THE JBBA

PEER REVIEWED RESEARCH

OPEN ACCESS
ISSN Online: 2516-3957
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-3-2-(5)2020

Privacy Laws, Genomic Data and Non-Fungible Tokens

[1]Daniel Uribe and [2]Gisele Waters
[1]Genobank.io, USA
[2]Engineering Hearts™, USA

Correspondence: daniel@genobank.io
Received: 19 April 2020 **Accepted:** 15 May 2020 **Published:** 30 May 2020

Abstract

This article analyses the main legal requirements in the California Consumer Protection Act (CCPA), general data protection regulation (GDPR) and the intersections between privacy laws, genomic data and smart contracts (such as fungible and non-fungible tokens [NFTs]). The CCPA and GDPR laws impose several restrictions on the storing, accessing, processing and transferring of personal data. This has generated some challenges for lawyers, data processors and business enterprises engaged in blockchain offerings, especially as they pertain to high-risk data sets such as genomic data. The technical features of NFT, distributed storage and wallets to trace and govern genomic (DNA) data sets will allow data donors to establish digital ownership and control in line with privacy laws using 'programmable privacy smart contracts'. To be legally compliant, the design of blockchain value propositions should include privacy-by-design capabilities in the smart contract coding language itself. This article describes three domains (privacy laws, genomics and NFTs) and begins to explore how data engineers can address the challenges of coding privacy laws, the legal requirements into smart contracts. This current approach focuses on NFTs and genomic data requirements which include the selection of genetic metadata borrowing from developing ERC specifications and their programming logic. Programmable privacy is a unique way to write and design computer code, which can automatically check the legal compliance of the smart contract in a trust-less and decentralised way. We exemplify the approach by describing the conceptual value proposition of Genobank.io, a privacy-preserving genomic data platform.

Keywords:

Blockchain, biobanking, biometric, smart contracts, California Consumer Protection Act, privacy, programmable, distributed storage, IPFS, genomics, DNA, data processor, privacy law, GDPR, CCPA, non-fungible tokens (NFTs), fungible tokens, ERC998, ERC1155, ERC721, data sovereignty, Ethereum

1. Introduction

The battle of legitimate authority and control over genomics [1] data introduces a substantial legal and computational burden on data privacy. Consumers are already suing doctors [2], hospitals and data processors to hold them liable for how they offer, interpret and counsel patients about genetic tests. In this article, we introduce one use case, Genobank.io [3], which aims to protect consumer privacy by engaging stakeholders at the intersection of privacy law, smart contracts [4] [5] using non-fungible tokens (NFTs) [6] [7] and genomics.

There are growing challenges in this complex ecosystem that can only be solved collaboratively [8]. Subject matter experts in all three domains (law, genomics and smart contracts) will be dependent on each other to achieve success and avoid risk. Here, the concepts, interrelationships and the implications of a specific use case in genomics: the implications of the California Consumer Privacy Act [9][10] (CCPA) and the European Union's general data protection regulation [11] (GDPR) to smart contracts, specifically NFTs in the blockchain [12], are presented. The Consumer Online Privacy Act (COPRA) [13] is also briefly overviewed. Two questions are posed as a starting point for stakeholder collaboration:

1. The human challenge: How do stakeholders with conflicting interests work together to ensure privacy laws protect the most personal, private, and sensitive data[1] derived from biospecimens [14]?
2. The technology challenge: How can privacy laws be coded [15] into smart contracts to protect high-risk data with strong consent and privacy mechanisms? In other words, how do you embed laws of the physical world into machine code with privacy as the highest value?

There are about 8 billion people on the planet and more than 26 million [16] have already analysed their DNA. Approximately a million people worldwide have had their whole genome sequenced [17].

> *So many people have had their DNA sequenced that they have put other people's privacy at risk. [18]*

On the other hand, 99% [14] of the world's genetic information has *yet* to be produced. Those global statistics represent billions of dollars in marketplace opportunity [19] and probably an equally large risk [20] [21] in liability. How the

opportunities and risks get defined in the next decade will be led by stakeholders working together across domains in law, genomics and technology.

Inevitable problems will arise if companies do not address the form and function of their technology solutions to face international and local data-privacy laws [22] [23], especially in the field of genomics. To create a fair and more secure marketplace for genetic information, privacy laws can be applied to the use of blockchain with NFTs (a type of smart contract). To help mitigate the gaps and challenges, stakeholders can also work together in transdisciplinary [24] ways that begin to create a common language [25] of understanding across the three domains of privacy laws, genomics and smart contracts. This article is a preliminary effort towards one of the much-needed stakeholder conversations and collaborations. This is a long-term endeavour where lawyers, data processors, genomic researchers and data subjects can define, together, what data practices and governance will be in the future.

At the intersection of the three domains, business enterprise is beginning to address this challenge by engineering various iterations of privacy-by-design offers and more specifically by engineering *privacy by blockchain design* [26] [27]. In the latter, solutions can be GDPR compliant and also include additional legal privacy requirements with strategic smart contract terms and conditions. These new business models are helping to raise data protection levels and aim to give back data ownership to individuals. Specifically, one such enterprise, Genobank.io, has focused on bringing smart contracts such as NFTs that combine unique value-added architectures to the privacy-by-design proposition for genomic data. Details are shared later; first, we introduce the primary concepts of the three domains.

2. Three domains: collaboration required

Privacy laws

The European Union's GDPR went into effect on 25 May 2018 and a similar law in California, the world's fifth largest economy, the CCPA, went into effect on 1 January 2020. The newest privacy legislation from the U.S. Congress is COPRA, a Federal Bill aimed at protecting the privacy of consumers online at the national level. If this Bill crosses the finish line in the future, it would finally strengthen the Federal Trade Commission's ability to enforce digital privacy protections. But other similar Bills introduced in the past have never made it. Regardless, international and local privacy laws are keeping many privacy and security officers awake at night. Those concerns will not be alleviated unless stakeholders work together on how to address the requirements and specifications for policy and practice.

A few legal experts have coined the CCPA law as 'GDPR *Lite*'. But others suggest the CCPA is *not Lite* [28] at all and there is much more to do with the CCPA than previously believed. Some privacy lawyers say that companies who have already addressed the requirements of the GDPR have *a lot more* to prepare in order to address the higher requirements in the CCPA. The CCPA intends to provide California residents with the rights to:

1. know what personal data is being collected,
2. know whether it is being sold or disclosed and to whom,
3. refuse the sale of their personal data,
4. access their personal data,
5. request a business delete any personal data,
6. and not be discriminated against for exercising their privacy rights.

These six essential rights are part of the new CCPA challenges that privacy lawyers, technologists, genomic researchers and data processors are faced with today. The new law also sets penalties of $2,500–$7,500 per violation [23] and a private right of action to individuals affected by a breach caused by a lack of reasonable security measures. Due to the provision of statutory damages, the risk of litigation [29] is very significant. Under the CCPA, an entity qualifying as a 'business' must also provide seven protections. For example, business must provide disclosures regarding the sale of personal information collected from or about covered consumers (id. § 1798.110(a), an opt-in requirement before selling a minor's personal information (id. § 1798.120(c), the ability for covered consumers to access and/or delete personal information collected from or about them (id. §§ 1798.105), and must also implement measures to prevent discrimination against consumers who exercise their rights under the CCPA (id. § 1798.125) among others.

A few of the conditions required by the CCPA suggest a substantially different way of doing business and a higher threshold for data governance than has been required previously. The law also expands upon *what* personal information is and *how* it is used by businesses.

Under the CCPA, personal data (identifiers, geolocation, internet activity, education and employment information among others) also includes biometric information. Biometric information is defined as 'an individual's physiological, biological, or behavioural characteristics, including deoxyribonucleic acid (DNA), that can be used singly or in combination with other identifying data, to establish identify' [9]. Examples such as imagery of the iris, retina, fingerprint, face, hand, palm, voice recordings, keystroke patterns, exercise data, gait patterns and *even sleep* are protected by the law.

Businesses should take heed, if personal or biometric data are gathered by a company, without notice, it is still considered private personal information and subject to legal protection. These new considerations on what kind of data and under what conditions the data are protected under the law sets a higher bar for data governance.

The newest privacy law proposed at the federal level may extend consumer protections even further. It was introduced by Senators Cantwell, Schatz, Klobuchar and Markey on 26 November 2019. COPRA is written to provide consumers with foundational data-privacy rights, creating strong oversight mechanisms and establishing meaningful enforcement of the same. This new legislation, as introduced, suggests that companies must not collect more information than they

'reasonably' need to function. COPRA is tremendously ground-breaking as proposed [30] and could, *if passed*, create the need for substantial liability and risk resource allocation in the future. The basic tenets of this new law include extended data-privacy rights (Title I), augmented oversight and responsibility (Title II) including a section on digital content forgeries and some added legal traction with Title III that adds miscellaneous sections on enforcement, civil penalties, authorisation of appropriations and severability among others.

The following genomic and digital data are considered *biometric information* that is to be protected online by the COPRA:

(i) fingerprints.
(ii) voice prints.
(iii) iris or retina scans.
(iv) facial scans or templates.
(v) deoxyribonucleic acid (DNA) information; and
(vi) gait.

Similar to CCPA, gait is also included; a person's manner of walking is protected biometric information. Excluded are writing samples, written signatures, photographs, voice *recordings* and demographic data. Also excluded are physical characteristics such as height, weight, hair colour and eye colour, provided that such data is *not used* for the purpose of identifying an individual's unique biological, physical or physiological characteristics.

COPRA would go further than past laws, in that it defines the terms 'collect' and 'collection' to mean buying, renting, gathering, obtaining, receiving, accessing or otherwise acquiring covered data *by any means*, including by *passively or actively observing the individual's behaviour*. The CCPA and COPRA are huge shifts in regulation and data governance towards protecting the rights of consumers as opposed to allowing any collection and use of consumer data for a company's own benefits.

Implications

All laws [31] are meant to protect general safety and ensure our rights as citizens against abuses by other people, by organisations, and by the government itself. Laws do this by requiring specific behaviours and prohibiting others. The CCPA as enacted will 'nudge' [32] and require companies to act differently. If enacted, COPRA, as the next-generation regulation, will push the 'nudging' further. As privacy lawyers, data processors, genomic researchers and DNA donors consider a path forward, we suggest stakeholders collaborate on how to manage the opportunities and risks to balance public and private interests. It is inevitable that the implementation of the CCPA (enacted law) will bring about drastic challenges to companies and developers using the blockchain, especially in regard to genomics.

Genomics

Genomics [33] [34] is a domain within genetics that concerns the sequencing and analysis of an organism's genome. It is an is an interdisciplinary field of biology focusing on the structure, function, evolution, mapping and editing of genomes. Experts in genomics seek to complete DNA sequences beyond just partial analyses in order to perform genetic mapping that can help understand disease. A genome is a complete set of DNAs including all genes in one organism. Due to the highly sensitive nature in the uniqueness of genomic data, privacy requirements are complex transaction-laden systems with layers of health information that need both legal and computational privacy protection. Privacy protections are only beginning to gain solid ground in the United States and have yet to be fully realised.

Next-generation sequencing and genome editing have helped to make medicine more precise and efficient, especially regarding disease diagnostics and treatment. But the rapid development can only be realised by the *aggregation and analysis of people's genomic and health data* at scale. Efficient processing of very large-scale genomic data sets creates risk in the marketplace of biometric information. For the most part, DNA donors have been left powerless [35] [36] without any control over their own personal genetic profiles, essentially left without sovereignty. Data sovereignty is the concept that information, which has been converted and stored in binary digital form, is subject to the laws of the country in which it is located. The CCPA, Health Insurance Portability and Accountability Act (HIPAA) [37] and the Genetic Information Non-discrimination Act (GINA) [38] are the first set of laws in the United States that are beginning to provide protection and sovereignty. But the global wars over genetic information [39] [40] have only just begun and case histories, in the United States for example, reflect the struggles that the private and public sectors continue to have with gaps and challenges to the four corners of the law.

With newer and stronger privacy laws, the government is approximating prudence [41] and protection for the general safety and security of its citizens. But technology providers can go further. The lingering gaps in regulation add persuasive motivation to ethical technology leaders to move beyond the minimal requirements of the law towards *ethical best* practices [42] [43]. Working together with regulators on ethical data governance and understanding, they can provide a value proposition that both protects the consumer and provides a marketplace competitive advantage. One does not have to exclude the other. Rapid developments in the aggregation and analysis of people's genomic and health data at scale *can* benefit individuals, the public and the private sectors *simultaneously*.

The new laws imposed and the plethora of lawsuits that businesses are enduring indicate, from the individual's perspective, that the CCPA and the like may not go far enough, yet, to protect an individual's biometric data [39] [44]. From the enterprise perspective, the risk of liability from intended, unintended and even derivative attempts at aggregation of de-identified biometric data to identifiable databases should be at least one reason to borrow from the spirit of the law and its legal premise to create privacy-by-design solutions with *grit. Using NFTs for genomics data may give both the individual and the enterprise a way to work together on balancing* disparate, indeed often conflicting interests. The use of NFTs to address this challenge will be explained shortly.

Blockchain

A blockchain [45] is a time-stamped series of records (like a record in a spreadsheet but written only once) that is managed by a cluster of computers not owned by any single entity. Blocks of data (i.e. block) are secured and bound to each other like a chain using cryptographic principles such as confidentiality, authentication, integrity and non-repudiation [46]. All data stored on the blockchain have a common history available to all network participants. With this mechanism, the chances of fraudulent activity or duplications is eliminated without the need of third-party intermediaries [47].

Otherwise known as a distributed public ledger [48] [49], a blockchain tracks assets and transaction records so that each data block contains a unique hash 'tag' (digital fingerprint/signature) and time-stamped batches of recent transactions plus a hash of the previous block [50]. Each record with an encrypted digital signature proving its authenticity in the blockchain is tamper proof and cannot be changed. Blockchain and smart contracts can help counter problems such as imbalances in data control, information islands, data tampering, theft, abuse, data leaking, grey data transactions and missing records [50]. As with other technologies, blockchain has augmented [51] its bandwidth and expanded its capacity.

There are four [52] generations of current blockchains across many industries [53] worldwide [54]. The use cases expand daily in healthcare [55] [56]. On top of privacy laws nudging new business behaviour, in the healthcare space, providers are already answering strong calls to give easy access and control of personal healthcare records to the patient. But a review of the usage of blockchain technology in healthcare reveals that a patient's sovereignty, privacy and security [57] is not the most prevalent foci necessarily. The vast majority of blockchain applications in healthcare have been implemented to address interoperability and the substantial siloed data structures among diverse organisations. This is why decentralised, immutable ledgers like the blockchain provide more portable, interoperable mechanisms for the correct processing and secure sharing of data [21] [58] [59].

To share medical data, and more importantly highly sensitive genomic data securely, it is required that parties agree on the structure and semantics of data sharing [50]. Again, the human challenge to using technology optimally is represented here. Taking full advantage of the promise blockchain and smart contracts offer to computational genomics [1] [43] [60] is a fit-for-purpose that should be taken seriously by collaborating at domain intersections. Implementing privacy laws in the genomic data ecosystem is also a socio-technical challenge, not just a technical one. Furthermore, the maturity of the blockchain field is timely now in consideration of the greater need to manage vast quantities and different kinds of data (e.g. biobanking and biometric data) that require inviolable privacy parameters [59] [61]. Although many blockchain applications are still in conceptual stages testing various aspects of the technology, these more complex requirements for security demonstrate a need for the added transparency, confidentiality and programmable privacy in smart contracts [61] [62].

Self-executing computer protocols such as smart contracts execute agreements based on computer algorithms between two or more parties while creating an indisputable record of transactions associated with granting and revoking access [63] to a data (cryptocurrency) wallet. To ensure control, data transactions are signed by the owner using a private key [1] [64]. Private keys are created when users create an account (crypto data wallet) on any Web3 decentralised platform. A crypto data wallet usually has two main purposes. The first is to be able to easily share your public address through the internet and second to securely store the corresponding private key(s). Private keys can be encrypted or unencrypted as decided by the level of security offered by the blockchain platform.

The main idea behind using a crypto data wallet for genomic data is to introduce a novel alternative for users to regain data sovereignty with the support of privacy laws. Data wallets will enable data subjects to become data custodians while interacting with a genomic data processor (labs or researchers, for example) without losing any control or ownership. Unlike when companies such as 23&Me sell an ancestry and health report to a specific consumer, they claim ownership and establish control over a consumer's genomic data. In contrast, a DNA data wallet allows users to temporarily grant access to a genomic data processor so they can execute an interpretation algorithm or other analyses. These analyses are governed by a smart contract that can be programmed to destroy or delete any digital computer instance that was created during the data processing for privacy purposes.

In other words, all instances of virtual machining can be deleted or destroyed by the terms and conditions of the smart contracts selected. This would be an equivalent to self-serving a consumer's right to be forgotten as a data subject/owner in GDPR and CCPA terms, respectively. There is no need for the data owner to keep a copy of the analytics or algorithms used for a report and there is no need for 23&Me to keep a copy of the data owner's DNA. Both parties are satisfied and protected. There is no justification or reason for the data owner to keep any IP from the data processor and no justification for the processor to keep a copy of the data owner's DNA. Then by integrating the terms and conditions of privacy laws into smart contracts with the specifications of NFTs, we suggest this combination of programmable privacy could be a novel and valuable form of next-generation privacy-preserving [65] technology.

This could dramatically change the status quo of data custodianship. Currently, the reality is data owners give away their rights, their custody and ownership to their DNA data or sell it for cents on the dollar [66] [67]. We argue crypto data wallets in combination with smart contracts, using NFTs, can disrupt the status quo of data ownership and governance.

All together, these mechanisms can facilitate a CCPA and GDPR compliant data management system by encoding in the

smart contract a set of rules that ensure privacy for consumer-sensitive data. In essence, smart contracts provide better security performance than traditional contract law because they are encoded and written in such a way that they guarantee the execution of explicitly specified conditions [5] [44].

Risks

With broad opportunities come many risks. Inherent in any technology innovation is the absence of time and conditions that help stress test the boundaries of any new applications. Here, two primary risks with these smart contracts will be addressed in the limited time and space allowed. One is the potential that private keys are lost or mishandled. The second is the security and privacy risks when the data is at rest or in transit.

According to Chainalysis, 19% of cryptocurrency holders lost digital assets due to mismanaged digital wallets and keys [68]. But the market has already responded by offering new private key recovery solutions, both for custodial and non-custodial authorisations. One such service is the Squarelink platform. For now, it is the only *pure* non-custodial private key recovery platform. Others rely on custodial key-management services like Amazon Cognito, for example [69]. Another mitigation scheme for lost keys and wallet access is known as secure attribute-based signatures that support multiple authorities for expanded authorised access [70]. Attribute-based signatures are also being explored and tested still. As to how to address the issue of risk when data is at rest or in transit, the maintenance of encryption, authorisation and authentication during both data states are absolutely crucial and possible with proxy re-encryption (PRE) schemes [71]. Data transit can also be limited through distributed storage governance. As explained earlier in the 23&Me example, software analysis can be 'brought to the data' rather than software or algorithms processing data from a corporate owned machine [72].

One configuration of data storage, for example, is private IPFS nodes hosting DNA data for a single owner [56]. IPFS is the new alternative to corporate controlled data storage. In other words, IPFS is controlled by a community of developers similar to Bitcoin where the data repositories are only owned by the creators of content that also hold the private keys. Data owners can allow trusted third-party validators and other authorised custodians [60] [61]. Using PRE layers such as Nucypher, consumers can securely share encrypted data without sharing their private key [73]. PRE serves as a means for delegating decryption rights, opening up applications that require delegated access to encrypted data (whether genomic or otherwise) [71].

By augmenting who gets access in these kinds of configurations, authorised custodians may be optionally established over time without compromising either the security or the integrity of the data and the data owner. Essentially PRE helps data owners share a secret with minimal risks to the secret or secret keeper [74]. Risks are thereby minimised more adequately within these frameworks as opposed to what is in existence in legacy healthcare and genomic data silos. The data owner can essentially rent out their data never losing control over it. Next, we explain how NFTs, specifically on top of these crypto privacy-preserving [65] offerings, create additional value for highly sensitive and scarce data like genomic data in the context of adhering to privacy laws.

Non-fungible tokens (smart contracts)

Gamers were first attracted to NFTs because they could represent the collectible creatures called CryptoKitties [75]. NFTs are now used by crypto artists, blockchain games and countless other users to ensure digital scarcity and ownership. NFTs are tokens *minted* on blockchains that are irreplaceable and individually unique [76] [77]. In contrast, fungible tokens refer to something that can easily be replaced by something identical and is interchangeable. A dollar bill is an example of a fungible item. If you were to lend a dollar, it wouldn't matter what dollar nor what fungible token representing it was returned. Non-fungible means that no other asset or representative token is exactly like it. This is both relevant and similar to the representation, form and function of genomic data. The NFT design is especially advantageous for managing the rights and ownership of highly scarce and unique assets, both on and off the blockchain.

In this same way, we believe using NFTs will assist in making genomics data portable beyond the specified solution across multiple environments, while still allowing for strong governance and control by the genomic data owner or authorised custodian. Thus, we identify the use of NFTs to represent individual user genomes. Unlike traditional cryptocurrency or ledger-based tokens, NFTs are not interchangeable – carrying their own information or other attributes that make them irreplaceable. NFTs on the Ethereum Blockchain are governed by two specifications known as ERC-721 and ERC-1155 [7] [78]. Additional Ethereum Request for Comments (ERCs) show developmental growth that may represent more robust specifications in genomics data use cases. See Table 1.

Table 1

Privacy law, genomic data, NFT/ERC developmental stages					
	ERC721	ERC998	ERC1155	ERC994	ERCXXXX (IDEAL)
Locked ownership (ownership loss prevented)	Yes	Yes	Yes	Yes	Yes
Non-fungible token collective ownership (parent, child, family tokens possible)	No	Yes	Yes	No	Yes
Semi-fungible (Can hold both non-fungible and fungible tokens)	No	No	Yes	No	Yes
Delegated to authorised custodians (suitable for "rent")	No	No	Yes	Yes	Yes
Metadata included for location of cytogenic data (e.g. (whole genome, chromosome, genes, SNPs)	No	No	No	No	Yes
Data maintenance and programmable privacy code schemas (GDPR, CCPA, COPRA, etc.)	No	No	No	No	Yes

ERC-721 defines a minimum interface written in Solidity [79] that allows unique tokens to be managed, owned and traded [78]. It does not mandate a standard for token metadata or restrict adding supplemental functions for genomics payloads. In the proposed solution, ERC-721 are used to store references to genomic material and searchable metadata attributes. Whereas ERC-721 mandates a unique token contract for each token created, ERC-1155 may be more efficient to create and bundle token transactions. ERC-1155 can be used to meter requests for genomic data and ensure that no user has more than their share of resources commuted to perform work in the data processors environment.

ERC-1155 provides additional flexibility over ERC-721 by creating flexible, re-configurable or exhaustible tokens. Alternatively, the ERC-998 extension to ERC-721 is still in draft but offers the idea of NFT collections such as parent, child and family DNA collections. The ERC-998 and future ERCs are developmentally better iterations on past ERCs with other limitations such as inefficient transfer capability, array length and inability to get token IDs [79]. But as illustrated in Table 1, in ERCXXX, Genobank is targeting the development of a future more robust solution specification to the challenges at the intersection of privacy laws, genomics and smart contracts.

Use case

Genobank is the first privacy-preserving personal DNA Kit (patented) that guarantees consumers' complete ownership and control over their DNA. It was founded so that patients can benefit from finding DNA-based clinical trials without risking their identities or control over their data. Genobank.io is built on an Oasis Lab decentralised cloud infrastructure [80] that allows developers to create Web 3.0 applications where users can own and control their genomic data in a peer-to-peer transaction mode. This offers a high-performing (1000s of transactions per second) confidential and privacy-preserving NFT [6] execution. Its purposeful design supports rigorous analysis using various security properties [63] [81]. The DNA crypto wallet allows users to purchase biospecimen extraction kits. Biospecimens include biomaterial such as saliva that render DNA and RNA genomic information. After the biospecimen is collected for the specific extraction kit, the user can choose to send the kit to their preferred CLIA Certified Laboratories Sequencing Service [82] for analyses. The biospecimen itself will remain at the CLIA Lab, but the digital data, analyses and any 'reporting' will be stored in a data wallet repository. The wallet repository is the 'place' where genetic data is 'banked'. The Genobank approach is still developing and refining itself as a value proposition. But unlike many existing options (e.g. LunaDNA, Nebula Genomics, EncrypGen [62] [66]), Genobank offers the DNA donor and data processor a secure platform where they can both ethically and efficiently process genetic data without DNA owners losing custody or control over their DNA.

3. Discussion

Over the last 10 years, laws, medicine and technology together with policy makers and regulators (including the United States Food and Drug Administration, FDA) have struggled to establish timely regulation [44] [60] and oversight over the direct to consumer genetic testing (DTC-GT) health market.

The DTC-GT market has pushed the boundaries of how society and the law will manage the value of privacy over profit and what that will look like in data governance practices. To date, companies such as 23andMe and Ancestry, among others [83], have shown an inexhaustible ability and willingness to exchange consumer information (e.g. statistics about raw genetic health risk and ancestry/genealogical data, and genetic data) with third parties [84] [35]. But now, even their third-party collaborators are at risk for liability issues because privacy laws like the CCPA are requiring different business behaviour than in the past.

Sharing, selling and reselling DNA data is not unique to companies like 23andMe, Ancestry and GSK [35]. History and the law provide an endless record of people and entities that find highly sensitive information like health and genetics data valuable [8] [83] [85]. Analysing millions of people's genetics alongside their health issues gives big pharma and data processors immense power and innumerable clues on the interplay between genetics and the conditions leading to untold future profits. Ensuring both the ethical and legal underpinnings of this marketplace may not be the norm now, but it could be in the future.

Platforms such as Genobank.io can help re-balance the power [86] between stakeholders where privacy laws are trying to redress negative outcomes on the public with NFTs and programmable privacy.

4. Conclusion

At the intersection of privacy law, genomics and smart contracts, stakeholders can either help drive or hinder progress to address the balance between public and private interests more fairly. Stricter privacy laws are not the only changes coming. Professional engineering and computer software standards are also changing the design and development landscape for technological innovations.

Various professional standards such as the IEEE P7000 series [42] and the new IEEE P2089 [87] standard for age appropriate digital services for children and P2418.6 [43] – the standard for the framework of distributed ledger technology (DLT) use in healthcare – are all being developed to help address obstacles, gaps and challenges in the digital data marketplace.

In the future, these professional standards exploring the ethical considerations of software engineering could be used in the courts, in conjunction with privacy law to protect consumers and data owners. Standards often add teeth [88] to

professional practices that add illustrative strength to law. These particular standards aim to integrate ethical guides that are meant to protect consumers from the *wild West* [89] markets of the past. In sum, the public can look forward to future benefits in regulation and standards that will challenge decades of laissez faire interests in the private sector.

The blockchain and smart contracts can be the language that frames new relationships between law, genomic data and technology. We ask you to collaborate with us and work together to address both the human and the technological challenges in this complex DNA data marketplace. Together, we can develop a better future between stakeholders to reduce litigation risk while making genomic data analysis safer and more private. Blockchain companies with ethical [67] [90] [91] foundations, like Genobank.io, will be setting themselves apart from others in the market. By offering programmable privacy with NFTs derived from privacy laws' terms and conditions [92], Genobank.io and stakeholders can help provide at least one novel approach to adding transparency and data owner sovereignty to the genomic data marketplace.

Competing interests:
Daniel Uribe is CEO of the company Genobank.io, used as the case study in this paper.

Ethical approval:
Not applicable.

Author's contribution:
Daniel Uribe is the main author.

Funding:
None declared.

Acknowledgements:
This paper was first presented at the 2nd Blockchain International Scientific Conference: ISC2020 at Edinburgh Napier University, Scotland (March 11, 2020). We would like to thank the session chairs and participants for their comments which significantly refined the conceptual landscape. We would also like to acknowledge, in no specific order, the help and guidance shared by the following individuals: Vitalik Buterin; Dulce Villarreal; Dr Naseem Naqvi FRCP, FHEA, MAcadMeded, MSc, FBBA; Dr Mureed Hussain MD, MSc, FBBA; Prof Bill Buchanan OBE, PhD, FBCS; Martin Docherty-Hughes; Dr Sean Manion, PhD; Prof Dr Marc Pilkington PhD; Prof. Daniel Catchpoole, PhD; Prof. Paul Kennedy, PhD; Gustavo Grillasca; Marco Montes; Everardo Barojas; Dr. Luis Garcia Puig; Angelica Estrada; Prof. Dawn Song, PhD and Vishwanath Raman, PhD. Finally, we thank the reviewers for their constructive feedback.

References:

[1] H. I. Ozercan, A. M. Ileri, E. Ayday, and C. Alkan, "Realizing the potential of blockchain technologies in genomics," *Genome Research*, vol. 28, no. 9. Cold Spring Harbor Laboratory Press, pp. 1255–1263, 01-Sep-2018.

[2] L. Goldman and J. Lewis, "See you in court," *Occupational Health*, 2001. [Online]. Available: https://www.genomeweb.com/scan/see-you-court#.Xh4wLUdKiUk. [Accessed: 14-Jan-2020].

[3] "GenoBank – Power of DNA." [Online]. Available: https://genobank.io/#product. [Accessed: 14-Jan-2020].

[4] M. Corrales, P. Jurˇ, and G. Kousiouris, *Legal Tech, Smart Contracts and Blockchain*. 2019.

[5] M. Corrales, P. Jurčys, and G. Kousiouris, "Smart Contracts and Smart Disclosure: Coding a GDPR Compliance Framework," in *Legal Tech, Smart Contracts and Blockchain*, M. Corrales, M. Fenwick, and H. Haapio, Eds. Singapore: Springer Singapore, 2019, pp. 189–220.

[6] C. Blenkinsop, "Non-Fungible Tokens, Explained | Cointelegraph," 2018. [Online]. Available: https://cointelegraph.com/explained/non-fungible-tokens-explained. [Accessed: 14-Jan-2020].

[7] T. Savel, K. Kuzmeskas, C. McFarlane, and M. Ulieru, "Tokens & The Internet of Value: Blending Game Theory, Computer Science, Psychology, and Economics," *Blockchain in Healthcare Today*, 2018. [Online]. Available: https://blockchainhealthcaretoday.com/index.php/journal/article/view/93. [Accessed: 14-Jan-2020].

[8] University of Minnesota, "Lawseq |Genomics Law." [Online]. Available: https://lawseq.umn.edu/. [Accessed: 14-Jan-2020].

[9] E. Chau, "Bill Text - AB-375 Privacy: personal information: businesses. CCPA," *California Legislative Information*, 2018. [Online]. Available: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375. [Accessed: 14-Jan-2020].

[10] D. Roland-Holst *et al.*, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations State of California Department of Justice Office of the Attorney General California Department of Justice Prepared for: Attorney General's Office Contents.* .

[11] European Parliament and Council of the European Union, *Regulation 5419/16 GDPR*, vol. 2016, no. April. 2016, p. 261.

[12] C. Agbo, Q. Mahmoud, and J. Eklund, "Blockchain Technology in Healthcare: A Systematic Review," *Healthcare*, vol. 7, no. 2, p. 56, Apr. 2019.

[13] E. Cantwell, Maria; Klobuchar, A; Markey, "16TH CONGRESS 1ST SESSION Consumer Online Privacy Act COPRA," *Congress.gov*, 2020. [Online]. Available: https://www.cantwell.senate.gov/imo/media/doc/COPRA Bill Text.pdf. [Accessed: 14-Jan-2020].

[14] D. Uribe, "International Workshop Data Protection in Real-Time: Transforming Privacy Law into Real Practice," in *Distributive Biobanking Models: Why Biospecimens Need*, 2019.

[15] Princeton University, "Machine-Language Programming," *Computer Science: An Interdisciplinary Approach*. [Online]. Available: https://introcs.cs.princeton.edu/java/63programming/. [Accessed: 14-Jan-2020].

[16] A. Regalado, "More than 26 million people have taken an at-home ancestry test - MIT Technology Review," *MIT Technology Review*, 2019. [Online]. Available: https://www.technologyreview.com/s/612880/more-than-26-million-people-have-taken-an-at-home-ancestry-test/. [Accessed: 14-Jan-2020].

[17] Y. Liu, "Progress review: genome sequencing - June 2019 - LessWrong 2.0," *Lesswrong.com*, 2019. [Online]. Available: https://www.lesswrong.com/posts/geE9t5Dm9iq6Y7nQ4/progress-review-genome-sequencing-

june-2019. [Accessed: 14-Jan-2020].

[18] D. Netburn, "So many people have had their DNA sequenced that they've put other people's privacy in jeopardy," *Phys.org*, 2018. [Online]. Available: https://phys.org/news/2018-10-people-dna-sequenced-theyve-privacy.html. [Accessed: 14-Jan-2020].

[19] "Global Blockchain in Genomics Market: Focus on Business Models, Services, Applications, End Users, 11 Countries Data, and Competitive Landscape - Analysis and Forecast, 2019-2029."

[20] Y. Erlich, T. Shor, I. Pe'er, and S. Carmi, "Identity inference of genomic data using long-range familial searches," *Science*, vol. 362, no. 6415, pp. 690–694, Nov. 2018.

[21] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 267–278, Jan. 2018.

[22] Future of Privacy Forum, "Comparing privacy laws: GDPR vs CCPA."

[23] "What Businesses Need to Know About the California Consumer Privacy Act," *American Bar Association*, 2019. [Online]. Available: https://www.americanbar.org/groups/business_law/publications/blt/2019/10/ca-consumer-privacy/. [Accessed: 14-Jan-2020].

[24] C.-H. Chen, I. O. S. Press, A. Trappey, M. Peruzzini, J. Stjepandić, and N. Wognum, "Transdisciplinary Engineering: A Paradigm Shift: Proceedings of the 24th ISPE Inc. International Conference on Transdisciplinary Engineering, July 10-14, 2017," 2017. [Online]. Available: http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1640417&lang=es&site=ehost-live&scope=site. [Accessed: 14-Jan-2020].

[25] G. Leeming, J. Cunningham, and J. Ainsworth, "A Ledger of Me: Personalizing Healthcare Using Blockchain Technology," *Frontiers in Medicine*, vol. 6. Frontiers Media S.A., 24-Jul-2019.

[26] M. Wirth, Christian; Kolain, "Privacy by BlockChain Design: A BlockChain-enabled GDPR-compliant Approach for Handling Personal Data," in *Proceedings of the ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies,* 2018, no. 10, pp. 1–8.

[27] Research and Markets, *Global Blockchain In Genomics Market By Type (Public, Federated, Private), By Application (Clinical Trials, IP Management, Drug Discovery, Data storage and security, Others), By Models, By Targets, By End User, By Region, Forecast & Opportunities,* 2025, Technical Report, Research and Markets,, Dublin, IE, May 2020. Accessed on: May 26, 2020. [Online]. Available https://www.researchandmarkets.com/reports/5022662/global-blockchain-in-genomics-market-by-type#pos-1.

[28] "Get Ready, CCPA Is No GDPR Lite - SecurityRoundTable.org." [Online]. Available: https://www.securityroundtable.org/get-ready-ccpa-is-no-gdpr-lite/. [Accessed: 14-Jan-2020].

[29] "US Data Privacy Evolution, California's CCPA is King," National Law Review, 2019. [Online]. Available: https://www.natlawreview.com/article/digital-revolution-takes-new-meaning-among-calls-heightened-us-data-privacy-measures. [Accessed: 14-Jan-2020].

[30] L. Feiner, "Senate Democrats reveal new COPRA digital privacy bill," 2019. [Online]. Available: https://www.cnbc.com/2019/11/26/senate-democrats-reveal-new-copra-digital-privacy-bill.html. [Accessed: 14-Jan-2020].

[31] The Judicial Learning Center, "Why Do We Need Laws? | The Judicial Learning Center," 2015. [Online]. Available: http://judiciallearningcenter.org/law-and-the-rule-of-law/. [Accessed: 14-Jan-2020].

[32] S. Abdukadirov, Ed., Nudge Theory in Action, 1st ed. New York, New York, USA: Palgrave Macmillan, 2016.

[33] E. Genomics and H. Evolutionary, "What is genomics? •," Genome, 2008. [Online]. Available: https://www.news-medical.net/life-sciences/What-is-Genomics.aspx. [Accessed: 15-Jan-2020].

[34] "A reference standard for genome biology," 2018.

[35] D. Roland, "23andMe and GSK are mining customers' DNA data in a hunt for new drugs - MarketWatch," Wall Street Journal, 2019. [Online]. Available: https://www.marketwatch.com/story/23andme-and-gsk-are-mining-customers-dna-data-in-a-hunt-for-new-drugs-2019-07-23. [Accessed: 15-Jan-2020].

[36] "The NIH Is Bypassing Tribal Sovereignty to Harvest Genetic Data From Native Americans - VICE," Vice.com, 2018. [Online]. Available: https://www.vice.com/en_us/article/8xp33a/the-nih-is-bypassing-tribal-sovereignty-to-harvest-genetic-data-from-native-americans. [Accessed: 15-Jan-2020].

[37] L. O. Gostin, "National health information privacy: Regulations under the health insurance portability and accountability act," J. Am. Med. Assoc., vol. 285, no. 23, pp. 3015–3021, Jun. 2001.

[38] L. M. Slaughter, "The Genetic Information Nondiscrimination Act: Why Your Personal Genetics are Still Vulnerable to Discrimination," Surgical Clinics of North America, vol. 88, no. 4. pp. 723–738, Aug-2008.

[39] S. M. Suter, "GINA at 10 years: The battle over 'genetic information' continues in court," J. Law Biosci., vol. 5, no. 3, pp. 495–526, May 2018.

[40] J. K. Wagner, "Disparate impacts and GINA: Congress's unfinished business," *J. Law Biosci.*, vol. 5, no. 3, pp. 527–549, May 2018.

[41] A. M. Yuengert and A. M. Yuengert, *Practical Wisdom and Economic Models of Choice*. Palgrave Macmillan US, 2012.

[42] "IEEE P7000 - Engineering Methodologies for Ethical Life-Cycle Concerns Working Group - IEEE P7000 Working Group," *IEEE*, 2016. [Online]. Available: https://sagroups.ieee.org/7000/. [Accessed: 15-Jan-2020].

[43] "P2418.6 - Standard for the Framework of Distributed Ledger Technology (DLT) Use in Healthcare and the

Life and Social Sciences," *IEEE*. [Online]. Available: https://standards.ieee.org/project/2418_6.html. [Accessed: 15-Jan-2020].

[44] E. W. Clayton, B. J. Evans, J. W. Hazel, and M. A. Rothstein, "The law of genetic privacy: Applications, implications, and limitations," *J. Law Biosci.*, vol. 6, no. 1, pp. 1–36, 2019.

[45] A. Rosic, "What is Blockchain Technology? A Step-by-Step Guide for Beginners," *Journal of Chemical Information and Modeling*, 2013. [Online]. Available: https://blockgeeks.com/guides/what-is-blockchain-technology/. [Accessed: 14-Jan-2020].

[46] H. Shaw, "A Cryptographic System Based upon the Principles of Gene Expression," *Cryptography*, vol. 1, no. 3, p. 21, 2017.

[47] "IPFS Cluster - Pinset orchestration for IPFS." [Online]. Available: https://cluster.ipfs.io/. [Accessed: 14-Jan-2020].

[48] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health Informatics J.*, vol. 25, no. 4, pp. 1398–1411, Dec. 2019.

[49] A. S. Bajaj, *Blockchain and Decentralized Applications.pdf*, Volume 1. Kharkiv, Ukraine: Distributer Lab, 2018.

[50] R. Ribitzky, U. Broedl, C. McFarlane, and K. A. Clauson, "Data Sharing? The Case for Blockchain at the Global Convergence of Healthcare, Life sciences, and Consumer Markets," *Blockchain Healthc. Today*, vol. 0, no. 0, Nov. 2018.

[51] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Application of Blockchain for the Next Generation of Cybersecure Industry 4.0 Smart Factories," *IEEE Access*, 2018.

[52] V. Nair, "What Will The Fourth Generation of Blockchain Look Like?," *Hakernoon*, 2019. [Online]. Available: https://hackernoon.com/what-will-the-fourth-generation-of-blockchain-look-like-daa5a4e90c59. [Accessed: 14-Jan-2020].

[53] "Blockchain Use Cases in 2020: Real World Industry Applications," *Consensys.com*, 2020. [Online]. Available: https://consensys.net/blockchain-use-cases/. [Accessed: 14-Jan-2020].

[54] Deloitte, "Deloitte's 2019 global blockchain survey," 2019.

[55] I. Barclay, A. D. Preece, I. Taylor, and D. Verma, "A conceptual architecture for contractual data sharing in a decentralised environment," in *Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications*, 2019, p. 15.

[56] O. Choudhury *et al.*, "Enforcing Human Subject Regulations using Blockchain and Smart Contracts," *Blockchain Healthc. Today*, Mar. 2018.

[57] H. D. Zubaydi, Y. W. Chong, K. Ko, S. M. Hanshi, and S. Karuppayah, "A review on the role of blockchain technology in the healthcare domain," *Electron.*, vol. 8, no. 6, pp. 1–29, 2019.

[58] M. D. Sorani *et al.*, "Genetic Data Sharing and Privacy," *Neuroinformatics*, vol. 13, no. 1, pp. 1–6, Jan. 2014.

[59] X. L. Jin, M. Zhang, Z. Zhou, and X. Yu, "Application of blockchain platform to manage and secure personal genomic data: A case study of lifecode.AI in China," *J. Med. Internet Res.*, vol. 21, no. 9, 2019.

[60] R. M. Hendricks-Sturrup and C. Y. Lu, "Direct-to-consumer genetic testing data privacy: Key concerns and recommendations based on consumer perspectives," *J. Pers. Med.*, vol. 9, no. 2, 2019.

[61] T. K. Mackey *et al.*, "'Fit-for-purpose?' - Challenges and opportunities for applications of blockchain technology in the future of healthcare," *BMC Med.*, vol. 17, no. 1, 2019.

[62] D. Grishin *et al.*, "Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation," *Blockchain Healthc. Today*, vol. 1, pp. 1–23, 2018.

[63] T. Nugent, D. Upton, and M. Cimpoesu, "Improving data transparency in clinical trials using blockchain smart contracts," *F1000Research*, vol. 5, 2016.

[64] A. M. Ileri, H. I. Ozercan, A. Gundogdu, A. K. Senol, M. Y. Ozkaya, and C. Alkan, "Coinami: A Cryptocurrency with DNA Sequence Alignment as Proof-of-work," Feb. 2016.

[65] M. Jones, M. Johnson, M. Shervey, J. T. Dudley, and N. Zimmerman, "Privacy-preserving methods for feature engineering using blockchain: Review, evaluation, and proof-of-concept," *J. Med. Internet Res.*, vol. 21, no. 8, p. e13600, Aug. 2019.

[66] E. Ahmed and M. Shabani, "DNA Data Marketplace: An Analysis of the Ethical Concerns Regarding the Participation of the Individuals," *Front. Genet.*, vol. 10, no. November, pp. 1–6, 2019.

[67] R. J. Cadigan, E. Juengst, A. Davis, and G. Henderson, "Underutilization of specimens in biobanks: an ethical as well as a practical concern?," *Genet. Med.*, vol. 16, no. 10, pp. 738–740, Oct. 2014.

[68] J. J. Roberts and N. Rapp, "Lost Bitcoins: 4 Million Bitcoins Gone Forever Study Says | Fortune," *Fortune*, 2017. [Online]. Available: http://fortune.com/2017/11/25/lost-bitcoins/. [Accessed: 16-Apr-2020].

[69] "Squarelink Rolls Out Non-Custodial Private Key Recovery for New Wave of DApps | Business Wire," *Business Wire*, 2020. [Online]. Available: https://www.businesswire.com/news/home/20191202005335/en/Squarelink-Rolls-Non-Custodial-Private-Key-Recovery-New. [Accessed: 16-Apr-2020].

[70] R. U. I. Guo, H. Shi, Q. Zhao, and D. Zheng, "Special Section on Research Challenges and Opportunities in Security and in Electronic Health Records SystemsSecure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain," *IEEE Access*, vol. 6, 2018.

[71] D. Nuñez, I. Agudo, and J. Lopez, "Proxy Re-

Encryption: Analysis of constructions and its application to secure access delegation," *J. Netw. Comput. Appl.*, vol. 87, pp. 193–209, 2017.

[72] F. Briscoe, "Innovations in Medical Genomics: What Are the Privacy and Security Risks?," 2017.

[73] D. Nunez, "Umbral: A Threshold Proxy Re-Encryption Scheme," *Github*, 2018. [Online]. Available: https://raw.githubusercontent.com/nucypher/umbral-doc/master/umbral-doc.pdf. [Accessed: 17-Apr-2020].

[74] A. Shamir, "How to Share a Secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[75] Cryptokitties, "CryptoKitties | Collect and breed digital cats!," *Cryptokitties.Com*, 2018. [Online]. Available: https://www.cryptokitties.co/about. [Accessed: 16-Apr-2020].

[76] M. Bal and C. Ner, "NFTracer: A Non-Fungible Token Tracking Proof-of-Concept Using Hyperledger Fabric," 2019.

[77] S. Chevet, "Blockchain Technology and Non-Fungible Tokens: Reshaping Value Chains in Creative Industries," 2018.

[78] K. Tut, "NFT and IPFS | Pinata," *Medium*, 2020. [Online]. Available: https://medium.com/pinata/who-is-responsible-for-nft-data-99fb4e8147e4. [Accessed: 16-Apr-2020].

[79] "solidity - ERC721 owned Tokens array length limitations on owners with thousands of tokens - Ethereum Stack Exchange." [Online]. Available: https://ethereum.stackexchange.com/questions/41937/erc721-ownedtokens-array-length-limitations-on-owners-with-thousands-of-tokens. [Accessed: 17-Apr-2020].

[80] "Developer Spotlight: Genobank.io - Oasis Labs - Medium." [Online]. Available: https://medium.com/oasislabs/developer-spotlight-genobank-io-7ebeb96dd0d2. [Accessed: 15-Jan-2020].

[81] R. Cheng *et al.*, "Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts."

[82] "State Agency & Regional Office CLIA Contacts | CMS." [Online]. Available: https://www.cms.gov/Regulations-and-Guidance/Legislation/CLIA/State_Agency_and_Regional_Office_CLIA_Contacts. [Accessed: 15-Jan-2020].

[83] HIPAA, "Legal News," *HIPAA JOURNAL*, 2020. [Online]. Available: https://www.hipaajournal.com/category/legal-news/. [Accessed: 15-Jan-2020].

[84] Y. Huang, "An Environment-Wide Study of Adult Cognitive Performance in the 23andMe Cohort," *medRxiv*, vol. 60, 2019.

[85] C. Loizos, "23andMe underscores that privacy-loving customers need to opt out of its data deal with GlaxoSmithKline | TechCrunch," *TechCrunch*, 2018. [Online]. Available: https://techcrunch.com/2018/09/05/23andme-underscores-that-privacy-loving-customers-need-to-opt-out-of-its-data-deal-with-glaxosmithkline/. [Accessed: 15-Jan-2020].

[86] R. Kain *et al.*, "Database shares that transform research subjects into partners," *Nat. Biotechnol.*, vol. 37, no. 10, pp. 1112–1115, Oct. 2019.

[87] "P2089 - Standard for Age Appropriate Digital Services Framework - Based on the 5Rights Principles for Children," *IEEE*. [Online]. Available: https://standards.ieee.org/project/2089.html. [Accessed: 15-Jan-2020].

[88] P. Cihon, "Standards for AI Governance: International Standards to Enable Global Coordination in AI Research & Development," 2019.

[89] Northeastern University, "The Wild West of IoT: Regulating Uncharted Territory - Level at Northeastern University | Blog," *Level*, 2019. [Online]. Available: https://www.northeastern.edu/levelblog/2018/04/11/wild-west-iot-regulating-uncharted-territory/. [Accessed: 15-Jan-2020].

[90] S. Spiekermann, J. Korunovska, and M. Langheinrich, "Inside the Organization: Why Privacy and Security Engineering Is a Challenge for Engineers," *Proc. IEEE*, vol. 107, no. 3, pp. 600–615, 2019.

[91] J. Hooker, "Ethics of Artificial Intelligence," *Tak. Ethics Seriously*, pp. 211–219, 2018.

[92] American Society of Human Genetics, "New file type improves genomic data sharing while maintaining participant privacy -- ScienceDaily," *Science Daily*, 2018. [Online]. Available: https://www.sciencedaily.com/releases/2018/10/181017141005.htm. [Accessed: 15-Jan-2020].

