. The extensive literature examining broader theories and practices regarding collectivity does not usually address *collective privacy* as this paper defines it. However the broader literature on collectivity is nevertheless an important aspect of understanding the ways collectivity may be expressed.

Sovereignty Network [4] and the Māori Data Governance Model, Te Kāhui Raraunga, and charter, Te Mana Raraunga Charter, among others. [5] [6] [7] [8]

In particular, the Māori literature and work around collective privacy is critically important as the ideas around collective privacy, and even the collective quality of certain data, is addressed directly. Kukutai explains that in the Māori model, collective rights may in some cases prevail over individual rights. She also notes that certain data have a "clear collective dimension," a category in which she includes DNA and genomic data, among other data types.[9] It is noteworthy that the Māori data governance framework Te Kāhui Raraunga, which is a formal treaty with the government of New Zealand, has specifically articulated collective privacy in the context of AI, delving deeply into how algorithms and other aspects of AI will be addressed in the Māori context.

2. What Constitutes a Group?

One of the challenges of collective privacy is definitional; ideas around collective or group privacy raise many questions about how the groups themselves are defined, or which groups would benefit from collective privacy protections, or how that could be fairly decided, and by whom. How to define a group is a foundational question that has to be addressed systematically when approaching the concept of collective

[4] Indigenous Data Sovereignty, or IDSov, is a significant movement across multiple jurisdictions and regions. Definitions about indigenous data sovereignty can vary regionally and culturally. Data sovereignty as it relates to collective privacy is the focus of this paper, however, the ideas of data sovereignty encompass much broader issues that extend beyond the scope of this paper. See: The Global Indigenous Data Alliance, <https://www.gida-global.org> [12.11.2025] .

[5] Te Kāhui Raraunga, <https://www.kahuiraraunga.io/maoridatagovernance> [12.11.2025]. See also Te Mana Raraunga Charter, <https://www.temanararaunga.maori.nz/tutohinga> [12.11.2025].

[6] For example, the Māori have distinct and well-developed concepts of collective privacy enshrined in their culture as well as tribal laws. The Māori consider privacy to be a collective right, to be effectuated collectively. There is a detailed and nuanced literature around concept of collective privacy for the Māori. This paper introduces the concept and develops it in contrast to the dominant individual concepts of privacy. For a detailed articulation of what indigenous peoples consider to be collective privacy, see, e.g., *Quince K., Houghton J.,* Privacy and Māori Concepts" in Privacy Law in New Zealand, 3rd ed., Thomson Reuters, Wellington, 2023, 43–136.

[7] This paper discusses the indigenous and multilateral literature regarding collective privacy in detail in the case study analyses in this paper.

[8] The Māori consider privacy to be a collective right, to be effectuated collectively. There is a detailed and extremely nuanced literature around this concept of collective privacy for the Māori. To begin to understand collective privacy, it is essential to understand the indigenous people's philosophy regarding collective privacy. See, e.g., *Quince K., Houghton J.,* "Privacy and Māori Concepts" in Privacy Law in New Zealand, 3rd ed., Thomson Reuters, Wellington, 2023, 43–136, <https://researchspace.auckland.ac.nz/handle/2292/67023> [12.11.2025].

[9] *Kukutai T.,* Indigenous Data Sovereignty – a New Take on an Old Theme, Science, Vol. 382, No. 6674, 2023. As quoted in the article, Kukutai explains collectivity in indigenous frameworks: "All of the CARE principles (collective benefit, authority to control, responsibility, and ethics) speak directly to collective rights and responsibilities. The Māori data sovereignty principles go one step further, stating that in some data contexts, 'collective Māori rights will prevail over those of individuals.' " The CARE principles Kukutai references were crafted by GIDA, the Global Indigenous Alliance. See: Care Principles, GIDA, <https://www.gida-global.org/care> [12.11.2025].

privacy. To accomplish this, the research for this paper examined a broad literature on groups.

To begin with, an illuminative body of work exists in the scientific literature about what constitutes a group. This literature includes mathematical representations and concepts of groups, which date back to the 1700s. In abstract algebra, "group theory" simply means the study of groups, which in the mathematics context are complex algebraic structures.[10] Algebraic group theory has influenced physics as well as set theory, both of which contribute interesting ideas to the study of groups, group dynamics, and other group structures. Physics incorporates group theory structures widely, particularly in the context of symmetry or invariance.[11] Group theory is considered by some theoretical physicists as the dominant organizing principle of modern physics.[12]

A key scholarly literature in social science regarding groups is *entitativity*, which is a core term of art regarding what constitutes a group of people that are bounded together in some way. Sociologist Donald Campbell introduced the term in 1958 to describe groups that had certain common characteristics. The higher the entitativity of a group, the more cohesive and bound together the group. Lickel *et al* defined the term of art as it is now known, that is, *entitativity* is the "…degree to which a collection of persons are perceived as being bonded together into a coherent unit." [13]

Campbell proposed a set of criteria for determining if a group could be considered as an entity fit for analysis in the social sciences. These included interactivity, similarity, sharing the same goal, sharing a common fate, and having a psychological or physical boundary to the group.[14] Subsequent research has found that three of the components in particular are usually involved in entitativity: "…'essence' (the group members' similarity), 'agency' (the goals and the interaction between group members) and 'unity' (the cohesion of a group and the degree of the group importance).[15] Additionally, the groups that display qualities of entitativity tend to cluster into four types of groups, ranked from most to least entitative: intimacy groups

[10] *Dummitt D. S., Foote R. M.,* Abstract Algebra, 3rd ed., 2003. See Part I: Group Theory, chapters 1-6, Group Theory.

[11] *D'Hoker E.,* Mathematical Methods in Physics - 231B - Group Theory, Mani L. Bhaumik Institute for Theoretical Physics, Department of Physics and Astronomy, Course Notes, 2019, <https://www.pa.ucla.edu/faculty-websites/dhoker-lecture-notes/graduate-courses/group-theory.pdf> [12.11.2025].

[12] Ibid.

[13] *Lickel B., Hamilton D.L., Wieczorkowska G., Lewis A., Sherman S.J., Uhles A.N.,* Varieties of Groups and the Perception of Group Entitativity, Journal of Personality and Social Psychology, 78(2), 2000, 223–246. See page 224 for the definition.

[14] *Campbell D. T.,* Common Fate, Similarity and other Indices of the Status of Aggregates of Persons as Social Entities, Behavioral Science, 1958, <https://doi.org/10.1002%2Fbs.3830030103> [12.11.2025].

[15] As quoted in: *Agadullina E. R., Lovakov A. V.,* Understanding Entitativity: Are There Real Differences between Approaches? Journal of the Higher School of Economics, 2017.

(such as family and friends), task groups, social categories (gender, race), and loose association groups (for example, people who like certain types of music).[16]

To explore collective privacy in depth across similar groups, this paper discusses and analyzes three case studies focused on groups that demonstrate high entitativity per Lickel *et al* and Agadullina *et al.* The first case study focuses on indigenous collective privacy frameworks, including the Māori algorithmic charter, a major part of the collective privacy literature. The second case study involves a large U.S. National Institutes of Health biobank called the All of Us program, which has set a goal of collecting 1 million genetic samples for research. The All of Us program undertook an extensive review in 2021 regarding the effectiveness of consent provisions under the current U.S. law to protect the privacy of DNA contributions made by U.S. tribal members. The findings of the NIH review raised extensive and complex issues, and noted that broad consent for genetic data donated to the All of Us biobank program would not provide effective privacy protections for tribal members under the existing law. The report raised the issue of what it called "identitativity" of an individual research subject to a specific tribal group, despite privacy protections and deidentification measures being in place.

The third case study involves a collective group of holocaust survivors who were liberated from the Mauthausen concentration camp in 1945 and who were still alive in 2016. A publication in Austria defamed these survivors as a collective group, and the survivors subsequently brought a case before the Austrian courts. The survivors were denied standing because they were seen as a collective group without individual privacy rights. This case was eventually brought before the European Court of Human Rights (ECHR). The ECHR's decision and arguments in this case study speak directly to important aspects of collective privacy and reveal stark gaps in protections for collective privacy, even in a country with strong data protection laws in place.

Prior to discussing the analysis of the case studies, it is essential to contextualize the discussion of collective privacy in the current technical, social, and legal contexts as applied within the dominant practices and laws today.

3. Collective Privacy and the Impact of AI and Machine Learning Ecosystems on Privacy and Data

The emergence of advanced forms of AI and deep learning[17] creates significant pressures on policies regarding the use of data broadly, and aggregated or deidentified data specifically. Regarding the application of AI to group concepts, there is already a

[16] *Agadullina E. R., Lovakov A. V.,* Understanding Entitativity: Are There Real Differences between Approaches? Journal of the Higher School of Economics, 2017.

[17] *Vaswani A., Shazeer N., Parmar N., Uszkoreit J., James L., Gomez A. N., Kaiser L., Polosukhin I.,* Attention is All You Need, arXiv:1706.03762v7 [cs.CL], <https://doi.org/10.48550/arXiv.1706.03762> [12.11.2025]. The paper was first presented at the 31st Conference on Neural Information Processing Systems (NIPS 22017), Long Beach, CA, USA. It is an influential landmark paper in the history of AI. See also: *Murgia M.*, Generative AI Exists Because of the Transformer, This is how it: Writes, Works, Learns, Thinks and Hallucinates, Financial Times, 2023.

body of extensive work. Entitativity criteria are already widely used as a core concept in sophisticated social research regarding groups;[18] entitativity research is also being applied in additional domains of research that stem from nascent areas of AI. For example, applying AI and deep learning-based research using the field of topological data analysis to the investigation of social group cohesion can be used to predict the composition and behavior of groups.[19] One exemplar in this area is research that combines entitativity with AI-enabled analysis to determine virtual and physical characteristics of high-entitativity groups and to forecast the impacts of these groups on others outside the group.[20] Large open data sets such as SALSA,[21] when combined with entitativity analysis results in rich and deep research about groups, many of which raise substantial ethical and privacy issues. With the advent of advanced reasoning Large Language Models or LLMs,[22] the ease of creating programming code to run entitativity or other group analysis against large datasets of individuals at scale has raised the importance of a systematic evaluation of the risks to collective privacy that can be seen emerging today.[23]

There is significant consensus-driven multistakeholder work that discusses in various ways the intersections of privacy and and advanced forms of machine learning and AI. These works identify risks and outline general principles. Important exemplars include UNESCO's Recommendation on the Ethics of Artificial Intelligence, which applies to all of its 194 member states.[24] OECD's AI Principles are also important. These principles were the first intergovernmental standard on AI to be published. The principles were developed by a consensus body of its member governments along with its formal advisory bodies, which include civil society, business, standards development organizations, and additional stakeholders. A group of AI experts were gathered by OECD in 2018 to engage with this process to ensure technical accuracy and depth. The OECD AI Principles were ratified in 2019 and updated in 2024.[25] However, while valuable and important, this early work by UNESCO and OECD does

[18] Bernado F., *Palma-Oliveira J. M.,* Tell me Where you Live…How the Perceived Entitativity of Neighborhoods Determines the Formation of Impressions About their residents, Frontiers in Psychology, 2022.
[19] *Liang C., Chen V., Shah J., Andrist S.,* Converting Spatial to Social: Using Persistent Homology to Understand Social Groups, ACM International Conference on Multimodal Interaction (ICMI), Canberra, Australia, 2025.
[20] *Bera A.,* Data Driven Modeling of Group Entitativity in Virtual Environments, VRST 2019, Tokyo Japan <https://arxiv.org/pdf/1810.00028> [12.11.2025].
[21] *Alameda-Pineda X.,* SALSA: A Novel Dataset for Multimodal Group Behavior Analysis, IEEE Trans Pattern Anal Mach Intell, 2016.
[22] Large Language Models or LLMs are architected utilizing transformer models. LLMs are often characterized by the exceptionally large datasets used to train the models. See Wikipedia entry "Large Language Model," <https://en.wikipedia.org/wiki/Large_language_model> [12.11.2025].
[23] In one example, a multitasking convolutional neural network was used to predict the Group Cohesion Score of groups of people using visual images of the group. *Gosh S.,* Predicting Group Cohesiveness in Images, 2019 International Joint Conference on Neural Networks (IJCNN), Budapest, Hungary, 2019, 1-8.
[24] Recommendation on the Ethics of Artificial Intelligence, UNESCO, 2022, <https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence> [12.11.2025].
[25] OECD AI Principles, 2019 (Ratified), 2024 (updated).

not incorporate a robust analysis of AI impacts on groups in regards to privacy specifically.

An early feasibility study from the Council of Europe's (COE) Ad hoc Committee on Artificial Intelligence, CAHAI, investigated possible elements of a legal framework on AI. In this study, the COE specifically discussed the impact of AI on groups, noting that groups may experience discrimination based on AI analysis. The conception of "groups" in the study was not differentiated according to group cohesion, and did not include a specific analysis of advanced AI techniques impacting group privacy, however, the study did consider utilizing anti-discrimination laws as a possible way of addressing group harms, where AI systems are being used to create new groups. Ultimately, the Council of Europe in its final version of the Framework Convention on Artificial Intelligence did not include group concepts, but the discussion of group action related to AI is still an important contribution.[26] [27]

Another important contribution by the Council of Europe is contained in its Recommendation on the protection of individuals with regard to automated processing of personal data in the context of profiling, where the Council included a discussion of AI and groups in this specific context, noting:

1 i-j:
"…High-risk profiling" may refer, inter alia, to:
…profiling operations that entail legal effects or have a significant impact on the data subject or on the group of persons identified by the said profiling;"

2.6:

"…Profiling must not result in discrimination against individuals, groups, or communities."

B. 78:

"…. AI applications should allow effective control, by the data subjects and groups concerned, of the effects of their applications on individuals, groups and society."

8.5:

[26] Council of Europe, Ad Hoc Committee on Artificial Intelligence (CAHAI), Feasibility Study, 17 December 2020, <https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da> [12.11.2025]. See for example Paragraphs 20, 25, and discussion in note 15 regarding discrimination. CAHAI was the forerunner to the CAI, which completed what became the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law. See note 26.

[27] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law, 5 September 2024.

> "The field of inquiry of supervisory authorities should be broadened to include collective and societal risks. Their opinions should mention such risks and their decisions should take them into consideration."[28]

The COE defined what it meant by AI, but it did not specifically define what constitutes a group, nor did it set out a specific definition of group privacy or collective privacy. It is an important contribution, but it does not provide a complete literature on the topic. The EU AI Act also discusses the concept of groups, noting in Article 5 specific prohibited practices regarding individuals and groups. Groups are not specifically defined, and the EU AI Act does not specifically address privacy.[29]

The most completely stated policy literature that addresses and defines collective privacy directly, including but not limited to the context of AI, is primarily written by or with indigenous peoples about tribal data and tribal data laws. This literature includes legal arguments that some tribal governments possess the authority to enact data privacy laws at the tribal level. The tribal laws define what constitutes tribal data. Tsosie states:

> "…federally-recognized tribal governments do possess the authority to enact laws at the tribal level. Although jurisdictional limitations may exist, tribal laws can help inform analogous federal and state policies governing data, for example, by defining what constitutes "tribal data" and what would be appropriate ways to secure tribal consent to collection, use or disposition of such data."[30]

These ideas and approaches can be seen articulated in a number of exemplars which articulate specifically what collective privacy is, including in the context of AI; one exemplar this paper already brought forward is the Māori Data Governance Model, Te Kāhui Raraunga, and charter, Te Mana Raraunga Charter. Another examplar comes from the First Nations Principles of OCAP, which establishes how First Nations'

[28] Council of Europe Recommendation of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Adopted by the Committee of Ministers on 3 November at the 1416th meeting of the Ministers' Deputies).

[29] EU Artificial Intelligence Act, Regulation – EU – 2024/1689. The EU AI Act is designed to funnel privacy concerns in AI to be addressed through other legislative and regulatory instruments, including the GDPR. The handoff of privacy between the EU AI Act and the GDPR is extremely complex. Notably for the topic of this paper, group concerns regarding *privacy* as defined in GDPR are not considered in the EU AI Act, which is why the AI Act is not further analyzed as a core topic in this paper. It bears stating here that in the GDPR, privacy is primarily effectuated at the individual level, not at the group level. In use case 3 in this paper, the analysis of Lewit v. Austria touches on the overarching articulation of rights at an individual level in EU legal instruments and the limitations of individual approaches in certain contexts. Because the EU AI Act does not address collective privacy, a detailed discussion of these issues vis à vis the EU AI Act and its interaction with the GDPR will be taken up in a separate paper that explores the topic further.

[30] *Tsosie R.,* Tribal Data Governance and Informational Privacy: Constructing 'Indigenous Data Sovereignty,' 80 Montana Law Review 229 (2019).

data and information will be collected, protected, used, or shared in Canada.[31] Despite these strong articulations of indigenous policy, the practical implementation of these policies remains a difficult challenge in the development and deployment of data governance policies, as well as deployment of AI tools and systems.

This indigenous literature regarding AI and collective privacy is immeasurably important. As discussed earlier in this paper, modern AI systems can be at odds with privacy rights generally, including emerging areas of collective privacy risks emerging in newer AI and machine learning analyses. Indigenous socio-technical approaches often stress privacy as a collective issue and not as only an individual issue; these policies comprise a core articulation of collective approaches to privacy today, as collective privacy is not yet a front-line discussion held in the dominant culture of privacy.

There is an additional body of literature developing around data, AI, and collective privacy which is being created by philosophers and technologists who do not generally reference indigenous concepts, rather they draw from their perceptions and analyses about the actions and impacts of technologies on privacy as a whole. The philosopher Alessandro Mantelero wrote about the opportunity that big data and advanced analytics provides for redefining and expanding the boundaries of data protection concepts to include group privacy rights. He writes:

> "The peculiar nature of the groups generated by big data analytics request an approach that cannot be exclusively based on individual rights. The new scale of data collection entails the recognition of a new layer, represented by groups' need for the safeguard of their collective privacy and data rights." [32]

The "new layer" Mantelero identified is an astute observation, and is substantiated by technical research in AI and entitativity.[33] However, current law that is focused on individual data rights has been constructed in such a way that collective data has been in many ways devalued as to its privacy importance. Notably, deidentified data sets are typically beyond the reach of much privacy law. This can introduce problems today when deidentified data is analyzed and/or scored and the results affect individuals. In addition, modern forms of AI can permit a variety of advanced analysis of data without deidentifying the data and without allowing anyone

[31] First Nations Information Governance Centre, *The First Nations Principles of OCAP*, https://fnigc.ca/ocap-training/.

[32] *Mantellerò A.,* From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era, 2017. Group Privacy. Philosophical Studies Series, vol 126. Springer, Cham. <https://doi.org/10.1007/978-3-319-46608-8_8> [12.11.2025].

[33] Research regarding high entitativity groups includes, for example, the definition of entitativity: *Lickel B., Hamilton D. L., Wieczorkowska G., Lewis A., Sherman S. J., Uhles A. N.,* Varieties of Groups and the Perception of Group Entitativity, Journal of Personality and Social Psychology, 78(2), 2000, 223–246. See page 224 for the definition. An example specific to AI includes: *Liang C., Chen V., Shah J., Andrist S.,* Converting Spatial to Social: Using Persistent Homology to Understand Social Groups, ACM International Conference on Multimodal Interaction (ICMI), Canberra, Australia, 2025.

to view, use, or disclose the identified data.[34] While this can be a potential privacy boon, the consequences to individuals can range from helpful to problematic. This kind of practice has meaningful implications in a world in which advanced forms of AI can achieve increasingly accurate analysis of deidentified and encrypted data which can then be applied at a group, household, or even individual level. The dominant privacy laws in place today typically favor individual privacy rights over collective privacy, and as such, often exempt deidentified data from privacy protections.

Mühlhoff and Ruschemeier articulate this problem in privacy as a consequence of predictive analytics and a lack of collective privacy protections, specifically calling their theory "predictive privacy." It is an intriguing formulation:

> "…We argue that the individualised concept of regulation, shaped by the dogma of fundamental rights, is unable to adequately capture the implications of predictive analytics. We show that predictive analytics is a problem of collective privacy and informal power asymmetries, and conceptualise the form of data power at work in predictive analytics as "prediction power". The unregulated prediction power of certain actors poses social risks, especially if this form of information power asymmetry is not normatively represented."[35]

The normative representation that is missing is that deidentified data is not typically seen as worthy of data protections. The underlying argument at the root of this perception is that collective privacy does not matter as much as individual forms of privacy. There is a basis in reality for these criticisms. For example, in the U.S., the Federal health privacy law, HIPAA, provides that protected health information regulated under HIPAA may be shared or sold if certain deidentification procedures and measures are applied. The HIPAA deidentification standard in place today dates back to the 1990s and is likely out of date in light of modern analytics and AI.[36] However, it is now a well-established practice and it would be extremely difficult to dislodge. Also in the U.S., the Fair Credit Reporting Act applies only to individuals. If, therefore, a risk score about a household uses broad demographic information and aggregate financial data without using regulated elements such as credit bureau data, Fair Credit Reporting Act rights do not apply.[37] The Court of Justice of the European Union has recently clarified certain aspects of data protections for pseudonymous

[34] *Nicholson W., Cohen G.,* Privacy in the Age of Medical Big Data, Nature Medicine 25, 2019, 37–43.
[35] *Muhlhoff R., Ruschemeier H.,* Predictive Analytics and the Collective Dimensions of Data Protection, 16.1 Law, Innovation and Technology, 2023.
[36] For example, HIPAA, the federal health privacy law, allows for the use of deidentified data when it meets certain criteria. An early foundational paper articulating how the technology was viewed at the time is: Sweeney L., Weaving Technology and Policy Together to Maintain Confidentiality. Journal of Law, Medicine & Ethics, 25, nos. 2&3, 1997, 98-110.
[37] Federal Trade Commission, Section 319 of the Fair and Accurate Credit Transactions Act of 2003: Fifth Interim Federal Trade Commission Report to Congress Concerning the Accuracy of Information in Credit Reports.

data, [38] however, direct or indirect individual identifiability of the data is still a key test of when data can be classified as personal data.[39]

The risk of reidentification of aggregate or deidentified datasets is shifting as compute power and analytical sophistication improves.[40] An additional challenge arises when data is analyzed while still deidentified, because this activity typically does not fall under current privacy laws that focus on individual rights. For example, large data pools can be analyzed and then scored using a variety of machine learning and AI techniques. The scores -- even though they contain no personally identifiable data -- can then be applied to neighborhoods, census blocks, or households.[41] Continuing this example, individuals living in neighborhoods scored as higher risk can be affected; this can occur even though the neighborhood score is an aggregate measure that did not use or reveal personally identifiable information.[42] While there can be regional variations of this process, a risk score when applied to a group of people, especially if individual data is held in the aggregate, may not be covered under any particular law. Meanwhile, aggregate data that is analyzed and scored can still act to categorize people, predict behaviors, and create a variety of impacts that can be meaningful in a range of ways, both positive and negative.

Analyzed from a purely technical point of view, AI analysis and scoring of deidentified or aggregate data (including aggregate medical data) is able to draw conclusions about groups of people. Yet the granting of individual privacy rights currently available in most privacy law does not appear to meaningfully assist the protection of collective privacy interests that might be present in some cases. This point is made eloquently by two Māori authors who writing about how non-indigenous privacy approaches differ from theirs:

> "There are discernible differences between Māori and non-Māori concerns about privacy. These different concerns were reflected in our different aspirations for the reform process. …. We contend that, while the new Act champions individualistic Western conceptions of privacy with little regard for collective

[38] ECLU:EU:C:2025:645, Case C-413/23 P, September 2025.

[39] Article 3 (6) of Regulation 2018/1725: "'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." See also Article 3 (1).

[40] *Sweeney L.,* You J. S., De-anonymizing South Korean Resident Registration Numbers Shared in Prescription Data*,* Harvard Journal of Technology Science, 2015, <https://techscience.org/a/2015092901/> [12.11.2025].

[41] Dixon P., Gellman R., The Scoring of America, World Privacy Forum, 2014, <https://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf> [12.11.2025].

[42] *Testimony of Pam Dixon regarding Data brokers and the impact on financial data privacy, credit, insurance, employment, and housing, before the United States Senate Committee on Banking, Housing, and Urban Affairs*, 2019, <https://www.banking.senate.gov/hearings/data-brokers-and-the-impact-on-financial-data-privacy-credit-insurance-employment-and-housing> [12.11.2025].

conceptions of privacy, Māori may nonetheless find privacy law useful to achieve certain ends…." [43]

It is true that collective interests do not appear prominently, or in many cases, at all in Western law. This is not in dispute here. What is in dispute is the effectiveness of existing dominant privacy laws in effectuating aspects of group privacy when considering certain privacy scenarios, including those involving AI systems.[44] Dominant privacy laws and norms do not sufficiently address what indigenous communities and others need to ensure that collective forms of privacy thought and policy at the tribal and other levels are incorporated and addressed. In addition, current privacy laws also do not sufficiently address need for collective privacy interests beyond indigenous communities.

4. Individual Privacy Rights and a Brief Background of the Evolution of Privacy Law

Some additional contextualization regarding the specifics of existing privacy law and norms here is useful before discussing the collective privacy exemplars, as this paper discusses specific elements of dominant and non-dominant privacy law.

The dominant expression of privacy norms today is expressed in the broad concepts of the European-based General Data Protection Regulation, or GDPR.[45] The GDPR did not originate from a policy vacuum — rather, it is the expression of a long process of development over time. Privacy has a well-defined, deep, and instructive history.

In the late 1960s, driven to a significant degree by rapidly developing information technologies, attention to data governance,[46] data protection, and privacy began

[43] *Houghton J., Quince K.,* Privacy and Māori Concepts" in Privacy Law in New Zealand, 3rd ed., Thomson Reuters, Wellington, 2023, 43–136, <https://researchspace.auckland.ac.nz/handle/2292/67023> [12.11.2025].

[44] Gucluturk O., How to Handle GDPR Data Access Requests in AI-driven Personal Data Processing, 2024, <https://oecd.ai/en/wonk/gdpr-data-access-requests> [12.11.2025]. Also see discussion of broad consent regarding human subject research in this paper.

[45] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[46] Data governance and privacy are related, however they are different in meaning. Even though these terms might be used in tandem, they are not interchangeable. Data governance is a comprehensive approach to the entirety of data of an organization or entitativity that ensures information is managed through the full data lifecycle. This can include data collection practices, data security, quality, documentation, classification, lineage, cataloging, auditing, sharing, and other aspects. Data privacy is a subset of data governance, and is best defined in context as forms of protecting either personal data, or the personal data of a group of people. An articulation of individual privacy may be seen in OECD's *Recommendation on Privacy* (the Fair Information Practice Principles) or in Directive 95/46/EC, 1995 O.J. (L 281) 31 and the General Data Protection Regulation. As discussed in this paper, while the overarching European conception of privacy is dominant in terms of legislation, there are other conceptions of privacy in other cultures. For example, community-based privacy norms

slowly, with small developments here and there around the world.[47] Fair Information Practices (FIPs),[48] the early core statement of data governance and privacy values started in 1973 in the United States, were restated by the Organization of Economic Cooperation and Development (OECD) in 1980,[49] and became the basis for many privacy laws and policies around the world.

Eventually, FIPs faded into the background, not because the policies were wrong, but because the general policies that served so well for so long were not specific enough to address ongoing developments in technology, industry, and government. To offer one example, FIPs did not call for privacy agencies, but countries quickly recognized the value of privacy agencies or data protection authorities, and the idea spread around the world. Data protection authorities function as enforcers of data protection and governance laws, and they help guide the implementation data governance ecosystems at the ground level effectively.[50]

Countries enacted different privacy laws beginning in the 1970s and 1980s. It did not take long before the differences and limits in these national laws created problems with international data flows. Europe begin to address these problems, and the EU, after some significant effort, adopted a Data Protection Directive in the 1990s.[51] The shortcomings of the Directive and the challenges with its implementation resulted in

articulated in the Maori approach, among others. In these cases, as discussed in this paper, privacy is seen as a community feature belonging to a group of people. See First Nations Information Governance Centre, *The First Nations Principles of OCAP,* https://fnigc.ca/ocap-training/(establishes how First Nations' data and information will be collected, protected, used, or shared); see also Te Mana Raraunga, the Māori Data Sovereignty Network, https://www.temanararaunga.maori.nz . For a general discussion of privacy, See Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on the books and on the ground,* 63 Stanford Law Review 247 (2011) (UC Berkeley Public Law Research Paper No. 1568385), <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1568385> [12.11.2025].

[47] The state of Hesse, Germany passed a federal law that regulated automated data processing in the public sector on October 7, 1970. (Bundesdatenschutzgesetz, or BDSG). In the same month and year, the U.S. passed its first major privacy law, the Fair Credit Reporting Act, which also is among the first laws to regulate machine learning. Other laws followed in the EU and the U.S. In 1981, the EU opened its Convention 108 for signature by EU members, and also by other countries. In the 1990s, the EU passed its landmark data protection Council Directive EU 95/46. More than 160 jurisdictions across the world now have some form of data governance/data protection legislation, mostly following the pattern of the second generation of EU 95/46, the EU General Data Protection Regulation. The uptake of the GDPR comprises a mature and nearly global regulatory footprint although significant differences in policy and implementation remain.

[48] *Gellman R.,* Fair Information Practices: A Basic History, Version 2.32 (July 2025), <https://bobgellman.com/rg-docs/rg-FIPShistory.pdf> [12.11.2025].

[49] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD (Feb. 12, 2002), <https://doi.org/10.1787/9789264196391-en> [12.11.2025].

[50] See generally Global Privacy Assembly, https://globalprivacyassembly.org, (the Assembly is comprised of the international data protection and privacy commissioners or authorities. They met the first time in 1979). See also Irish Data Protection Commission, https://www.dataprotection.ie; Data Protection Office Mauritius, https://dataprotection.govmu.org/SitePages/Index.aspx; Personal Information Protection Commission Japan, https://www.ppc.go.jp/en/; Office of the Privacy Commissioner for New Zealand (Te Mana Matapono Matatapu), <https://www.privacy.org.nz/privacy-act-2020/privacy-principles> [12.11.2025] (examples of the work of data protection authorities).

[51] Directive 95/46/EC, 1995 O.J. (L 281) 31.

its replacement by the EU General Data Protection Regulation[52] which has been enforced since 2018. Many other countries around the world now follow the EU privacy model in some manner.[53] There is little to no question that GDPR is normative. The GDPR forms the foundation for a nearly global set of data protection laws today.[54]

However, as privacy laws and institutions spread into the developing world, it became clear over time that solutions that seemed responsive in theory did not always work well in practice. Sometimes, ideas that worked in one context or jurisdiction or social context did not fit in others.[55] For example, GDPR-like legislation, with its focus on individual privacy rights does not always fit well in indigenous contexts, where privacy and data are often handled as community rights.[56] GDPR-like legislation has also been a difficult task for small island nations, who often have very small populations and may not have enough resources to launch a comprehensive data protection regime.[57] The data governance and privacy learning curve stretches over decades, and the various stakeholders in the data ecosystems are still learning.

A significant global conversation is underway in the data protection sphere regarding the relationship between the GDPR and AI. Among the many questions at

[52] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[53] Pam Dixon, research; John Emerson, data visualization and design, *Global Table of Countries with Data Privacy Laws, Treaties, or Conventions*, World Privacy Forum, June 2024, <https://worldprivacyforum.org/posts/countries-with-data-privacy-laws/> [12.11.2025].

[54] More than 165 countries or jurisdictions have passed either GDPR, or very similar legislation, or have a draft bill. See Dixon and Emerson, *Global Table of Countries with Data Privacy Laws, Treaties, or Conventions*, World Privacy Forum. For a detailed discussion of GDPR and its impact, See: Graham Greenleaf, *Global Data Privacy Laws 2023: International Standards Stall, but UK Disrupts,* Privacy Laws & Business International Report 8-15, UNSW Law Research Paper No. 23-50, (2023). See also: Graham Greenleaf, *Global Data Privacy Laws 2023: 162 National Laws and 20 Bills.* Privacy Laws and Business International Report (PLBIR) 1, 2-4, UNSW Law Research Paper No. 23-48, February 2023.

[55] Michael Pisa, Pam Dixon, Benno Ndulu, Ugonma Nwankwo, *Governing Data for Development: Trends, Challenges, and Opportunities,* Center for Global Development, November 12, 2020. https://www.cgdev.org/publication/governing-data-development-trends-challenges-and-opportunities.

[56] As discussed in this paper, there have been significant advances in regards to the data rights of Indigenous people. This extends to the rights of Indigenous people to develop their own methods of data governance, which can, depending on context, grant community-level privacy rights which operate substantially differently than individual privacy rights enshrined in the GDPR. These contextual differences have meaningful implications for AI governance tools and their use. See First Nations Information Governance Centre, *The First Nations Principles of OCAP*, https://fnigc.ca/ocap-training/(establishes how First Nations' data and information will be collected, protected, used, or shared); see also Te Mana Raraunga, the Māori Data Sovereignty Network, https://www.temanararaunga.maori.nz; see also United Nations, G.A. Res 61/295 art. 18 (Sept. 13, 2007) (provides Indigenous peoples' right to participate in decision-making in matters which would affect their rights, through representatives chosen by them in accordance with their own procedures, as well as to maintain and develop their own Indigenous decision-making institutions).

[57] Pam Dixon, research; John Emerson, data visualization and design, *Global Table of Countries with Data Privacy Laws, Treaties, or Conventions*, World Privacy Forum, June 2024. https://worldprivacyforum.org/posts/countries-with-data-privacy-laws/ . See in particular: Small Island Nations filter. The small island group of countries has notably low adoption of GDPR-like regulations.

hand are those interrogating whether the GDPR is fit for purpose regarding AI privacy challenges, or whether there should be new privacy regulations that focus only on AI or its subset issues such as generative forms of AI.

The pace of regulatory activity addressing AI contrasts with the development of data governance and privacy laws and norms, which took place over a long period of time. Certain advanced forms of AI, however, jumped to public and policy awareness quite rapidly in comparison to the pace of privacy regulatory activity. One example may be seen in the days and months following the launch of ChatGPT in November 2022.[58] ChatGPT and generative AI models captured the interest of many regulators. Discussions, proposals, and rules of varying quality for generative AI models resulted, and rapidly so.[59]

To date, the initial flurry of activity has resulted in the fairly rapid passage of many focused laws at the subnational level, for example, many jurisdictions have passed narrow legislation regarding generative AI, among other narrower topics addressing AI issues.[60]

The European Union's AI Act is the most significant comprehensive AI bill to be enacted thus far.[61] While most countries have not yet followed Europe's example yet, there is a great deal of activity and discussion around AI-related legislation and a great deal of discussion around individual privacy rights in the AI context.[62] It is worth recalling that various forms of machine learning have been used and regulated for many decades. Credit score regulations —addressing data inputs, algorithms, set points, and other aspects of machine learning — exist in some jurisdictions and have since the 1970s.[63] These early forms of machine learning regulations often include well-understood and familiar governance mechanisms, such as error correction, a formal dispute process, government oversight, and other forms of consumer redress. These established methods of governance of credit scoring are well-understood. The procedural, and administrative controls used in these types of regulations are international norms. But today these normative solutions to privacy challenges are not as effective within certain AI contexts. The new territory of advanced AI is much more

[58] *Introducing ChatGPT*, OpenAI, 30 November 2022, <https://openai.com/index/chatgpt/> [12.11.2025].
[59] See generally the OECD AI Observatory, particularly the *Global AI law and Policy Tracker,* AI Observatory, OECD, <https://oecd.ai/en/dashboards/policy-initiatives> [12.11.2025].
[60] In the U.S. as of 2025 all 50 states have introduced or enacted laws regarding AI. See National Conference of State Legislators, *Artificial Intelligence Legislation Tracker*. <https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation> [12.11.2025].
[61] EU Artificial Intelligence Act, Regulation – EU – 2024/1689. As mentioned in note 29, this paper does not analyze the EU AI Act's impact on collective privacy; while the EU AI Act does discuss groups in several specific contexts, for example, it prohibits discrimination in credit scoring, the discussion in the Act is not focused on privacy. The EU AI Act does not specifically address privacy, so it is not analyzed here as the focus is on collective privacy.
[62] *OECD AI Policy Navigator*, AI Observatory, OECD, <https://oecd.ai/en/dashboards/national> [12.11.2025]. See also: IAPP Global AI Law and Policy Tracker, IAPP. <https://iapp.org/resources/article/global-ai-legislation-tracker/> [12.11.2025].
[63] The Fair Credit Reporting Act in the U.S. is an exemplar of such a regulation. Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq.

uncharted, particularly in regards to how privacy itself is changing within AI ecosystems.[64]

One of the questions raised by the advances in AI is if the established methods of governance currently used in individual rights-based privacy-focused regulations and policies are going to be sufficient to address collective forms of privacy risks that are emerging, particularly in AI and machine learning ecosystems. Not all of the answers are fully developed yet, but it is becoming clearer that collective privacy is emergent as a new area that will need to be addressed. The case studies in this paper shine a light as to where key gaps are in the current system of privacy governance and raise key questions about how to begin thinking about this area of risk more systematically.

5. Case Studies in Collective Privacy

This paper examines three distinct case studies in collective privacy. The case studies were selected because the groups involved exhibit demonstrable entitativity, which is necessary to find case studies that are clear enough for an analysis.

The first case study focuses on indigenous collective data privacy rights, first broadly, then with a focus on the government treaty that establishes collective privacy for the Maori. This is a highly defined, high entitativity group, and the case study is focused on and legislatively defines collective privacy with specificity. The second case study is focused collective privacy and the biomedical analysis of genetic data, which includes another high entitativity group, that of the analysis of Native Americans' DNA in the context of a large U.S. genetic biobank. In this case study, there is an exceptional discussion of consent in the context of collective privacy and the failure of existing law to be able to protect the genetic data from reidentification. The third case study is of a holocaust survivor who was defamed as part of a collective group of survivors of the Mauthausen concentration camp; he sued on the basis that although the defamation was collective, that the privacy rights afforded to him by law should still apply because he was an identifiable member of the collective group. This case was heard before the European Court of Justice and was decided in his favor.

[64] A global review of AI governance tools and analysis of their effectiveness and fitness for purpose concluded that current privacy norms do not yet address the full range of the forthcoming problems related to privacy automation -- essentially machine oversight at scale – among other challenges. Kate Kaye and Pam Dixon, *Risky Analysis: Assessing and Improving AI Governance Tools - An International review of AI governance tools and suggestions for pathways forward*, World Privacy Forum, December 2023.

5.1. Case Study: Indigenous Collective Privacy Rights and Data Sovereignty

While most legislation today principally articulates privacy and related rights as individual rights, privacy also exists as a collective or community-based privacy right as well.[65] Group privacy can be found throughout the governance spectrum, from multilateral to national to tribal.

International Customary Law[66] provides significant indigenous rights to privacy and data sovereignty. The most important document is the United Nations Declaration on the Rights of Indigenous Peoples, (UNDRIP), which sets forth core rights of indigenous peoples to govern themselves.[67] Several governments also apply the same principles to AI governance.

Several articles of UNDRIP outline the key contours of collective rights, autonomy, self-government, and certain rights to privacy, among others:

> Article 4
>
> Indigenous peoples, in exercising their right to self-determination, have the right to autonomy or self-government in matters relating to their internal and local affairs, as well as ways and means for financing their autonomous functions.
>
> Article 7
>
> 1. Indigenous individuals have the rights to life, physical and mental integrity, liberty and security of person.
>
> 2. Indigenous peoples have the collective right to live in freedom, peace and security as distinct peoples and shall not be subjected to any act of genocide or any other act of violence, including forcibly removing children of the group to another group.
>
> Article 12

[65] For example, the Māori have distinct and well-developed concepts of collective privacy enshrined in their culture as well as tribal laws. The Māori consider privacy to be a collective right, to be effectuated collectively. There is a detailed and nuanced literature around concept of collective privacy for the Māori. This paper introduces the concept and develops it in contrast to individual concepts of privacy. However, for a detailed articulation of what indigenous peoples consider to be collective privacy, the original source material is essential to study. See, e.g., Khylee Quince and Jayden Houghton, *Privacy and Māori Concepts* in Stephen Penk and Nikki Chamberlain (eds) _Privacy Law in New Zealand_ (3rd ed, Thomson Reuters, Wellington, 2023) 43–136.

[66] Customary international law refers to international obligations arising from established international practices and not from formal written conventions and treaties. International Customary Law relevant to indigenous rights and privacy includes the United Nations Declaration on the Rights of Indigenous Peoples, (UNDRIP), which sets forth core rights of indigenous peoples to govern themselves. In national legislation, these ideas are set out in for example, the U.S. Federal Indian Law, Canadian law, and New Zealand law, among others.

[67] United Nations Declaration on the Rights of Indigenous Peoples, Resolution adopted by the General Assembly on 13 September 2007, 62/295.

1. Indigenous peoples have the right to manifest, practise, develop and teach their spiritual and religious traditions, customs and ceremonies; the right to maintain, protect, and have access in privacy to their religious and cultural sites; the right to the use and control of their ceremonial objects; and the right to the repatriation of their human remains.

Article 18

Indigenous peoples have the right to participate in decision-making in matters which would affect their rights, through representatives chosen by themselves in accordance with their own procedures, as well as to maintain and develop their own indigenous decision-making institutions.

Article 19

States shall consult and cooperate in good faith with the indigenous peoples concerned through their own representative institutions in order to obtain their free, prior and informed consent before adopting and implementing legislative or ad ministrative measures that may affect them.

In national legislation, these ideas are set out in U.S. Federal Indian Law, Canadian law, and New Zealand law, among others. Further, important policy literature written by indigenous people's addresses data held at the tribal level. Tsosie, a major contributor to this literature, argues that tribal governments possess the authority to enact data privacy laws at the tribal level to define what constitutes "tribal data." [68] This is a foundational issue that is highly relevant to AI and research, among other areas. Related issues are collective data ownership, collective privacy rights, and the collective application of ethical principles. These types of approaches can be seen, for example, in the U.S. Indigenous Data Sovereignty Network and the Māori Data Governance Model, Te Kāhui Raraunga. Another indigenous governance framework is the First Nations Principles of OCAP.[69] OCAP, (Ownership, Control, Access, and Possession) expressly establishes how First Nations' data and information in Canada will be collected, protected, used, or shared. Any AI standards development work in Canada should ensure that the OCAP principles are respected and that representatives from Canada's First Nations can participate in the standards development processes.

[68] *Tsosie R.,* Tribal Data Governance and Informational Privacy: Constructing 'Indigenous Data Sovereignty,' 80 Montana Law Review 229 (2019)

[69] *The First Nations Principles of OCAP*, First Nations Information Governance Centre, <https://fnigc.ca/ocap-training/> [12.11.2025].

In regards to AI specifically, the Māori crafted an important and influential policy literature, in which Kukutai et al explain that indigenous concepts of privacy are inherently collective. The New Zealand government works with the Maori to co-develop AI policy frameworks to be used whenever indigenous data or rights may be involved. New Zealand's approach to AI sets an important precedent. The structure of New Zealand's approach is set to make a potentially significant long term impact on global standardization models and efforts.

5.2. New Zealand Government's and the Māori's Data Governance Co-design Efforts

First, by way of background, New Zealand started early in its work on AI. In 2017, it established a Government Chief Data Steward (GCDS) role via mandate. New Zealand already has a body of work and practice regarding data stewardship.[70] The Chief Data Steward is role is filled by the Chief Executive of Statistics New Zealand (Stats New Zealand). The role has several functions: to set mandatory standards; to enable a "common approach to the collection, management and use of data across government;" and to "direct the adoption of common data capabilities."

The Chief Data Steward developed a Data Strategy and Roadmap,[71] provided leadership in developing transparency and accountability for AI in the government context,[72] created a broad Data Stewardship Framework, ~~work on open data,~~ and developed a cooperative framework collaboratively with the Māori.[73] This effort initially sought to ensure that work done regarding Covid-19 was respectful to Maori approaches. Subsequently, this work was extended further in AI and into and accountability and standards development processes in collaboration with the Maori.

Structurally, New Zealand's framework of data stewardship is inclusive and interdependent across the whole of government. New Zealand describes its data stewardship framework as including a range of roles with governance functions in New Zealand's data system, including the:

---

[70] Government Chief Data Steward Mandate, Office of the Minister of Statistics New Zealand, <https://www.stats.govt.nz/assets/Uploads/Corporate/Cabinet-papers/Strengthening-data-leadership-across-government-to-enable-more-effective-public-services/strengthening-data-leadership-across-government-to-enable-more-effective-public-services-redacted.pdf> [12.11.2025].

[71] *The Government Data Strategy and Roadmap*, Government Chief Data Steward, September 2021, <https://www.data.govt.nz/leadership/strategy-and-roadmap/> [12.11.2025].

[72] Algorithm Assessment Report, Stats NZ, 2018, <https://www.data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-assessment-report/> [12.11.2025].

[73] Māori Data Governance Co-design Review, Te Kāhui Raraunga, January 2021, <https://www.kahuiraraunga.io/_files/ugd/b8e45c_0b1a378da21c459eb4fb88dfbf6aea81.pdf> [12.11.2025]. See also: COVID-19 Lessons Learnt: recommendations for improving the resilience of New Zealand's government data system. Stats NZ Tatauranga Aotearoa, March 2021, <https://data.govt.nz/docs/covid-19-recs-report/> [12.11.2025].

- Government Chief Data Steward,
- Government Chief Information Security Officer,
- Government Chief Digital Officer,
- Government Chief Privacy Officer,

The Privacy Commissioner, Ombudsman, Auditor General, and Chief Archivist also have roles.

The Privacy Commissioner's role is defined in the NZ Privacy Act of 2020, which has 13 information privacy principles, and requires agencies to report certain data breaches to the Privacy Commissioner. New Zealand's privacy laws are aware of GDPR, and as such it qualifies as a modern data protection law, but the Act is not identical to GDPR and uses different terminology.

New Zealand's approach to algorithms, or AI and machine learning is progressive and inclusive. In 2018, New Zealand released its Algorithm Assessment report, which covered the practices of 14 government agencies.[74] It is among the earliest instances of a robust, mature discussion of data governance, management, standards, stewardship, open data, and privacy in the area of government use of algorithms. The 2018 report led to the July 2020 release of the first iteration of the Algorithm Charter for Aotearoa New Zealand by the Minister of Statistics.[75] The Charter is notable for its approach to providing for means of appeal of decisions informed by AI. New Zealand also released an initial algorithm toolkit in 2021 to implement the charter.[76]

As of 2024, the government of New Zealand has updated and expanded its AI-related materials in regards to its charter in an overarching toolkit, with its most recent update being 2023.[77] There are many features of the toolkit that are worth imitating, including the impressive list of signatories to the charter. These signatories specifically include the Ministry of Māori Development as well as other NZ Ministries.

Specific to indigenous-informed approaches to AI is the New Zealand Government's Algorithm impact assessment user guide.[78] The Guide offers a detailed discussion of New Zealand's relationship with the Māori. It reflects with specificity its commitment to honor the Māori approach to data and ensures the use of algorithms is consistent with the articles and provisions in its charter.

[74] Algorithm Assessment Report, Stats NZ, 2018, <https://www.data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-assessment-report/> [12.11.2025].

[75] Algorithm Charter for Aotearoa New Zealand, Stats NZ. July 2020, <https://www.data.govt.nz/assets/data-ethics/algorithm/Algorithm-Charter-2020_Final-English-1.pdf> [12.11.2025].

[76] Government Algorithm Transparency and Accountability, Stats NZ. March 2021, <https://www.data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability> [12.11.2025].

[77] Algorithm Charter for Aotearoa New Zealand, which includes foundational work from the following: Principles for the safe and effective use of data and analytics Government use of artificial intelligence in New Zealand. Trustworthy AI in Aotearoa - AI principles Open government partnership Data protection and use policy and Privacy, human rights, and ethics framework.

[78] Algorithm impact assessment user guide, New Zealand Government, Te Kāwanatanga o Aotearoa, December 2023, <https://data.govt.nz/assets/data-ethics/algorithm/AIA-user-guide.pdf> [12.11.2025].

The guide notes on p. 29:

"General guidance to meet the Partnership commitment in the Charter you should:

- incorporate te ao Mãori perspectives into the design and use of algorithms
- ensure algorithm development and use is consistent with Te Tiriti o Waitangi
- consider how Mäori data sovereignty will be maintained
- assess how algorithm use will impact iwi and Mäori.

Te ao Mäori acknowledges the interconnectedness and interrelationship of all living and non-living things via spiritual, cognitive, and physical lenses. This holistic approach seeks to understand the whole environment, not just parts of it. (This definition comes from Treaty of Waitangi/Te Tiriti and Mãori Ethics Guidelines for: Al, Algorithms, Data and IOT.)"

Further into the Algorithmic assessment user guide, Question 5.3 on page 32 notes that:

"Mãori data is not owned by any one individual, but is owned collectively by one or more whanau, hapu or iwi. Individuals' rights (including privacy rights), risks and benefits in relation to data need to be balanced with those of the groups of which they are a part. (This definition comes from https://www.temanararaunga.maori.nz/)
Mäori data sovereignty recognises that Mäori data should be subject to Mãori governance — the right of Mäori to own, control, access and possess Mãori data. Mãori data sovereignty supports tribal sovereignty and the realisation of Mäori and iwi aspirations. (This definition comes from https: // www.temanararaunga.maori.nz/)"

The express acknowledgement of indigenous approaches to data and AI by the government of New Zealand in its AI policy sets a critically important example for other governments to follow. It is possible to incorporate multiple points of view regarding data. It will be important to ensure that global standards development efforts take note of the indigenous approaches that are either formal guidance or law in other countries. Arguably, standards efforts would do well to look into informal guidance as well.

For AI standards and policy in the indigenous context, several national governments adopted UNDRIP as a matter of national law. For example, New Zealand is a signatory to UNDRIP and has formal agreements. In 2021, Canada passed an Act

respecting the United Nations Declaration on the Rights of Indigenous Peoples [79] This bill brings Canadian law into alignment with UNDRIP.

5.3. Case Study: Human Subject Biomedical Research and Collective Privacy: "Broad Consent" to Research Uses of Genetic Biobank Data May Not Covered Under the Common Rule or Other Health or Research Privacy Law

Human subjects of biomedical research may often have collective privacy interests in biobanks holding their biological or genetic samples and other data that is used in the aggregate for analysis in medical research. An important case study in this realm comes from a large biomedical research effort in the U.S. In 2015, the National Institutes of Health (NIH) in the United States launched a precision medicine initiative that sought to collect 1 million biospecimens for study.[80] [81] The NIH consulted with tribal stakeholders for its biobank project, and has publicly acknowledged tribal sovereignty. The NIH wrote a report about this engagement in 2023 [82] The report is groundbreaking in many ways, and contains an important articulation of tribal concerns. According to the report, "Through the consultation process, tribal leaders have expressed deep concern about the use of data for secondary (future) research…"[83]

Also in the report, the NIH specifically described group or collective privacy impacts, which in this case could stem from the ability to identify a tribal research participant as part of an identifiable group.

The NIH's response to this concern is important because it contains a rare discussion of the idea of "broad consent" and the secondary use of the data identified as belonging to a particular group in the context of deidentification. Deidentification, in the U.S. context, as discussed in this paper, typically creates exemptions from privacy law, even when genetic or biological data is involved, depending on the context. This exemption is particularly difficult when it applies to research that includes biological samples and the potential for genetic linking. This is a deeply nuanced and difficult area of policy.

[79] An Act respecting the United Nations Declaration on the Rights of Indigenous Peoples, Bill C-15, Parliament of Canada, <https://www.parl.ca/LegisInfo/en/bill/43-2/C-15> [12.11.2025].
[80] *All of Us Research Program,* National Institutes of Health, <https://allofus.nih.gov/about/faq> [12.11.2025].
[81] Gellman R., Dixon P., Privacy, the Precision Medicine Initiative, & the All of Us Research Program: Will Any Legal Protections Apply? World Privacy Forum, March 16, 2017.
[82] All of Us Tribal Engagement, NIH, <https://allofus.nih.gov/about/diversity-and-inclusion/tribal-engagement> [12.11.2025].
[83] *All of Us Research Program Tribal Consultation Final Report March 2021*, National Institutes of Health. March 2021, <https://allofus.nih.gov/all-us-research-program-tribal-consultation-final-report> [12.11.2025].

The NIH stated in its report:

"Broad consent and secondary research

All data and biospecimens provided through the research platform will be de-identified in compliance with the standards of the Common Rule, and All of Us does not plan to share any readily identifiable data or biospecimens. All of Us currently does not seek broad consent for secondary research as defined in the 2018 Common Rule. That type of broad consent is required only when the secondary use will consist of readily identifiable data and samples. Data types are deemed "identifiable" if there is a significant chance that the data, either alone or in combination with other data, would render the identitativity of an individual participant readily discoverable. In other words, identifiability is less about an individual data element than about the data in context. Nevertheless, certain information, such as a name or Social Security number, would be inherently identifiable. In addition, certain other data elements, such as narrative fields from electronic health records, where such identifiers are more likely to be featured, are deemed potentially identifiable and must be heavily altered before becoming eligible to be shared with researchers.

The discussion of identifiability at the individual level, however, does not take into consideration the concern over group identifiability. In most cases, creating definable groups within data is a crucial part of the research process. In some cases, allowing for subpopulations to be singled out can put these subpopulations at risk for stigma and discrimination. The All of Us Research Program actively works to prevent, to the extent possible, the conduct of any stigmatizing or discriminatory research with the All of Us resources. The program also acknowledges that some groups, communities, and other defined subpopulations, even where stigma or discrimination may be a risk, may wish to make their group, community, or subpopulation discoverable within the dataset in the interests of promoting research that could address health disparities. However, particularly where there are historical reasons contributing to elevated risk of stigmatizing or discriminatory research, All of Us will look for guidance from those groups, communities, and subpopulations, including Tribal Nations, for how to approach group identifiability and appropriate harm mitigation strategies.

The program recognizes that there is a concept of broad consent that is not fully accounted for by broad consent as defined by regulation. The program acknowledges that it is requesting broad consent from participants according to the conceptual interpretation, rather than the specific regulatory provision in the 2018 Common Rule." [84] [Emphasis supplied].

Among the privacy challenges in human subject research in large biobank contexts is that existing privacy protections that depend on the use of deidentification as a privacy-preserving tool do not always apply. Genetic identification of groups of

[84] *All of Us Research Program Tribal Consultation Final Report* March 2021, National Institutes of Health. March 2021, <https://allofus.nih.gov/all-us-research-program-tribal-consultation-final-report> [12.11.2025].

people is possible within deidentified datasets, depending on context. In the NIH study, the NIH admits that there is a risk of identifiability of biospecimens to a broader and identifiable group, and it acknowledges that existing Common Rule protections do not address this risk. This is noted in the statement: "The program acknowledges that it is requesting broad consent from participants according to the conceptual interpretation, rather than the specific regulatory provision in the 2018 Common Rule." [85] Broad consent, again, is particularly challenging policy issue, and it is essential to resolve the question of what to do with "broad consent" in the tribal context, as well as outside of the tribal context.

In addition to this risk, an additional challenge, is that the right to collective privacy will make it very challenging to protect in an environment saturated with AI processing of biobank data samples. These two trends interact with each so as to deeply exacerbate the challenges for effectuating either individual or collective privacy in certain biobank contexts. The NIH's use of the term "identitativity" to describe the risk biospecimens may have regarding identifiability to a particular group is helpful here, as it interacts with the literature on entitativity, particularly as seen in the Lewit case study which follows.

5.4. Case Study: Lewit v. Austria and the European Court of Human Rights Regarding Individual Members of Collective Groups

In July 2016, Mr. Aba Lewit of Austria filed an appeal of a claim for compensation related to a defamation case to the European Court of Human Rights,[86] alleging that his privacy rights had been violated when a group of concentration camp survivors that he was part of were collectively defamed by a right wing publication. The case was unusual in that the publication in question did not specifically name Lewit or any of the other former prisoners, rather, the publication named as a collective group the survivors who had been liberated from the Mauthausen concentration camp in 1945. The publication had described the concentration camp survivors in highly derogatory terms, including characterizing them as having participated in criminal activities.

Initially, in June 2016, a group of 8 former Mauthausen camp prisoners plus 2 others, a daughter of a deceased former Mauthausen prisoner and a former prisoner at the Theresienstadt concentration camp, brought a defamation case before the Graz Civil Court. The Graz Civil Court granted an interim injunction in August of that same year, which was upheld on appeal and also upheld by the Supreme Court. In February 2017 the proceedings were terminated by a court settlement which required the

[85] *All of Us Research Program Tribal Consultation Final Report* March 2021, National Institutes of Health. March 2021, <https://allofus.nih.gov/all-us-research-program-tribal-consultation-final-report> [12.11.2025].
[86] *Lewit v. Austria*, Application No. 4782 / 18, Judgment 10 October 2019).

publication to issue a retraction. Because Lewit was not a party to the June 2016 claim, he was not bound by this settlement.

In a separate proceeding, 9 of the 10 claimants from the initial defamation suit plus Lewitt filed for compensatory damages resulting from the defamatory article. The ECHR described the arguments the group of survivors made regarding their identitativity, or potential for identification as a member of a specific group, as follows:

"The claimants argued that in defamation cases against a group of people, it was decisive for the question of their legal standing that every individual belonging to that group was identifiable, even if not named personally - which was the case here. They reiterated that they had all been victims of the National Socialist regime, and had been imprisoned because of their origins, their beliefs or their faith. At the time of their arrest and/or deportation to the concentration camps, some of them had been children, and others political detainees. They had never committed any criminally significant acts, either before their imprisonment or after their liberation from the concentration camps."[87]

Despite these arguments, in September 2016, the Graz Regional Criminal Court dismissed the survivors' claims for compensation. The ECHR discussion of this fact noted that "…The decisive question for the court was whether an average consumer would individually recognize the claimants and would associate the defamatory allegations with them" (Para 21). The Criminal Court's specific argument was premised on the fact that in 1945 there were around 20,000 survivors who had been liberated from the camp, which in its judgment was too large of a collective group to allow for the identification of individual member of that group. The Austrian lower court essentially used an argument of privacy through numerical obscurity to deny standing to the individual members of the collective group.

It was Lewit who made an appeal of the Austrian court's decision to the Grand Court. In the appeal, Lewit argued that the suit was wrongfully decided, and that he was in fact identifiable because at the time, he was 96 years old and was one of only a very few survivors of Mauthausen still alive. As such, at the time of the article's publication he was identifiable by members of the local community as a Mauthausen survivor and thus was defamed by the publication's remarks about the group. The ECHR discussed this issue in its decision that: "The Court has held that any negative stereotyping of a group, when it reaches a certain level, is capable of impacting on the group's sense of identity and the feelings of self-worth and self-confidence of members of the group. It is in this sense that it can be seen as affecting the private life of members of the group (see Aksu v. Turkey [GC], nos. 4149/04 and 41029/04, § 58, ECHR 2012). The Court considers that similar considerations apply in the instant case, when it comes to the defamation of former Mauthausen prisoners, who, as survivors of the Holocaust, can be seen as constituting a (heterogeneous) social group." (Para. 46)

The ECHR also noted that in cases where groups were seeking damages for defamation that… "If the group consists of a large number of people, the domestic courts have generally found that individuals were not affected. However, in certain

[87] Id. At Paragraph 19.

cases the Supreme Court has accepted that members of larger groups were personally affected (see for instance judgments of 11 January 1978, no. 10 OS 196/77 and 29 June 2011, no. 15 OS 15q/10k.) (Para. 36).

The ECHR ultimately agreed with Lewit, and convicted the Republic of Austria for violating Article 8 of the European Convention on Human Rights, which protects private and family life. The court found that the lower Austrian courts had wrongfully dismissed the original defamation lawsuits brought by the Mauthausen survivors, and that the corresponding judgments were seriously flawed in their reasoning. The ECHR ruled that the lower courts should have properly evaluated the number of remaining survivors of the Mauthausen concentration camp in 2016, and whether the survivors could be individually identifiable.

The ECHR's judgment is now used in training activities for judges and candidate judges in order to increase sensitivity for cases with references to Austria's past. Abe Lewit died in November 2020 at the age of 97. He lived to see his case successfully decided in his favor.

This case study brings forward several critically important issues in considering collective privacy. Certainly a core issue is that the camp survivors in this case had to prove individual identifiability or impact at an individual level to be able to effectuate their privacy rights under European law. This was made very clear throughout the case. It was only in proving individual identifiability and impact that Lewit was able to successfully bring his case.

The Levit case further sharpens the question that was raised in the biomedical case study in this paper: that is, what is the risk that an individual has of being reidentified back to a particular group? How does this risk change with the entitativity of a particular group? Are there factors that increase or decrease the risk? This paper postulates that if there is a history of stigma or discriminatory actions against a definable group with high entitativity, then a potential for identitivity to that group can represent a risk in and of itself. This postulation raises many additional questions.

It is arguable that even at a high number like 20,000, that the Mauthausen survivor group had many pathways of vulnerability regarding identification to Mathausen and potential stigma. Hiding in a big crowd is not effective "privacy by obscurity" in every case. This was true for the Mauthausen survivors in their lifetimes, and it is also true for those living in a digitalized world. So, when should group privacy be defensible under privacy law? Only when the group is small? Only when there is the possibility of identification with the group?

The NIH in its report discussed identitativity as the test for potential stigma. If a test for the risk of identitativty of an individual back to a group to determine privacy risk can be taken as a hypothesis, then it is the identitativity created by the contextual relationship of an individual to a group that matters, and this may not be dependent on group size. Identitativity may occur in groups of many sizes. No matter what the questions may be, one thing is certain: Lewit was forced to prove his *identifiability* to

a group that had characteristics of high sparsity in order to effectuate his privacy rights.

While the Lewit case was properly decided given its parameters, it does highlight a meaningful gap in privacy protections; in a digitalized world, high-sparsity (or low numbers of group members) should not be the gauge by which a right to privacy is determined; this is because a potentially stigmatizing analysis that identifies group members can be accomplished at scale and quickly in today's digital ecosystems. The larger group of Mathausen survivors from 1945 onward may have had experiences of stigma even with the higher numbers of group members.

Regarding entitativity, two of the exemplars in this paper describe groups with high entitativity based on significant ethnic and tribal linkages. In the Lewit case, the group demonstrated high entitativity in that the group were bounded by their shared history as prisoners of the notorious Mauthausen concentration camp,[88] and then lived for many years to interact as survivors of that ordeal. The research on entitativity indicates that there are different types of entitativity, and groups can arrive at entitativity in different ways. The Mulhausen concentration camp imprisoned people from multiple ethnic backgrounds, including people of Romani origin, among others.[89] This leads to the reasoning that the uniqueness of the collective group of survivors, and their historic significance are among the key qualities of the group's entitativity. Without being able to interview the survivors, it is difficult to determine definitively what additional qualities may have added to the entitativity.

In 2016, when very few individuals were left of the original group, a question arises as to how the entitativity of this group may have changed over time. How did sparsity impact the entitativity of the group? Was the shared experienced of both a traumatic and historic nature the core of the entitativity of this group?

6. Conclusion

Today, the strongest protections in collective privacy includes those for tribal groups that have certain rights under UNDRIP, and may also have additional rights based on further laws, treaties, or agreements. The Māori, as discussed extensively in this analysis, have formal collective privacy rights through an agreement with the government of New Zealand. The NIH All of Us report identified something quite important, that even non-identifiable individuals, if they are able to be connected to a larger group with entitativity, may suffer from certain stigmas or discriminations by that associativeness.

Under the normative privacy thought that is enshrined in the majority of country-level privacy legislation today, it is primarily individuals who are granted certain privacy rights. As was well-stated and proven in the NIH report, "The discussion of

[88] *76 years later, we remember Simon Wiesenthal's liberation from Mauthausen*, Simon Wiesenthal Center, 6 May 2021, <https://www.wiesenthal.com/about/news/76-years-later-we-remember.html> [12.11.2025].
[89] Mauthausen Concentration Camp, Wikipedia, <https://en.wikipedia.org/wiki/Mauthausen_concentration_camp> [12.11.2025].

identifiability at the individual level, however, does not take into consideration the concern over group identifiability." The Lewit case before the European Court of Human Rights was decided in his favor because he could prove his identifiability as an individual and therefore was able to effectuate the rights afforded to him individually under the European Charter of Human Rights. The collective group of survivors of the notorious Mauthausen concentration camp did not qualify under the law at that time for collective privacy protections. The European Court of Human Rights did rule in Lewit's favor, and it wrestled in its decision with the conflict between individual rights of privacy and that in some situations group-related privacy harms may affect individuals.

The individual focus on current normative privacy law has been functional for many years and is useful. But an ocean of digitalized information and data about people and groups of people is now interacting with advanced versions of AI and machine learning which have capabilities to create groups, make inferences about groups, and apply these inferences, in some cases with particularity, rapidly, and at scale. AI is becoming an increasing part and parcel of many aspects of modern life. It is important to look at groups of people, and specifically at the issue of collective privacy and think broadly and widely about what privacy protections may be needed for groups, in what circumstances, and what that process might be.

There are significant questions that need to be asked and addressed in the context of collective privacy. Among the first of these questions is how can a group be meaningfully identified as rising to the level of needing collective privacy protections or rights? The concept of entitativity is helpful here, but more work is needed to respond to the question of what the NIH report terms "group identitativity." This is a term that is not used frequently in discussing privacy, but the NIH and Lewit case studies indicate that the issue of group identitativity needs to be discussed.

When does being part of a group – or being identifiable to a particular group - rise to importance regarding collective privacy needs? When, specifically, and in what contexts do collective privacy rights matter? This is hopefully a conversation that will be undertaken by as many stakeholders as possible and inclusive of the indigenous, technical, policy, legal, human rights, privacy, and other experts needed for providing inputs and analysis.

In looking for existing frameworks that might be used to address the challenging issues regarding group privacy, the history of indigenous peoples' and the longstanding, detailed governance philosophy and frameworks that exists around collective privacy is arguably among the most, if not the most, instructive and important governance that is already in place. The Māori approaches in New Zealand stand as important and specific exemplars of respectful and workable approaches, and the treaty that exists between New Zealand and the Māori provides precise language that can be studied in the collective privacy context.

The biobank context is an extremely challenging one. What protections will be needed as biomedical analysis becomes more and more capable? The tribal collective privacy gaps regarding broad consent have already been documented. Are there challenges for additional groups? Can these challenges be quantified so as to create solutions?

There are many lessons that can be drawn from what is now known about collective privacy. Lessons can be drawn regarding collective privacy from socio-technical challenges and approaches to solutions in the AI context, and there are also critical lessons to be learned in certain types of human subject research, particularly in biobanks. Fortunately, exemplars of existing policies in collective privacy in the indigenous context can provide a starting point.

The issue of collective privacy deserves substantial attention and research going forward, including assessing and addressing collective privacy risks from AI analysis and applications, and including learning from indigenous frameworks that are already in place. To leave this work undone would be to miss an opportunity to address a meaningful technical and philosophical shift that is developing in our time. The opportunity to address collective privacy risks and solve the problems these risks can present is one that must not be squandered.

Bibliography:

1. Declaration on the Rights of Indigenous Peoples, United Nations, (adopted 2 October 2007 UNGA Res 61/295).
2. Directive 95/46/EC, 1995 O.J. (L 281) 31 and the EU General Data Protection Regulation.
3. *Ahuriri-Driscoll A.,* Enacting Kaitiakitanga: Challenges and Complexities in the Governance, 2014.
4. *Callison C.,* Material Culture in Flux: Law and Policy of Repatriation of Cultural Property, University of British Columbia Law Review, Special Issue, 1995, 165-181.
5. *Campbell D. T.,* Common Fate, Similarity and other Indices of the Status of Aggregates of Persons as Social Entities, Behavioral Science, 1958, <https://doi.org/10.1002%2Fbs.3830030103> [12.11.2025].
6. *Coll T., Taylor J. (eds.),* Indigenous Data Sovereignty: Toward an Agenda, 2016.
7. Council of Europe, Ad Hoc Committee on Artificial Intelligence (CAHAI), *Feasibility Study*, 17/12/2020, <https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da> [12.11.2025].
8. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law, 5/12/2024, <https://rm.coe.int/1680afae3c> [12.11.2025].

9. Council of Europe, Overview of the Council of Europe Activities in the Field of Artificial Intelligence, <https://rm.coe.int/brochure-artificial-intelligence-en-march-2023-print/1680aab8e6> [12.11.2025].
10. Co-designing Māori Data Governance, (Stats NZ) Data.gov.nz, Fata toolkit, <https://data.govt.nz/toolkit/data-governance/maori/> [12.11.2025].
11. *Dixon P., Milanes V., et al.* The Twin Transition from a Global Perspective: Framing the Debate. Presentation of Preliminary Research regarding the Twin Transition - Summary Report from a Series of Global Roundtables. OECD Ministerial Meeting, Gran Canaria Span. World Privacy Forum and ADC tor los Derechos Civiles. 13/12/2022, <https://www.worldprivacyforum.org/wp-content/uploads/2022/12/Twin_Transition_Report1_WPF_ADC_13December2022_fs.pdf> [12.11.2025].
12. *Erueti A.,* the UN Declaration on the Rights on Indigenous Peoples: A New Interpretive Approach, Oxford University Press, 2022.
13. *Gonzalez C. G.,* Environmental Justice, Human Rights and the Global South, 13 Santa Clara Journal of International Law 151, 2015.
14. *Helfer L. R., Austin G. W.,* Human Rights and Intellectual Property: Mapping the Global Interface, Cambridge University Press, 2011, rev. 2017.
15. *Karjala D. S.,* Robert Kirkwood Paterson, Looking beyond Intellectual Property in Resolving Protection of Intangible Cultural Heritage of Indigenous Peoples, Cardozo Journal of International and Comparative Law, Vol. 11, 2003, 633.
16. *Kukutai T., Campbell-Kamariera K., Mead A., Mikaere K., Moses C., Whitehead J., Cormack D.,* Māori Data Governance Model Te Kāhui Raraunga, <https://tengira.waikato.ac.nz/__data/assets/pdf_file/0008/973763/Maori_Data_Governance_Model.pdf> [12.11.2025].
17. Maori Sovereignty Network, Te Mana Raraunga, Māori Data Audit Tool, <https://static1.squarespace.com/static/58e9b10f9de4bb8d1fb5ebbc/t/59152b7db8a79bdb0e64424a/1494559615337/Māori+Data+Audit+Tool.pdf> [12.11.2025].
18. Māori Data Sovereignty Network, Te Mana Raraunga, the <https://www.temanararaunga.maori.nz> [12.11.2025].
19. *Mercredi O.,* Aboriginal Languages Celebrated, Saskatchewan Indian, Vol. 22, no. 4, 1993, 8.
20. Model Development Lifecycle (MDL) Item 22, 13, <https://www.msd.govt.nz/documents/about-msd-and-our-work/work-programmes/initiatives/phrae/mdl-governance-guide-for-effective-operational-algorithm-decision-making.pdf> [12.11.2025].
21. *Ouden D. A. E., O'Brien J. M.,* Recognition, Sovereignty Struggles, and Indigenous Rights in the United States: A Sourcebook, University of North Carolina Press, 2013.

22. *Phillips J.,* Australia's Heritage Protection Act: An Alternative to Copyright in the Struggle to Protect Communal Interests in Authored Works of Folklore, Pacific Rim and Policy Journal, Vol. 18 no. 3, 2009, 547-573.
23. Presentation of Jong-Sung Hwang, President, National Information Society Agency on Korea's Digital Bill of Rights and Evolution of Digital Inclusion and Presentation by Tahu Kukutai, Māori Data Governance Model, Data for Self Determination, at OECD event: Presentation of Charter on the Values and Principles for a Digital Shared Prosperity Society: Digital Bill of Rights, The Government of the Republic of Korea, 2023.
24. Remarks of Terina Fa'agau Devin Kamealoha Forrest, Presentation for Privacy tutorial hosted by World Privacy Forum and WACV Conference: AI Governance and data protection: Problem solving for Computer Vision and more, WACV conference, Hawaii, 8/01/2024.
25. *Skogstad L.,* Whose Artificial Intelligence? Design Assembly, <https://designassembly.org.nz/2023/05/08/whose-artificial-intelligence-reflecting-on-the-intersection-of-ai-and-te-ao-maori/> [12.11.2025].
26. The Government of New Zealand, Te Ao Māori Framework, Te Anga Ao Māori, <https://www.hqsc.govt.nz/assets/Misc/Te_Ao_Maori_Framework_FINAL.pdf> [12.11.2025].
27. The Government of New Zealand, Te Ao Māori Framework Implementation Guide, <https://www.hqsc.govt.nz/assets/Misc/Implementation_guide_Te_Ao_Maori_Framework_FINAL.pdf> [12.11.2025].
28. The First Nations Principles of OCAP, First Nations Information Governance Centre, <https://fnigc.ca/ocap-training/> [12.11.2025].
29. *Tsosie,* Tribal Data Governance and Informational Privacy: Constructing 'Indigenous Data Sovereignty,' 80 Montana Law Review 229 (2019)
30. U.S. Indigenous Data Sovereignty Network, <https://usindigenousdatanetwork.org/resources/> [12.11.2025].
31. Visit to Costa Rica – Report of the Special Rapporteur on the rights of indigenous peoples, A/HRC/51/28/ Add.1, United Nations. Human Right Council Fifty-first session, 12 Sept - 7 October 2022, <https://www.ohchr.org/en/documents/country-reports/ahrc5128add1-visit-costa-rica-report-special-rapporteur-rights-indigenous> [12.11.2025].
32. *Walter M., Kukutai T.,* Indigenous Data Sovereignty and Policy, Routledge: London, 2020.