Journal of Law, Medicine & Ethics (2026), **54**, 2, 238–250
doi:10.1017/jme.2026.10259

CAMBRIDGE UNIVERSITY PRESS

Independent Articles

Beyond Individual Privacy: A Layered Diagnostic Model for Analyzing Genetic Data Governance

Ruoxin Su
Faculty of Law and Criminology, Vrije Universiteit Brussel, Brussels, Belgium

Abstract

Human genetic data are simultaneously deeply personal, familial, and strategically valuable, raising regulatory challenges that individual-centered privacy frameworks only partially address. This is highlighted by the recent high-profile bankruptcy filing by 23andMe, which triggered widespread public concerns extending beyond consumer privacy interests to potential national security risks. To address this, this paper proposes a three-layer diagnostic model for more comprehensive analysis of genetic data governance: (1) individual privacy as sensitive personal data; (2) relational and group (privacy) interests reflecting genetic data's shared nature; and (3) the state or strategic layer treating genetic information as a national asset relevant to public health and security. Drawing on comparative examination of select jurisdictions and critical review of scholarship, this integrated framework offers researchers, policymakers, and private actors a practicable pathway to navigate the complex governance challenges posed by genetic data.

Keywords: Genetic Data Governance; Privacy; Relational Interests; National Strategic Resource; Biosecurity

1. Introduction

In March 2025, 23andMe, a leading direct-to-consumer (DTC) genetic testing company based in the United States, filed for bankruptcy protection to facilitate a court-supervised sale.[1] Given that the company holds genetic data of around 15 million people, this incident triggered public concerns regarding the legal and ethical vulnerabilities inherent in such vast commercial genomic databases.[2] Although the company announced that it "has not changed how it manages or protects customer data" — and required any potential buyer to comply with its privacy policy and applicable data privacy laws[3] — customers, driven by anxiety about data custodianship, privacy security, and the uncertain fate of 23andMe, took concrete steps to protect their genetic information (most commonly by deleting accounts and personal data).[4] Initial concerns centered, understandably, on the individual privacy interests of millions of consumers of the company. Yet the discourse quickly extended beyond the individual, touching upon potential risks to biological family members whose genetic information could be revealed by a single individual's DNA sequence, and raising questions about the potential acquisition of this massive dataset by foreign entities, thereby invoking the government's national security concerns.[5] On June 30, 2025, a bankruptcy court approved the sale of 23andMe to TTAM Research Institute, a non-profit medical research organization founded by one of 23andMe's co-founders, which subsequently completed the acquisition in July and committed to perpetually adhere to the company's existing privacy policy while providing customers with choice and transparency regarding their personal data.[6]

This incident therefore provides a stark, real-world prompt for rethinking the dimensions through which we ought to analyze issues relating to genetic data governance in contemporary times. While human genetic data has emerged as a critical asset in many areas like personalized medicine, forensic science, and anthropological studies, legal frameworks have traditionally governed it almost exclusively through the lens of individual data privacy.[7] This conventional perspective, deeply rooted in data protection laws such as the General Data Protection Regulation (GDPR) of the European Union (EU), is increasingly challenged by the complex realities of modern genomics, where the data's value is simultaneously collective, strategic, and even geopolitical. Nevertheless, this lens relies heavily on the individual-centric perception and offers little possibility to extend to the relational and collective considerations concerning genetic data that are increasingly important in public discourse.[8] Though the characteristics of relational privacy, group interest, and national interests embodied by genetic data have been noted in the existing scholarship and some jurisdictions, it is necessary to bridge the critical gap between the multifaceted nature of genetic data and prominent individual-centric thinking through a new analytical approach integrating these dimensions.

This paper proposes and develops a three-layer diagnostic model for analyzing genetic data governance as its principal contribution. It aims to contribute to a relatively structured analytical lens for private actors, researchers, and policymakers to anticipate the multidimensional implications of genomic activities, such as data breaches, cross-border research collaborations, and international acquisitions involving genetic assets. To this end, this

Email: ruoxin.su@vub.be

Cite this article: R. Su. "Beyond Individual Privacy: A Layered Diagnostic Model for Analyzing Genetic Data Governance," *Journal of Law, Medicine & Ethics*, **54**, 2 (2026): 238–250. https://doi.org/10.1017/jme.2026.10259

© The Author(s), 2026. Published by Cambridge University Press on behalf of American Society of Law, Medicine & Ethics. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/jme.2026.10259 Published online by Cambridge University Press

paper employs a combined research methodology, including doctrinal analysis of primary legal instruments and case law (with particular emphasis on EU data-protection doctrine), critical engagement with secondary scholarship to identify conceptual gaps, and a targeted comparative review of regulatory practice in jurisdictions that exemplify divergent logics (notably emerging biosecurity concerns in the US and China). It is noted that this paper does not examine the EU's Member State laws in detail, as the focus is to abstract recurring governance patterns rather than to be exhaustive.[9] Also, the model deliberately remains descriptive rather than prescriptive, primarily built upon a comparative reading of existing legal and policy responses across prominent jurisdictions and existing scholarship.

The following sections of the paper proceed as follows. Section 2 develops the individual-privacy layer and emphasizes genetic data as sensitive personal data. Section 3 advances to the layer representing relational interests, focusing on the inherent familial and collective implications of genetic information. Section 4 explores the strategic national-asset layer and reconceptualizes genetic data as integral to public health and national security, drawing primarily on legislative developments of proactive biosecurity-oriented jurisdictions. Subsequently, Section 5 synthesizes these three layers into one analytical model, exploring possible tensions and conflicts between the layers, acknowledging the model's limitations, and suggesting its practical application in real-world scenarios.

2. Individual Privacy Layer: The Foundation and Its Limits

The first and most established layer is the individual-centric view, which usually treats genetic information as a sensitive form of personal data requiring heightened protection. This perspective forms the doctrinal foundation for many contemporary legal frameworks governing genetic data and serves as the essential starting point for analysis of other layers. This section will explore the robust, yet ultimately incomplete, legal basis for this view, drawing on EU data protection law and the jurisprudence of European courts, as well as existing scholarship.

2.1 Genetic Data as Sensitive Personal Data in EU Data Protection Law

GDPR stands as a cornerstone of the contemporary EU legal framework designed to protect individuals' data, which came into effect on May 25, 2018.[10] The GDPR's framework is built upon a set of core principles that govern the lifecycle of personal data: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, and accountability. Its conceptualization of genetic data is pivotal since its predecessor, the Data Protection Directive 95/46/EC,[11] did not provide a definition or specify the legal nature of genetic data. Although the Article 29 Working Party issued some opinion on genetic data in 2004, its recognition of the sensitive nature of genetic data remained implicit "considering the extremely singular characteristics of genetic data and their link to information that may reveal the health condition or the ethnic origin."[12] It is not until the GDPR's formal introduction of the definition of genetic data that genetic data is explicitly classified as a "special category of personal data," usually referred to as sensitive personal data, in EU law. These special categories of personal data, also including other types such as biometric data, data concerning health, and data revealing racial or ethnic origin, enjoy reinforced legal protection under the GDPR due to their inherent sensitivity in relation to fundamental rights and freedoms of individuals.[13]

The definition of genetic data in the GDPR adopts an explicitly individual-centric —or more precisely, a sample-owner-centric — approach. Under Article 4(13), genetic data is defined as "personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question."[14] Two observations could be made from this formulation. First, the genetic data protected by the GDPR are conceived as data derived from the analysis of biological material (such as chromosomal, DNA, or RNA analysis) of the data subject, rather than from biological material belonging to other persons (such as biological relatives whose genetic information is intrinsically linked). Second, the provision frames the unique physiological or health-related information as belonging to, and thus primarily concerning, that individual, while remaining silent about the ways in which such information may also implicate other data subjects or broader groups. As Kuru recognizes, a teleological reading confines GDPR protection of genetic data to the individual data subject — that is, data derived from and concerning that person — excluding other individuals from the protection.[15] This narrow focus highlights the constraints of an individual-centric framework when applied to the inherently shared nature of genetic information. For example, an individual's decision to undergo a DTC test may reveal pathogenic variants that are heritable and indicate an increased risk of certain cancers (e.g., BRCA1/2),[16] whereas an individual-only legal framing fails to adequately capture the downstream familial implications.

The GDPR imposes a general prohibition on the processing of sensitive personal data, including genetic data,[17] a rule that can only be lifted under a limited number of specific, conditional exceptions. These exceptions include processing for reasons such as "explicit consent," "substantial public interest," "public interest in the area of public health," or for "scientific or historical research purposes." Member States of the EU also retain a certain degree of discretion to introduce further conditions for the processing of genetic data.[18] These exceptions reflect a long-standing and inevitable tension between protecting an individual's fundamental right to data privacy and the pursuit of benefits for society as a whole. In the case of genetic data, this is most evident in the balance between individuals' genetic privacy and public health advancements derived from genetic research. The legal debate surrounding this balance is a central point of conflict, foreshadowing the need for a broader analytical model that extends beyond individual privacy.

In other EU data-related legislation, the definition of genetic data largely mirrors that set out in the GDPR,[19] maintaining an individual-centric approach that focuses narrowly on information revealing unique genetic characteristics derived from a person's own biological samples. The concept of genetic data as primarily implicating individual privacy is similarly enshrined in many jurisdictions around the world — such as the US, Canada, and the UK, where legal frameworks often situate genetic information within the broader category of sensitive personal data and emphasize the individual's right to control its use and non-discrimination. However, beyond this predominant framing, certain jurisdictions have begun to recognize that genetic data also raise concerns that extend beyond individual privacy — for instance, by implicating national interests and collective identities. These emerging perspectives, which depart from or supplement the traditional individual-centric view, will be examined in greater depth in Sections 3 and 4.

https://doi.org/10.1017/jme.2026.10259 Published online by Cambridge University Press

2.2. Jurisprudence of European Courts

The individual-privacy character of genetic data has long been recognized in the jurisprudence of the European Court of Human Rights (ECtHR or "the Court"),[20] although the Court's evolving case law has also addressed other dimensions of genetic information (see Section 3). Before the GDPR's formal definition, the ECtHR decided a number of cases concerning genetic information, often under varying labels, such as "DNA data," "DNA profile," "DNA information," or "DNA records."[21] The cases discussed in this section are purposively selected as illustrative, focusing on landmark or representative decisions of the ECtHR rather than as the output of a systematic review.

Particularly, the Court consistently held that the collection and retention of an individual's genetic data by public authorities constitutes an interference with their right to private and family life as protected by Article 8 of the European Convention on Human Rights (ECHR), which may be justified only if it is "necessary in a democratic society" for legitimate aims such as national security, crime prevention, or the protection of health.[22] In *Van der Velden v. The Netherlands*, considered the earliest case concerning genetic information, the Court found that the systematic retention of an individual's cellular material (which the court treated as a proxy for the genetic information contained within) and DNA profile is "sufficiently intrusive" to amount to an interference with Article 8 ECHR, given the potential future uses of such material beyond mere neutral identification.[23] In the following landmark *S. and Marper v. The United Kingdom* case, the Court described DNA information as having an "intrinsically private character," noting that the information extracted from an individual's cells is "highly personal" and can disclose sensitive facts such as health status.[24] Furthermore, in cases such as *Aycaguer v. France*, the Court has emphasized that prolonged retention — here, a forty-year period with an effective practical result of indefinite storage — is disproportionate and therefore cannot be justified as necessary in a democratic society.[25] Similarly, in *Gaughran v. the United Kingdom* and *Trajkovski and Chipovski v. North Macedonia*, the Court consistently held that the blanket, indefinite retention of convicted persons' DNA profiles without adequate safeguards "fails to strike a fair balance between the competing public and private interests" and thus exceeds the State's acceptable margin of appreciation.[26] Together, these decisions underscore the ECtHR's consistent recognition of the particular sensitivity of genetic data and its focus on proportionality, retention, and sufficient safeguards when public authorities process such information.

The Court of Justice of the European Union (CJEU) has likewise reinforced the individual-privacy character of genetic data, particularly in the context of Law Enforcement Directive 2016/680 (LED), which governs police and justice processing of personal data.[27] In its 2023 judgment in *V.S. v. Ministerstvo na vatreshnite raboti*, the CJEU held that genetic data falls within the special category of personal data subject to enhanced protection under the LED, and that the systematic collection of such data for police records is, in principle, incompatible with the LED unless the competent authority can demonstrate strict necessity and the absence of less intrusive means to achieve their objective.[28] The CJEU's subsequent ruling in *NG v. Direktor na Glavna direktsia 'Natsionalna politsia' pri MVR – Sofia* sharpened this principle, concluding that the indefinite or generalized retention of genetic data (for example, retention "until death") for persons convicted of offenses is contrary to the LED.[29] It emphasized that retention must be strictly necessary, limited in time, and subject to periodic review.[30] This decision also reinforces the core EU data protection principles of data minimization and proportionality. Both rulings demonstrate that the CJEU, like the ECtHR, regards genetic data as a highly personal and sensitive category of information, warranting stringent safeguards to protect individual privacy. Moreover, the CJEU's jurisprudence builds upon the principles established in the ECtHR, applying them directly to the framework of EU data protection law and thereby solidifying the legal position that genetic data's inherent sensitivity demands heightened protection and careful, limited use by public authorities.

Nevertheless, the jurisprudence of the two European courts, the ECtHR and the CJEU, remains premised on a strict one-to-one relationship between a person and their genetic information, a model that emerged before the full implications of genomic science were appreciated. This traditional framing, while providing a necessary baseline, overlooks the inherently shared character of genetic data and the cascade of consequences that a single person's data can have on others. Nevertheless, academic analysis suggests that these court decisions contain the seeds of a broader conception of privacy — one that recognizes collective and relational dimensions of genetic information — and thus provide a natural transition to the next layer of the model (see section 3).

2.3. Inherent Limitations

It should be noted that most of the reported cases of the ECtHR and the CJEU concern state action such as law enforcement, public health, or other government uses, whereas other parts of the paper also discuss private and research uses. State uses can give rise to particular harms — such as risks of genetic searches, criminal prosecution, or deprivation of liberty — that make strong individual protections especially salient in that context.[31] By contrast, private and research uses more commonly implicate risks of commercialization, re-identification, discrimination, and epistemic bias. Despite these differences, there are important overlaps (for example, re-identification risks and familial impacts) that call for both context-sensitive rules and cross-cutting protections. While a detailed analysis of these different contexts is beyond the scope of this paper, it is still necessary to recognize both the shared features of genetic risk and the context-specific weight, which should be taken into account when translating the layered model (as proposed in Section 5) into concrete policy instruments.

Although, as analyzed in Section 2.2, case law of these two European courts and the GDPR provide a robust foundation for individual privacy, they struggle to capture the multidimensional nature of genetic information. Recent work highlights a familial and relational dimension entailed by genetic information while often overlooked by individualism in law and bioethics, arguing for the insufficiency of exclusively relying on the data-subject model of autonomy.[32] This narrow focus reveals a critical gap in the law's ability to address other potentially important dimensions of genetic data than individual privacy, foreshadowing the need for reconceptualizing its nature through a legal lens.

Genetic information processing, which has been long believed to impose serious threats to the rights of the individual donor in ECtHR jurisprudence, may also bring certain groups into focus as subjects of processing, creating distinct collective interests that may justify recognizing groups as separate legal subjects of protection.[33] A central critique of the GDPR's individual-centric model is its failure to adequately protect the interests of these genetically related data subjects, or even entire groups. The GDPR's definition ties

https://doi.org/10.1017/jme.2026.10259 Published online by Cambridge University Press

genetic data exclusively to the individual from whom the biological sample is derived, ignoring the shared nature. As Hallinan and de Hert have found, significant legal technical difficulties would appear when extending the GDPR to genetic groups, such as the problem of defining and identifying groups that are genetically influenced, and the new form of interest conflict created by genetic groups that challenges the GDPR-shaped bilateral relationship between data subjects and data controllers.[34] Similarly, Kuru's analysis again emphasizes the GDPR's failure to provide an effective protection for genetic groups, despite the fact that some mechanisms like data protection impact assessment (DPIA) and right to compensation may offer ancillary protection to individual members of genetic groups.[35] However, such interpretation could also lead to ambiguous and contradictory outcomes the GDPR cannot resolve, given that these mechanisms remain designed around the individual data subject.[36]

Furthermore, existing data protection regulations tend to overlook the nuanced nature of genetic data itself, treating it as a uniformly sensitive and uniformly personal category. As pointed out by Rahnasto, such an approach ignores two distinct problems: (a) identifiability is context-dependent, given that many sequence elements are population-common or non-identifying on their own; and (b) sensitivity likewise varies, with much genetic information relating to benign, ubiquitous markers or functionally uninterpretable features.[37] This one-size-fits-all legal conception (for example under the GDPR), while providing a high degree of protection, can also be disproportionate and create unnecessary hurdles for beneficial activities like scientific research. Towards a more granular and dynamic approach for protection and governance, other potential dimensions need to be explored to enrich the legal understanding of genetic data, a task that the next section will undertake by examining the relational and familial dimensions.

3. Relational Layer: The Familial and Collective Interests Dimension

Based on the individual privacy aspect, the second layer of the proposed model seeks to address the inherent shared nature of genetic data, which is a distinctive and more complex characteristic compared to other types of personal data. While the individual-centric perspective remains dominant in the general legal understanding of genetic data, it reveals significant inadequacies given that one's genetic data also simultaneously implicates their family, ancestors, and descendants. A target review of existing literature (see Section 3.1) indicates that this relational dimension challenges and reconceptualizes the conventional notion of privacy, moving from an exclusive focus on the individual to a broader consideration of collective interests. Nevertheless, existing laws and jurisprudence rarely substantively recognize or engage with this dimension as an extension of individual privacy.

3.1. Relational Genetic Interests in Existing Literature

The very nature of genetic data challenges the legal concept of the autonomous and isolated data subject. In metaphors created by Knoppers and Beauvais for debates surrounding genetic privacy, the human genome is framed as the common heritage of humanity in the 1990s and genomic databases as global public goods in the 2000s, implying the conceptual limits of a purely individualist governance paradigm.[38] As a biological record of familial inheritance, one individual's genomic sequence and scientific results based on such information can provide significant insights into the health predispositions, ancestry, and even identity of their relatives.[39] Accordingly, one family member's decision to participate in a genomic database can implicate the entire family, since submitting a biological sample for sequencing and storage may effectively render the familial genome (or substantial portions of it) accessible to third parties without collective consent or control.[40] This is also the case where individuals publicly post identifiable genetic data, obtained from direct-to-consumer genetic test companies, to find relatives, join condition-specific communities, or facilitate research, and their kin lack any practical ability to prevent such revelations and access to these data by others.[41] De Groot points out that the individual informed-consent approach does not account for the shared nature of genomic information and its broader ethical and political implications on communities and genetically-related groups, and proposes a "genomics-specific contextual integrity approach" that is sensitive to group interests such as vulnerable and indigenous populations.[42]

It has been widely discussed that clinicians and researchers usually encounter moral dilemmas, particularly regarding whether to share potentially lifesaving genetic data with a patient's relatives over the patient's objections, and determining who holds lawful decision-making authority over the disclosure of post-mortem genomic findings that could have material implications for surviving biological relatives.[43] Although the relational character of genetic information has long been recognized in bioethics, the legal duties of clinicians are contested and legally nuanced. For instance, while US clinicians have traditionally been viewed as restricted from disclosing genetic risk information to relatives without patient consent under the Health Insurance Portability and Accountability Act (HIPAA), legal scholarship notes that multiple forms of provider-mediated direct contact are actually permissible under HIPAA to facilitate ethical obligations of family care and improve identification of clinically actionable risk.[44] Recent developments in other jurisdictions illustrate evolving regulatory response; for example, updated Australian privacy guidance now explicitly permits clinicians to collect contact details from patients and notify at-risk relatives where a serious genetic threat to life or health exists and obtaining prior consent is impracticable.[45] Taken together, these legal and ethical complexities and the expanding prevalence of predictive genomic information exacerbates tensions between individual privacy and relatives' health interests, which points to the need for clarified legal exceptions and well-defined professional responsibilities that permit appropriately direct disclosure in limited, preventable-risk circumstances.

Legal scholarship has begun to articulate this conceptual shift by distinguishing between different forms of collective genetic interests. Hallinan and de Hert, for example, propose the notion of a "genetic group" — groups that share common genetic architecture across multiple individuals — and divide it into two subtypes according to whether the group can manifest a collective personality to communicate and exercise collative self-determination.[46] The first subtype, "genetic class," maps onto readily recognized social or political groups whose members are typically conscious of their membership and may organize collectively (sometimes through legally recognized representative bodies, as with certain ethnic minorities).[47] The second subtype, "genetic category," denotes a grouping that lacks a distinct social existence, whose members may be unaware they share relevant genetic features and therefore cannot form a collective identity, organization, or channels of communication.[48] Although these subtypes differ in the degree of social and organizational autonomy, both raise collective interests

https://doi.org/10.1017/jme.2026.10259 Published online by Cambridge University Press

that merit legal protection. Genetic classes — by virtue of their social constitution and possible representation — warrant mechanisms that recognize collective agency and enable group-based remedies where data processing undermines members' self-development; genetic categories likewise require protective measures focused on preventing harms such as stigma, discrimination, and mischaracterization that can affect members as a whole even in the absence of an organized collective actor.[49]

Relatedly, Leib-Neri and Prince advance the concept of an "intimate genetic community" to capture genetic privacy shared by interconnected social groups, including (1) one's biological family, (2) one's ancestry group, and (3) cohorts defined by particular variants associated with specific conditions and diseases.[50] Recent literature on law-enforcement uses of genetic information has introduced the term "genometric data" to refer to personal data generated through specific technical processing of identification markers in the human genome that allow or confirm unique identification of an individual.[51] This concept departs from a strictly data-subject-centric framing (such as the GDPR's emphasis on the sample owner) because the markers relied upon may not necessarily originate from the individual being identified but can be used inferentially to identify or locate biological relatives. The attendant notion of "genometric data privacy" therefore reflects the joint interest of both an identified individual and their genetic relatives in protecting uniquely identifying genomic signals,[52] reaffirming the relational dimension of genetic interests within the family circle. Given the heightened potential for intrafamilial and social harms, scholars argue that law enforcement uses of genometric data, most notably familial searching, should be tightly circumscribed, employed only as a last resort, and subject to rigorous procedural and substantive safeguards.[53]

Genetic privacy is increasingly understood not merely as an individual interest but as encompassing collective stakes — such as claims of ownership, control, and non-interference — held by families and broader communities, while many of their members may not be fully aware of the interdependent risks posed by genomic disclosure.[54] The increasingly easy-to-access genetic testing and the aggregation of population-scale genomic datasets through big genetic data have transformed information that was traditionally viewed as private into a resource capable of yielding far more extensive inferences over time.[55] The volume of information that could be inferred in the future will also increase, concerning disease risks, phenotypic traits, hereditary conditions, and markers of ancestry not only about the sample-donor but also about others who share substantial portions of their genome.[56] From both legal and ethical perspectives, it creates a tricky problem to identify and determine the interests of which groups should be recognized and protected in coordination with individual interests. In the familial context in particular, protection and balance of individual's privacy and autonomy with the family's benefit-sharing rights and autonomy also becomes a key legal and ethical dilemma for policymakers and legislators.[57]

Some European scholars have proposed extending the GDPR's protections to encompass genetic groups, which, in turn, underscores the necessity to look beyond the aspect of individual privacy. However, this approach would pose difficult legal-technical problems like legal uncertainty, conflicts of interest, and disproportionate burdens, since the core concepts, principles, and mechanisms of the GDPR are designed around individual data subjects.[58] Given the inherently shared character of genetic information and the limits of the existing data-protection architecture, genetic data may constitute the GDPR's Achilles' heel, exposing doctrinal tensions unless focused and updated guidance clarifies whether and how group interests can be accommodated within the regime.[59] Voices from public health and bioethics echo these concerns. Scholars note that biobanks exemplify a classical public health dilemma where the governance of biobanking and genomic medicine remains anchored in individualist principles like informed consent, autonomy, and privacy, while public health issues have a necessarily strong collectivist orientation, making the reconciliation of individual rights and community claims unavoidable in public health genomics.[60] Moreover, bioethical critiques call for a more structural reform, moving beyond the model of discrete "private rooms" for individuals toward institutional architectures that create legitimate "family rooms" or communal places where familial and community interests are deliberatively represented and protected.[61] Taken together, interdisciplinary scholarship reinforces the case for a diagnostic framework that explicitly registers collective and relational dimensions of genetic data alongside individual rights.

3.2. Recognition of Relational Dimension in Current Frameworks

Although most contemporary frameworks have not fully formalized a comprehensive model of group genetic interests, several key international instruments and regional precedents have implicitly or explicitly recognized its existence, providing a "small but growing" body of legal foundation for this second layer of the model.[62]

At the international level, UNESCO's Universal Declaration on the Human Genome and Human Rights of 1997, the first global instrument to articulate ethical and legal limits on human genome research,[63] provides an early and concise precedent for recognizing the communal consequences of genetic science. Its Article 10 states: "no research or research applications concerning the human genome, in particular in the fields of biology, genetics and medicine, should prevail over respect for the human rights, fundamental freedoms and human dignity of individuals or, where applicable, of groups of people." Although it is non-binding and short on operational detail, the text offers clear normative guidance for treating certain genetic harms as implicating family- or group-level concerns rather than solely individual privacy.

The subsequent International Declaration on Human Genetic Data of 2003 elaborates the special status of human genetic data by recognizing its potential to have a "significant impact on the family … and in some instances on the whole group to which the person concerned belongs," and to possess "cultural significance for persons or groups."[64] Its Article 7 requires states and actors to guard against discrimination and stigmatization for the use of human genetic data, expressly extending the protection to individuals, families, groups, or communities; Article 14 requires the protection of the privacy and confidentiality of genetic data linked to "an identifiable person, family or, where appropriate, group." Taken together, these soft-law texts anticipate a relational dimension of genetic information and supply a normative obligation on states and researchers to weigh collective interests alongside human rights when designing research, consent processes, and governance regimes.

In Europe, early recognition of the relational character of genetic data appears in the Council of Europe (CoE)'s Recommendation No. R (97) 5 of 1997, which treats genetic data as "concerning the hereditary characteristics of an individual or concerning the pattern of inheritance of such characteristics within a related group of individuals," and emphasizes the importance of the quality, integrity, and availability of such data for the health of an individual's family.[65] It further advises that, absent appropriate domestic

https://doi.org/10.1017/jme.2026.10259 Published online by Cambridge University Press

safeguards, incidental or unexpected findings of genetic analysis should be disclosed to the sample donor where disclosure is unlikely to cause serious harm to relatives or others linked by descent.[66] The CoE's Additional Protocol to the Convention on Human Rights and Biomedicine concerning Genetic Testing for Health Purposes develops this relational dimension more concretely: it acknowledges the "particular bond that exists between members of the same family"; reiterates the prohibition on discrimination and stigmatization of individuals and groups on genetic grounds; and permits, under narrowly defined conditions, genetic testing of a person unable to consent "for the benefit of family members."[67] Together, these provisions illustrate an initial, albeit limited relational approach that, in certain circumstances, allows individual autonomy to be balanced against the health interests of the wider family unit. While the clinical context naturally foregrounds familial implications due to the direct management of hereditary disease risks, such relational concerns are not unique to medicine; rather, they also extend to other contexts such as DTC testing and research biobanks, driven by the inherently shared nature of the data itself.

The Article 29 Working Party (Article 29 WP), the predecessor of the European Data Protection Board (EDPB), likewise recognized the unique data protection challenges posed by genetic information and urged a perspective that is "more than merely individualistic perspective" in its early advisory capacity.[68] Its 2004 Working Document on Genetic Data observes that genetic information can disclose attributes both at the individual level and at a group level — encompassing blood relatives across generations and socially salient collectives such as ethnic communities — and suggests that this gives rise to a "new, legally relevant social group … namely, the biological group," including not only family members with kinship but also persons outside the family circle like gamete donors.[69] Article 29 WP further noted that this expansion of the relevant class of affected persons complicates the application of conventional individual data rights. Tensions can arise, for example, between a data subject's "right to know," whose exercise may have implications for genetically related persons, and relatives' "right not to know," where disclosure would intrude on their private life or cause psychological harm — particularly in respect of untreatable, serious genetic conditions.[70] As it recommended, a delicate and case-by-case balance of competing interests needs to be made to weigh the gravity and foreseeability of harm to relatives and proportionality in disclosure.[71] This also indicates that the context and sensitivity of risks need to be given more consideration in assessing relational genetic claims.

Notably, the ECtHR's case law also exhibits a tendency, albeit occasional, of recognizing the relational character of genetic information, though this has not been substantively developed.[72] Crucially, even where courts acknowledge these wider interests, the discussions of familial implications are frequently subsumed within judgments that ultimately revert to an expressly individual-level framing. To date, the Court has not adjudicated a case that specifically defends the distinct rights of genetic relatives as such.[73] In the landmark *S. and Marper v. the United Kingdom*, the Court nevertheless observed that biological samples and DNA profiles "contain a unique genetic code of great relevance to both the individual and his relatives," and recognized that such data can be used to establish familial links and to infer probable ethnic origin.[74] The Court, however, proceeded to assess the matter through the familiar lens of the individual's right to respect for private life under Article 8 ECHR, leaving discrete group interests and implications silent. Notably, a subsequent decision, *Gaughran v. the United Kingdom*, reinforced the point that indefinite retention of genetic data of convicted individuals is unacceptable in part because it can continue to affect persons biologically related to the data subject.[75] The Court in this case reiterates the highly sensitive nature of using DNA profiles to establish potential familial relationships, stating that such a capability alone is sufficient to conclude that retaining genetic data interferes with the Article 8 right of the individual concerned.[76]

By contrast, the CJEU has not produced a distinct "group privacy" doctrine for genetic data yet, while its existing case law acknowledges the broader proposition that disclosures about one individual can give rise to privacy intrusions for third parties who share the relevant relational ties.[77] The relational approach has found more explicit judicial recognition in some European states, notably England and Wales, where domestic judges have held that clinicians may owe a duty to consider the interests of a patient's genetic relatives when deciding whether to disclose health information that could prevent or materially reduce a serious risk of harm.[78] Although scientific and ethical literature has long acknowledged that an individual is not the sole stakeholder in their genetic information,[79] the two principal European Courts, the ECtHR and the CJEU, have so far refrained from developing an autonomous doctrine recognizing relatives' genetic interests. Even so, their reasoning, read together with national rulings, could still offer a focused jurisprudential lens for reassessing whether and how the right to privacy should be reconceptualized to address the particular challenges posed by genetic data.[80]

4. Strategic National Asset Layer: The Biosecurity Dimension

Beyond the interests of individuals, families, and communities, genetic data could also implicate distinct state-level strategic concerns. This leads to the understanding and reconceptualization of genetic data as a resource of public significance through the third layer, typically integral to a state's public health, economic competitiveness (notably in biotech and precision medicine), and national security. This framing does not necessarily displace or diminish individual privacy protections but supplements those protections through state power to manage and regulate population-scale genomic resources in order to safeguard collective interests. While the EU's approach has largely developed from an individual-centric data protection, comparative experience — most notably in jurisdictions that have adopted explicit biosecurity-oriented statutes and governance mechanisms (e.g., China and the US) — shows a growing tendency to treat genetic data as a matter of state-level importance. Beyond the major powers, assertions of sovereignty over genetic data are also visible in countries such as Mexico, South Africa, and India.[81] These commitments to collective or national genomic solidarity, however, have been widely debated by scholars, who caution that restrictive sovereignty claims may impede genomic and data sharing and, in turn, exacerbate existing data biases.[82] Moreover, genomic governance in some jurisdictions (e.g., the US, Canada, Australia) raises distinct tribal-sovereignty concerns for Indigenous communities involved in biomedical research.[83] These issues should be treated separately from, and may at times conflict with, broader national-sovereignty claims.

The notion of state sovereignty over biological resources is not something new, but has been explicitly enshrined in several international instruments like the Convention on Biological Diversity (CBD),[84] and the Nagoya Protocol on Access to Genetic Resources and the Fair and Equitable Sharing of Benefits Arising from their

https://doi.org/10.1017/jme.2026.10259 Published online by Cambridge University Press

Utilization (Nagoya Protocol).[85] The Nagoya Protocol establishes that states have sovereign rights over their natural resources, including genetic resources — and, subject to domestic legislation or regulatory requirements, access for utilization must secure "prior informed consent" of the state and agree to "mutually agreed terms" for benefit-sharing.[86] However, human genetic resources (HGRs) are explicitly excluded from the scope of CBD and the Nagoya Protocol, which focus on plant, animal, and microbial resources.[87] While human genetic research also involves issues of benefit sharing among states, the essential differences between HGRs and non-HGRs, notably the former involving fundamental rights like human dignity and privacy, determine that the logic of "sovereignty over biological resources interstate transactions" established by the Nagoya Protocol should not be applied to the former.[88] The prevailing bioethical position frames benefits from human genetic research as a form of common heritage of humankind, entitling society at large to share in those gains; and in practice, distribution is often mediated through a pragmatic fair-exchange arrangement between the healthcare industry and research subjects.[89]

The CBD (and its implementing instruments) supplies the conceptual foundation for contemporary notions of biosovereignty.[90] Whilst it is difficult to specify how far the principle of national sovereignty over biological resources embodied in the CBD and the Nagoya Protocol furnishes a conceptual blueprint for state control over HGRs, the connection between human genetic data and national security concerns has become markedly more pronounced in major global players such as China and the US. These jurisdictions have moved beyond a privacy-first approach to enact or propose assertive legislative and administrative measures that explicitly foreground biosecurity and state stewardship of genomic resources.

4.1. China's Regulatory Approach to Human Genetic Resources Under Biosecurity

China has been considered as a very consistent and assertive jurisdiction where HGRs including genetic data are explicitly recognized as a national strategic resource in law.[91] Its Biosecurity Law of 2021,[92] along with the 2019 Regulations on the Management of Human Genetic Resources,[93] consolidates a decades-long effort of policy and regulatory activities asserting state authority and control over genetic data. It should be noted that China's Biosecurity Law is dedicated to biological risks and governance of the country, covering HGRs, animals, plants, microorganisms, and other biological resources that may affect public health, agriculture, ecosystems, or national security.[94] Unlike the CBD and the Nagoya Protocol, China embeds HGRs within a broader biological security governance architecture that reaches beyond conventional public health.

China's Biosecurity Law expressly announces that the state enjoys sovereignty over its human genetic resources and biological resources. It establishes a comprehensive administrative licensing system that strictly regulates the collection, preservation, use, and transfer of HGRs, particularly in international scientific collaborations, whether for commercial purposes or research.[95] Notably, this framework issues many restrictions on foreign entities regarding access to the state's HGRs, prohibiting them from collecting or preserving HGRs within China and transferring the state's HGRs to entities outside China.[96] A key requirement for collaborative research activities using China's HGRs is that foreign entities must partner with a domestic Chinese entity under a government-approved license, and guarantee the substantial participation, full data access, and benefit-sharing interests of the Chinese entity.[97]

The rationale is explicitly tied to national security. This biosecurity-oriented approach is a direct reflection of China's "holistic national security" strategy, which views all domains, including political, economic, military, and biological, as interconnected and critical to state security.[98] Administrative controls, most visibly the stringent double security review system for important human genetic data and HGRs, function as the tools through which the state primarily exercises its sovereignty to prevent risks to public health, technological advantage, and national security.[99] Furthermore, the mandatory benefit-sharing and domestic-participation requirements also produce a protective economic effect by ensuring that scientific and commercial value generated from Chinese HGRs is at least partially retained or channeled through domestic actors. This is, however, worrying from the perspective of international scientific communities, who considered that such an expanded national control over genetic data would make research collaboration even more difficult.[100] While China is one of the clearest statutory examples of asserted biosovereignty over HGRs, comparable tendencies can be detected elsewhere. It has been noted that many jurisdictions' governance regimes for biomedical research, clinical genomics, and biobanking incorporate *de facto* assertions of state control over population-based genetic information,[101] albeit with varying emphases and legal mechanisms.

4.2. An Emerging Reactive Biosecurity Approach in the US

In the US, recent policy and legislative developments show a marked trend of elevating human genomic data, as a kind of sensitive personal data, to a national security concern, departing from a predominantly privacy-focused regulatory model. The most direct and immediate administrative measure is the Biden administration's Executive Order 14117 issued on February 28, 2024, aiming to address threats to the country's strategic advantages, national security, and foreign policy posed by the continuing effort of certain countries of concern to access Americans' sensitive personal data and US government-related data.[102] It explicitly lists categories such as personal health data and human genomic data within the scope and authorizes regulatory interventions to restrict or prohibit certain data transactions deemed to pose unacceptable national-security risks.

This Executive Order was implemented through rules issued by the Department of Justice that took effect on April 8, 2025, and targets human genomic data as the most sensitive category of information among the regulated categories.[103] While the "bulk threshold" for personal health data is set at 10,000 US persons, the threshold for human genomic data is dramatically lower, at more than 100 US persons collected or maintained. This lower threshold underscores the unique and disproportionate national security risk the US government attributes to this type of data, particularly the possible use of identifying population-based vulnerabilities for military purposes like developing bioweapons and the potential for re-identification when combined with other datasets.[104] Whilst it has also been noted that economic considerations prevail over military ones in the US, national security concerns exist over the transfer of human genomic data, as large-scale human genomic data together with enhanced AI capabilities could significantly strengthen a country's long-term advantages in healthcare and advanced technologies that are critical to national competitiveness.[105]

Parallel to executive action, congressional initiatives such as the BIOSECURE Act introduced in the 118th Congress focus on the biotechnology supply chain and the flow of citizen genetic data therein. The proposed BIOSECURE Act pursues statutory means to

https://doi.org/10.1017/jme.2026.10259 Published online by Cambridge University Press

prohibit federal agencies from contracting with or providing grants to certain biotechnology providers, notably Chinese biotechnology companies like BGI Group and WuXi AppTec that are deemed to pose a national security risk.[106] Whilst commentaries note that the practical effect of this initiative could force US biopharmaceutical companies to consider severing contractual arrangements with actual or potential targeted biotechnology companies in order to maintain their business relationship with the federal government,[107] the very rationale of this Act is the concern that certain foreign governments could utilize their own domestic data laws to compel these designated biotechnology providers to transfer US citizens' genetic data for any potential economic and military use. Accordingly, it seeks to cut off the flow of Americans' genetic data to foreign adversaries by controlling the instruments and services used in the US. In this sense the BIOSECURE Act complements the Executive Order as the former controls who collects and processes the data through economic coercion and supply chain restrictions, while the latter regulates what the types of data could leave the country and how.

Scholars observe that characterization of human genomic data as a national strategic resource by the US could be largely provoked by US-China geopolitical rivalry.[108] Whilst different from China's approach, which claims national sovereignty over all genetic resources, the US approach is best characterized as precautionary and reactive, responding to perceived strategic competition and national-security threats related to human genomic data, and thus narrower than China's. These developments also illustrate how national-security framing can materially reorient human genomic resource governance from an exclusive emphasis on individual privacy toward additional administrative controls that treat population-scale genetic data as strategic assets.

4.3. Relevant Initiatives in Europe

While the EU's position on genetic data remains predominantly rooted in the individual-centric philosophy of the GDPR, there are a few recent initiatives suggesting a subtle but significant shift in thinking. For instance, the 1+ Million Genomes (1+MG) initiative is designed to create a federated data infrastructure that allows for the secure sharing of genomic data for research and public health across the EU.[109] This represents a recognition that genomic data, aggregated at a continental scale, is a valuable asset for public health and economic competitiveness. The EU's characterization of genomic data as a strategic resource could also be indirectly traced to its strategy for data policy, primarily driven by economic concerns over data and legislative leverage in healthcare areas in the post-GDPR time, such as the creation of a European Health Data Space (EHDS).[110] While not as obvious and proactive as that of China or the US, the EU's recent moves signal a growing understanding of the collective and strategic value of genetic data, moving away from a fragmented country-by-country approach toward a more unified pan-European one.

The UK's approach, while not as legally prescriptive as those of China or the US, also reflects a growing awareness of genetic data as a nationally significant scientific and economic asset. Its Biological Security Strategy sets out a high-level framework to mitigate biological risks — whether they are natural, accidental, or deliberate — and to enhance national resilience to a spectrum of biological threats by 2030.[111] Although it does not explicitly single out human genetic datasets, it provides a policy backdrop that informs risk assessments and access controls for genomic resources. At the same time, a state-led push to develop population-scale genomic infrastructure, notably through initiatives like Genomics England[112] and the Genome UK strategy,[113] treats genomic data as core components of future healthcare and nationally significant research. While governance debates have foregrounded security and ethical concerns regarding foreign access to UK citizens' genomic data,[114] the UK has not formally designated genomics as "critical infrastructure" due to the existing strong legislation governing the healthcare sector.[115]

The divergence of these national frameworks underscores a critical geopolitical dynamic. The EU's model is founded on fundamental human rights, China's on state sovereignty and economic protectionism, and the US on the prevention of specific perceived threat. It remains unclear whether there will be an emerging geopolitical contest for state control over human genetic data, elevating it to the status of a strategic asset akin to rare earth minerals. However, regardless of the divergence, scholars worry that laws and policies treating genomic data as a national strategic resource could indeed pose additional obstacles to the development of globally accepted guidelines and international scientific collaboration, such as genomic commons, open access, and international data sharing.[116]

5. Synthesizing the Layers, Tensions, and Limitations

The analysis above demonstrates that the legal and ethical landscape of genetic data is profoundly multi-layered. No single paradigm, be it individual privacy, relational interest, or state strategic resource, can fully capture its complexities. This paper thus argues that a comprehensive analysis of any genetic data issue requires an integrated framework that considers all three layers as interrelated lenses (see Figure 1). A legal challenge in one layer, as seen in the 23andMe case, could inevitably trigger a cascade of consequences in the others.

The model places the three lenses in concentric (and somewhat overlapping) relation. The innermost layer is the individual-privacy layer, primarily built upon traditional data-protection doctrines, data subject rights, and the GDPR-style instruments that prioritize individual autonomy and informational self-determination. Surrounding that is the relational layer, representing family, kin, and collective interests that arise from the collection and processing of an individual's genetic data. The shared nature of genetic data sits at the core of this layer, surrounded by questions such as shared vulnerability, reciprocal obligations, and potential group harms. The outermost layer is the strategic national-asset (biosecurity) layer, considering that states may treat population-scale genomic resources and infrastructure as matters of public health, economic competitiveness, or national security. This architecture maps where existing laws and policies tend to primarily focus on their genetic data governance and, in turn, aims to recommend an approach to comprehensive thinking and assessment through all three layers. It should be noted that these layers are neither strictly hierarchical nor mutually exclusive but interrelated, as a single processing act may trigger more than one layer in different jurisdictions.

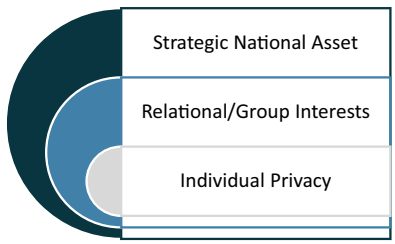


Figure 1. A layered diagnostic model for genetic data governance.

https://doi.org/10.1017/jme.2026.10259 Published online by Cambridge University Press

It should be borne in mind that tensions and interactions always exist between layers. For example, the individual layer privileges an individual's autonomous control over their own genetic data, while the relational layer recognizes that the same data simultaneously disclose information about living or future family members, giving rise to a consent dilemma in which one individual's decision to disclose or share genomic data can effectively make an irrevocable decision for biologically related others.[117] The robust individual consent mechanism may therefore leave relatives unprotected, and remedial measures like mandatory familial notification and multilateral consent can be operationally and ethically complex and worrying in some way. Importantly, this tension is rarely (and not easily) resolved by law, which typically defaults to the principle of individual control over their genetic privacy in most national data privacy laws. While certain ethical instruments like Canada's guidelines for health research involving aboriginal people attempt to bridge this gap by imposing community-consent requirements, it still remains distinct from and cannot substitute for the obligation of obtaining participants' individual consent.[118] The dynamics within this tension reveal that the question of how far one person's right to self-determination can extend when the subject matter is relational by its nature remains contested and context-dependent, calling for empirical, ethical, and legal coordination rather than a one-size-fits-all doctrinal solution.

Another example of such inter-layer tensions arises between the relational layer and the national-interest layer, where the former reveals collective societal benefit while the latter represents the national and sometimes geopolitical interest. The relational and public-interest significance of broad sharing of aggregated genomic data, for example through biobanks, has been widely recognized in public health advancement and innovation.[119] Conversely, a government might impose national security constraints, such as export controls and procurement restrictions, to limit cross-border sharing and foreign participation in research engaging with population-based genomic data in light of biosecurity and economic competitiveness concerns. As scholars note, additional obstacles may arise under those national policies treating genomic data as a national strategic resource, and the amount of genomic data available for shared use and access in various public and private databases as the commons will be accordingly impacted.[120] This tension could also be considered as an interaction between these two layers in the sense that the collective interests in the relational layer are reframed as national collective interests where the beneficiaries and acceptable uses of genetic data significantly change.

While this layered model aims to offer a relatively comprehensive analytical lens, it is very necessary to acknowledge the limitations, which should be noted in the real application. First, this model does not aim to provide a "one-size-fits-all" solution for considering the legal implications of issues related to human genetic data, nor does it supply a universal hierarchy for resolving conflicts among interests of different layers. Rather, it aims to map where the implications might arise and why certain layers cannot be ignored. This model is thus descriptive rather than prescriptive. Second, it should be recognized that the layer considering genetic data as a national strategic resource could inevitably carry a kind of legislative bias as it is constructed primarily based on contemporary regulatory responses from major geopolitical actors like the US and China. As discussed in Section 4, while other jurisdictions currently do not show a very explicit biosecurity motive over human genetic data, the regulatory response in the US and China has demonstrated that such strategic national interests have become sufficiently institutionalized to qualify as a legal layer of governance. Third, this model requires dynamic updating as advancing technologies continually alter the risk profiles and governance requirements of genetic data. Moreover, along with the trend of legislative developments and geopolitics in other jurisdictions, layers of this model, particularly the one that reveals the character of a national strategic resource, might need to be revisited or reconceptualized in the future.

Even so, given its comprehensive and cross-jurisdictional nature, this layered model offers significant practical utility as a diagnostic tool for organizations operating in the complex global genomics ecosystem. It offers a structured framework for analyzing potential governance risks that transcend specific national boundaries. Key beneficiaries would include private DTC genetic testing companies operating across multiple markets, international collaborative research consortia (for example involving biosciences, anthropology, and other disciplines using human genetic data), and biopharmaceutical companies managing global research and development pipelines. Under this model, data processing activities will be assessed not only through the lens of individual privacy, but also through the consideration of relational (community) interests as well as the macro-level dimension of national strategic interests.

To illustrate the practical application of this framework, consider a scenario where a DTC company intends to license a large aggregated dataset to a foreign pharmaceutical entity. Under the current individual-centric model, the company's primary compliance burden is on individual consent and rights. However, applying this proposed three-layered framework would expand the company's governance responsibilities to include a community impact assessment to prevent collective stigmatization or discrimination (Layer 2) and, probably, a review of national interests to evaluate biosecurity risks associated with bulk data export (Layer 3). In doing so, this model enables organizations to anticipate potential conflicts between different layers and jurisdictions, thereby allowing them to proactively strengthen genetic data governance strategies and make them more resilient in order to mitigate risks arising from differing regulatory priorities.

6. Conclusion

Existing literature and legislative as well as policy developments in major jurisdictions have demonstrated that the conventional individual-centric paradigm for genetic data governance is no longer suitable in an era when such information is increasingly considered as a multi-layered asset with profound implications for families, society, and national interests. Just as the 23andMe bankruptcy illustrates, a single incident could be strong enough to trigger worries at different dimensions across the individual privacy right, relational and group interests, and national security. Particularly, the cross-boundary activities engaging genetic data, either commercial or non-commercial, and geopolitical dynamics would further intensify these worries.

Accordingly, this article proposes a layered diagnostic model to offer a relatively comprehensive analytical framework for genetic data governance and implication assessment (or reassessment), moving beyond the limitations of the existing widely perceived approach to individual data privacy protection. The foundational layer, primarily rooted in the historically abundant legal protection over genetic data through the individual privacy right, provides a necessary but insufficient starting point. The second layer is built upon relational or group interests carried by one's genetic information and highlights the shared and immutable nature of genetic information, which fundamentally challenges key issues like

https://doi.org/10.1017/jme.2026.10259 Published online by Cambridge University Press

individual consent and the right to know (or not to know) of other genetically related persons. The third layer reveals how major jurisdictions, driven by differing national interests such as biosecurity, geopolitics, and economic competitiveness concerns, are increasingly treating genetic data as a strategic asset, leading to a fragmented and ideologically diverse global governance landscape. By integrating these three perspectives, the model provides a diagnostic tool for a more complete legal and ethical analysis which acknowledges the complex and interconnected nature of genetic information and potential external forces impacting its governance other than its intrinsic nature (i.e., reframing genetic data as a national strategic asset by the state).

It should be noted that several limitations of this model cannot be ignored in practical application. It is in essence non-prescriptive and does not replace jurisdiction-specific legal analysis or supply a universal hierarchy for resolving conflicts among individual, relational, and state interests. Moreover, this model requires ongoing refinement or, if necessary, reconceptualization based on evolving global legislative, geopolitical, and technological changes, particularly for the state layer which is principally grounded in contemporary regulatory practice in major actors (notably the US and China).

While primarily descriptive, this three-layer model offers an analytical pathway for policy design in genetic data governance, rather than prescribing a one-size-fits-all legislative solution. For instance, policymakers can utilize it to identify where current frameworks may over-emphasize individual privacy while leaving relational or national-security risks exposed. This approach also facilitates the mapping of harms and interests across all three layers, allowing policymakers to assess the shifting weights of these interests in various contexts and develop more proportionate and context-sensitive instruments. Furthermore, as the strategic significance of human genetic data grows globally, this model provides a necessary lens to anticipate regulatory divergences. It helps stakeholders understand fundamental conflicts between jurisdictions with differing priorities (such as those prioritizing national assets versus individual rights) and guides cross-jurisdictional dialogue. By accounting for these distinct layers of concern, future policy development can advance toward a more holistic governance structure that reflects the uniquely multi-dimensional nature of genetic data.

Looking ahead, it is necessary for future research to explore the long-lasting tensions and interactions between these layers, such as the balance between the rising national biosecurity concerns and individual and group interests enjoyed over their genetic information, and the practical challenges of operationalizing the model in genetic data governance, such as refining the consent mechanism to integrate familial interests. What is for sure is that genetic data governance requires moving beyond a single-issue focus and embracing a multi-layered approach that reflects the true nature of genetic data as a shared, sensitive, and strategic resource.

Acknowledgements. This work is part of the author's doctoral research project at Vrije Universiteit Brussel, Belgium. The author wishes to express sincere gratitude to her supervisor, Prof. Dr. Paul Quinn, for his invaluable support and guidance throughout the writing of the manuscript. The author also wishes to express sincere gratitude to the participants of the Privacy Law Scholars Conference (PLSC) Europe 2025 for their constructive comments and feedback on an earlier draft of this work.

Funding. Open access funding provided by Vrije Universiteit Brussel under the open access agreement with Cambridge University Press.

Disclosures. The author reports there are no competing interests to declare.

Declaration of Generative AI Tools in the Writing Process. The author reports the use of Google's Gemini 2.5 and Gemini 3 models to improve the language and readability of this work, and subsequently reviewed, edited, and takes full responsibility for the content of this work.

Ruoxin Su, LLM, is a faculty member of Law and Criminology at Vrije Universiteit Brussel, Brussels, Belgium, and a doctoral researcher in the VUB Health & Aging Law Lab (within the Research Group on Law, Science, Technology & Society). Su has published on data privacy law, medical device regulation, FemTech, and related topics.

Reference

1. Juliana Liu, "Genetic testing firm 23andMe files for bankruptcy", CNN, March 24, 2025, https://edition.cnn.com/2025/03/24/tech/23andme-bankruptcy-hnk-intl/ (last visited February 25, 2026).
2. Liz Mineo, "What happens to your data if 23andMe collapses?" Harvard Gazette, March 20, 2025, https://news.harvard.edu/gazette/story/2025/03/what-happens-to-your-genetic-data-if-23andme-collapses/ (last visited February 25, 2026).
3. 23andMe, "23andMe Confirms All Potential Buyers Must Agree to Comply With Privacy Policy and Applicable Law," press release, March 26, 2025, https://mediacenter.23andme.com/press-releases/23andme-confirms-all-potential-buyers-must-agree-comply-privacy/ (last visited February 25, 2026).
4. Bhanvi Satija and Siddhi Mahatole, "Consumers urged to delete 23andMe data as bankruptcy sparks privacy fears," Reuters, March 25, 2025, https://www.reuters.com/business/healthcare-pharmaceuticals/new-york-attorney-general-urges-23andme-users-delete-their-data-2025-03-25/ (last visited February 25, 2026).
5. J. B. Branch, "Privacy, Consent, and National Security After the 23andMe Bankruptcy," Lawfare, July 17, 2025, https://www.lawfaremedia.org/article/privacy–consent–and-national-security-after-the-23andme-bankruptcy/ (last visited February 25, 2026); *Securing Americans' Genetic Information: Privacy and National Security Concerns Surrounding 23andMe's Bankruptcy Sale*, US House Committee on Oversight and Government Reform, 119th Cong. (2025), https://oversight.house.gov/hearing/securing-americans-genetic-information-privacy-and-national-security-concerns-surrounding-23andmes-bankruptcy-sale/ (last visited February 25, 2026).
6. 23andMe, "23andMe Receives Court Approval for Sale to TTAM Research Institute, a Nonprofit Public Benefit Corporation," press release, June 30, 2025, https://mediacenter.23andme.com/press-releases/23andme-receives-court-approval-sale-ttam-research-institute/ (last visited February 26, 2026); 23andMe, "TTAM Research Institute, A Nonprofit Public Benefit Corporation, Completes The Acquisition of 23andMe Assets," press release, July 14, 2025, https://mediacenter.23andme.com/press-releases/ttam-research-institute-nonprofit-public-benefit-corporation/ (last visited February 26, 2026).
7. Zhiyu Wan et al., "Sociotechnical safeguards for genomic data privacy," *Nature Reviews Genetics* 23, (2022): 429–45, https://doi.org/10.1038/s41576-022-00455-y; Johanna Rahnasto, "Genetic data are not always personal — disaggregating the identifiability and sensitivity of genetic data," *Journal of Law and the Biosciences* 10, no. 2 (2023): lsad029, https://doi.org/10.1093/jlb/lsad029.
8. Taner Kuru and Iñigo de Miguel Beriain, "Your genetic data is my genetic data: Unveiling another enforcement issue of the GDPR," *Computer Law & Security Review* 47 (November 2022): 105752, https://doi.org/10.1016/j.clsr.2022.105752.
9. In this paper, the term "Member States" refers to sovereign countries that are member of the European Union (EU). For an up-to-date list, see "EU Countries," European Union, https://european-union.europa.eu/principles-countries-history/eu-countries_en (last visited February 26, 2026).
10. 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, hereinafter "GDPR"), 2016 O.J. (L 119) 1, http://data.europa.eu/eli/reg/2016/679/oj (last visited February 26, 2026).

https://doi.org/10.1017/jme.2026.10259 Published online by Cambridge University Press

11. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281/31), http://data.europa.eu/eli/dir/1995/46/oj (last visited February 26, 2026).
12. Article 29 Data Protection Working Party, *Working Document on Genetic Data*, 12178/03/EN WP 91 (2004), https://www.cipil.law.cam.ac.uk/resources/article-29-working-party-documents-archive-1997-2018#year%202004 (last visited February 26, 2026).
13. GDPR, Recital 51
14. GDPR, Article 4(13)
15. Taner Kuru, "Genetic Data: The Achilles' Heel of the GDPR?" *European Data Protection Law Review* 7, no. 1 (2021): 45, https://doi.org/10.21552/edpl/2021/1/8.
16. "Genetic tests to check your cancer risk," National Health Service (NHS), https://www.nhs.uk/tests-and-treatments/genetic-tests-for-cancer-risk/ (last visited February 26, 2026)
17. GDPR, Article 9(1)
18. GDPR, Article 9(2) and (4)
19. For example, Article 2(1) of the recently adopted European Health Data Space Regulation (EHDS) states to apply the definition of genetic data in the GDPR. By the time of writing, the definition of genetic data has not been seen in other EU data legislation than the GDPR and EHDS.
20. In this paper, the term "the Court" refers to the European Court of Human Rights, https://www.echr.coe.int/ (last visited February 26, 2026).
21. Oliver M. Tuazon et al., "Genometric data privacy within the ECHR regime," *International Data Privacy Law* 15, no. 1 (2025): 1–17, https://doi.org/10.1093/idpl/ipaf004.
22. European Court of Human Rights, Council of Europe, *European Convention on Human Rights* (2025), https://edoc.coe.int/en/european-convention-on-human-rights/5579-european-convention-on-human-rights.html# (last visited February 27, 2026).
23. *Van der Velden v. The Netherlands*, App. No. 29514/05 (December 2006)
24. *S. and Marper v. The United Kingdom*, App. No. 30562/04, 30566/04, §72–73 and §104 (December 4, 2008)
25. *Aycaguer v. France*, App. No. 8806/12, §42 and §45 (June 22, 2017)
26. *Gaughran v. the United Kingdom*, App. No. 45245/15, §96 (February 13, 2020); *Trajkovski and Chipovski v. North Macedonia*, App. No. 53205/13, 63320/13, §54 (February 13, 2020)
27. Directive (EU) 2016/680, 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 119) 89 (EU), http://data.europa.eu/eli/dir/2016/680/2016-05-04 (last visited February 26, 2026).
28. Case C-205/21, *V.S. v. Ministerstvo na vatreshnite raboti*, ECLI:EU:C:2023:49 (January 26, 2023)
29. Case C-118/22, *NG v. Direktor na Glavna direktsia 'Natsionalna politsia' pri MVR – Sofia*, ECLI:EU:C:2024:97, §73 (January 30, 2024)
30. Ibid.
31. Natalie Ram et al., "Genealogy databases and the future of criminal investigation," *Science* 360, no. 6393 (2018): 1078–79, https://doi.org/10.1126/science.aau1083.
32. Deborah R. Gordon and Barbara A. Koenig, "'If relatives inherited the gene, they should inherit the data.' Bringing the family into the room where bioethics happens," *New Genetics and Society* 41, no. 1 (2022): 23–46, https://doi.org/10.1080/14636778.2021.2007065.
33. Dara Hallinan and Paul de Hert, "Genetic Classes and Genetic Categories: Protecting Genetic Groups Through Data Protection Law," in *Group Privacy*, ed. Linnet Taylor et al. (Springer International Publishing, 2017), https://doi.org/10.1007/978-3-319-46608-8_10.
34. Hallinan and de Hert, "Genetic Classes and Genetic Categories."
35. Kuru, "Genetic Data."
36. Kuru, "Genetic Data."
37. Rahnasto, "Genetic data are not always personal."
38. Bartha Maria Knoppers and Michael J. S. Beauvais, "Three decades of genetic privacy: a metaphoric journey," *Human Molecular Genetics* 30, no. R2 (2021): R156–60, https://doi.org/10.1093/hmg/ddab164.
39. Yaniv Erlich et al., "Identity inference of genomic data using long-range familial searches," *Science* 362, no. 6415 (2018): 690–94, https://doi.org/10.1126/science.aau4832; Badri Padhukasahasram, "Inferring ancestry from population genomic data and its applications," *Frontiers in Genetics* Volume 5-2014 (2014), https://www.frontiersin.org/journals/genetics/articles/10.3389/fgene.2014.00204 (last visited February 26, 2026); Ben Chan et al., "Genomic Inheritances: Disclosing Individual Research Results From Whole-Exome Sequencing to Deceased Participants' Relatives," *American Journal of Bioethics* 12, no. 10 (2012): 1–8, https://doi.org/10.1080/15265161.2012.699138.
40. Jorge Nicolás Lafferriere, "Protecting Privacy and Family Life in the Era of Recreational Genetics and Big Data," *International Journal of the Jurisprudence of the Family* 7 (2016): 33–60, https://ssrn.com/abstract=3224025.
41. Ellen Wright Clayton et al., "The law of genetic privacy: applications, implications, and limitations," *Journal of Law and the Biosciences* 6, no. 1 (2019): 1–36, https://doi.org/10.1093/jlb/lsz007.
42. Nina F. de Groot, "A contextual integrity approach to genomic information: what bioethics can learn from big data ethics," *Medicine, Health Care and Philosophy* 27 (2024): 367–79, https://doi.org/10.1007/s11019-024-10211-0.
43. Jennifer Couzin-Frankel, "Divulging DNA Secrets of Dead Stirs Debate," *Science* 343, no. 6169 (2014): 356–57, https://doi.org/10.1126/science.343.6169.356; Ellen Wright Clayton, "Families through the Lens of Genomics: Obligation or Consideration?" in *Promoting the "Human" in Law, Policy, and Medicine*, ed. Edward S. Dove et al., (Brill, 2025): 306–16, https://doi.org/10.1163/9789004688544_042.
44. Nora B. Henrikson et al., "What guidance does HIPAA offer to providers considering familial risk notification and cascade genetic testing?" *Journal of Law and the Biosciences* 7, no. 1 (2020): 1–14, https://doi.org/10.1093/jlb/lsaa071.
45. Jane Tiller and Margaret F. A. Otlowski, "Clinicians' discretion to contact patients' at-risk relatives about their genetic risk: new guidance from Australia's privacy regulator provides timely clarification," *Medical Journal of Australia* 223, no. 3 (2025): 123–26, https://doi.org/10.5694/mja2.52712.
46. Hallinan and de Hert, "Genetic Classes and Genetic Categories."
47. Hallinan and de Hert, "Genetic Classes and Genetic Categories."
48. Hallinan and de Hert, "Genetic Classes and Genetic Categories."
49. Hallinan and de Hert, "Genetic Classes and Genetic Categories."
50. Marisa A. Leib-Neri and Anya E. R. Prince, "Privacy and the Genetic Community," *American Journal of Bioethics* 22, no.7 (2022): 70–72, https://doi.org/10.1080/15265161.2022.2075972.
51. Tuazon et al., "Genometric data privacy."
52. Tuazon et al., "Genometric data privacy."
53. Knoppers and Beauvais, "Three decades of genetic privacy"; Tuazon et al., "Genometric data privacy."
54. Hallinan and de Hert, "Genetic Classes and Genetic Categories."
55. Knoppers and Beauvais, "Three decades of genetic privacy"; Paul Quinn and Liam Quinn, "Big genetic data and its big data protection challenges," *Computer Law & Security Review* 34, no. 5 (2018): 1000–18, https://doi.org/10.1016/j.clsr.2018.05.028.
56. Quinn and Quinn, "Big genetic data."
57. Gordon and Koenig, "'If relatives inherited the gene."
58. Hallinan and de Hert, "Genetic Classes and Genetic Categories."
59. Kuru, "Genetic Data."
60. Eric M. Meslin and Ibrahim Garba, "Biobanking and public health: is a human rights approach the tie that binds?" *Human Genetics* 130, (2011): 451–63, https://doi.org/10.1007/s00439-011-1061-2.
61. Gordon and Koenig, "'If relatives inherited the gene."
62. Hallinan and de Hert, "Genetic Classes and Genetic Categories."
63. UNESCO General Conference, Universal Declaration on the Human Genome and Human Rights (November 11, 1997), 29 C, art. 16, https://www.unesco.org/en/legal-affairs/universal-declaration-human-genome-and-human-rights?hub=387 (last visited February 27, 2026).
64. UNESCO General Conference, International Declaration on Human Genetic Data (October 16, 2003), 32 C, res. 22, art. 4, https://www.unesco.org/

https://doi.org/10.1017/jme.2026.10259 Published online by Cambridge University Press

en/legal-affairs/international-declaration-human-genetic-data?hub=387 (last visited February 27, 2026).
65. Council of Europe, *The Protection of Medical Data: Recommendation No. R (97) 5* (Committee of Ministers, February 13, 1997), https://search.coe.int/cm?i=09000016804f0ed0 (last visited February 27, 2026).
66. Council of Europe, *The Protection of Medical Data*
67. Council of Europe, *Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Genetic Testing for Health Purposes* (Council of Europe Treaty Series 203, 2009), art. 4, ch. VI, https://www.coe.int/en/web/conventions/-/council-of-europe-additional-protocol-to-the-convention-on-human-rights-and-biomedicine-concerning-genetic-testing-for-health-purposes-cets-no-203-tra (last visited February 27, 2026).
68. "Article 29 Working Party," European Commission, https://ec.europa.eu/newsroom/article29/items/itemType/1358 (last visited February 26, 2026).
69. Article 29 Data Protection Working Party, *Working Document on Genetic Data.*
70. Article 29 Data Protection Working Party, *Working Document on Genetic Data.*
71. Article 29 Data Protection Working Party, *Working Document on Genetic Data.*
72. Róisín Á. Costello, "Genetic Data and the Right to Privacy: Towards a Relational Theory of Privacy?" *Human Rights Law Review* 22, no. 1 (2022): ngab031, https://doi.org/10.1093/hrlr/ngab031.
73. Tuazon et al., "Genometric data privacy."
74. *S. and Marper v. The United Kingdom*, §72-77
75. *Gaughran v. the United Kingdom*, §81
76. Ibid., §81
77. Costello, "Genetic Data and the Right to Privacy."
78. *ABC v St George's Healthcare NHS Trust & Ors* [2020] EWHC (Eng.).
79. Knoppers and Beauvais, "Three decades of genetic privacy."
80. Costello, "Genetic Data and the Right to Privacy."
81. Ruha Benjamin, "*A Lab of Their Own*: Genomic sovereignty as postcolonial science policy," *Policy and Society* 28, no.4 (2009): 341–55, https://doi.org/10.1016/j.polsoc.2009.09.007.
82. Eric T. Juengst and Eric M. Meslin, "Sharing with Strangers: Governance Models for Borderless Genomic Research in a Territorial World," *Kennedy Institute of Ethics Journal* 29, no.1 (2019): 67–95, https://doi.org/10.1353/ken.2019.0000; Joy Y. Zhang, "Commoning genomic solidarity to improve global health equality," *Cell Genomics* 3, no.10 (2023): 100405, https://doi.org/10.1016/j.xgen.2023.100405.
83. Matthew Z. Anderson et al., "A Tribal data repository to advance Indigenous health and sovereignty," *Nature Genetics* 57 (2025): 2614–19, https://doi.org/10.1038/s41588-025-02382-0.
84. Secretariat, *Convention on Biological Diversity* (CBD) (United Nations Environmental Programme, 2011): 79, https://www.cbd.int/convention/text (last visited February 27, 2026).
85. Secretariat, *Nagoya Protocol on Access to Genetic Resources and the Fair and Equitable Sharing of Benefits Arising from their Utilization to the Convention on Biological Diversity* (Nagoya Protocol) (United Nations Environmental Programme, 2011), https://www.cbd.int/abs (last visited February 27, 2026).
86. *Nagoya Protocol*, art. 6
87. Article 2 of CBD defines "genetic material" as any material of plant, animal, microbial, or other origin containing functional units of heredity, without taking human genetic materials into consideration.
88. Doris Schroeder and Carolina Lasén-Díaz, "Sharing the Benefits of Genetic Resources: From Biodiversity to Human Genetics," *Developing World Bioethics* 6, no. 3 (2006): 135–43, https://doi.org/10.1111/j.1471-8847.2006.00148.x.
89. Schroeder and Lasén-Díaz, "Sharing the Benefits of Genetic Resources"; Bege Dauda and Kris Dierickx, "Benefit sharing: an exploration on the contextual discourse of a changing concept," *BMC Medical Ethics* 14 (2013): 36, https://doi.org/10.1186/1472-6939-14-36.
90. Joy Y. Zhang, "What Do the British and Chinese Governing Visions on Human Genomic Research Tell Us about Biosovereignty?" *Asian Biotechnology and Development Review* 25, no. 1&2 (2023): 5, https://www.researchgate.net/publication/373293783_What_Do_the_British_and_Chinese_Governing_Visions_on_Human_Genomic_Research_Tell_Us_about_Biosovereignty (last visited February 26, 2026).
91. Kyle McKibbin and Mahsa Shabani, "Genomic Data as a National Strategic Resource: Implications for the Genomic Commons and International Data Sharing for Biomedical Research and Innovation," *Journal of Law, Medicine & Ethics* 51, no. 2 (2023): 301–13, https://doi.org/10.1017/jme.2023.77.
92. "**Biosecurity Law of the People's Republic of China"** (Biosecurity Law) (Standing Committee of the National People's Congress, October 17, 2020), English translation available at https://www.lawinfochina.com/display.aspx?id=43149&lib=law&EncodingName=big5/ (last visited February 26, 2026).
93. "**Regulation on the Management of Human Genetic Resources"** (People's Republic of China, December 7, 2019), English translation available at https://www.chinalawtranslate.com/en/p-r-c-regulation-on-the-management-of-human-genetic-resources/ (last visited February 26, 2026).
94. Biosecurity Law, Article 2
95. Biosecurity Law, Article 53 and Article 56
96. Biosecurity Law, Article 56
97. Biosecurity Law, Article 59
98. Liang Huigang et al., "Significance of and Outlook for the Biosecurity Law of the People's Republic of China," *Journal of Biosafety and Biosecurity* 3, no. 1 (2021): 46–50, https://doi.org/10.1016/j.jobb.2021.06.004.
99. Jiajv Chen and Wei Li, "Is cross-border transfer of China's human genetic data an impossible mission?," *Human Genetics* 144 (2025): 715–25, https://doi.org/10.1007/s00439-025-02756-8; Lingqiao Song et al., "Statistic tells: the regulatory pendulum of permit trajectories in China's genetic governance (2021–2024)," *Frontiers in Genetics* 16 (2025): 1611003, https://doi.org/10.3389/fgene.2025.1611003.
100. Smriti Mallapaty, "China expands control over genetic data used in scientific research," *Nature* 605, (2022): 405, https://doi.org/10.1038/d41586-022-01230-z.
101. Zhang, "What Do the British and Chinese Governing Visions on Human Genomic Research Tell Us about Biosovereignty?"
102. Exec. Order No. 14117, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, 89 Fed. Reg. 15421 (2024).
103. Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 28 C.F.R. § 202, 90 Fed. Reg. 1636 (2025).
104. Preventing Access to U.S. Sensitive Personal Data
105. Zijing Yang, "Geopolitics and Strategic Competition Behind U.S.-China Genomic Data Policies," Law and Biosciences Blog, September 1, 2025, https://law.stanford.edu/2025/09/01/geopolitics-and-strategic-competition-behind-u-s-china-genomic-data-policies/ (last visited February 26, 2026)
106. *H.R. 8333: BIOSECURE Act*, 118th Congress (2024), https://www.congress.gov/bill/118th-congress/house-bill/8333/text/eh (last visited February 26, 2026).
107. Andrew Dockham et al., "BIOSECURE Act: 2025 Version," Freshfields, September 11, 2025, https://blog.freshfields.us/post/102l4p9/biosecure-act-2025-version (last visited February 26, 2026); Geoffrey Lin et al., "Reintroduction of the BIOSECURE Act: Potential Impact on the Biotechnology Industry,", Ropes & Gray, September 3, 2025, https://www.ropesgray.com/en/insights/alerts/2025/09/reintroduction-of-the-biosecure-act-potential-impact-on-the-biotechnology-industry (last visited February 26, 2026).
108. McKibbin and Shabani, "Genomic Data as a National Strategic Resource."
109. "European '1+ Million Genomes' Initiative," European Commission Digital Strategy, September 5, 2025, https://digital-strategy.ec.europa.eu/en/policies/1-million-genomes (last visited February 26, 2026).
110. McKibbin and Shabani, "Genomic Data as a National Strategic Resource."
111. Deputy Prime Minister and the Chancellor of the Duchy of Lancaster, "UK Biological Security Strategy," UK Parliament, June 12, 2023, https://www.gov.uk/government/publications/uk-biological-security-strategy (last visited February 27, 2026).
112. "Powering genomic medicine, together," Genomics England, https://www.genomicsengland.co.uk/ (last visited February 27, 2026).
113. Lord Bethel of Romford et al., "Genome UK: The Future of Healthcare," Cabinet Office, September 26, 2020, https://www.gov.uk/government/publications/genome-uk-the-future-of-healthcare/ (last visited February 27, 2026).
114. House of Commons, "Genomics and National Security," Volume 729, debated on March 8, 2023, https://hansard.parliament.uk/commons/2023-03-08/

https://doi.org/10.1017/jme.2026.10259 Published online by Cambridge University Press

debates/3F7E5903-596F-492A-B130-A4503928CA7F/GenomicsAndNationalSecurity/ (last visited February 27, 2026).
115. Kate Johnson, "Genomics sector won't be designated critical infrastructure in UK," Progress Educational Trust, April 22, 2024, https://www.progress.org.uk/genomics-sector-wont-be-designated-critical-infrastructure-in-uk/ (last visited February 27, 2026).
116. McKibbin and Shabani, "Genomic Data as a National Strategic Resource."
117. Rachel Horton and Anneke Lucassen, "Consent and Autonomy in the Genomics Era," *Current Genetic Medicine Reports* 7 (2019): 85–91, https://doi.org/10.1007/s40142-019-00164-9; Gordon and Koenig, "'If relatives inherited the gene."
118. "CIHR Guidelines for Health Research Involving Aboriginal People (2007–2010)," Canadian Institutes of Health Research, June 27, 2013, https://cihr-irsc.gc.ca/e/29134.html (last visited February 27, 2026).
119. Elisabet Rodriguez Llorian et al., "A Rapid Review on the Value of Biobanks Containing Genetic Information," *Value in Health* 26, no. 9 (2023): 1286–95, https://doi.org/10.1016/j.jval.2023.02.017.
120. McKibbin and Shabani, "Genomic Data as a National Strategic Resource."

https://doi.org/10.1017/jme.2026.10259 Published online by Cambridge University Press