MORE BLOCKCHAIN MORE PRIVACY PROBLEMS: PRIVACY RIGHTS & THE MOSAIC THEORY IN THE AGE OF BLOCKCHAIN TECHNOLOGY

Carson Lloyd*

Cite as: Carson Lloyd, *More Blockchain More Privacy Problems: Privacy Rights & The Mosaic Theory in the Age of Blockchain Technology*, 32 RICH. J.L. & TECH. 34 (2025)

* Carson Lloyd is a PhD Researcher at the University of Birmingham and Visiting Lecturer at Birmingham City University. The author's research examines the intersection of individual privacy rights and emerging technologies. This article investigates how courts and legislatures at the federal and state levels in the United States, focusing on the state of California and the healthcare sector, have responded to the privacy concerns posed by blockchain technology. Applying the mosaic theory of privacy as a lens, this article assesses whether existing legal frameworks can keep pace with rapid technological innovation. It is concluded that while U.S. courts and legislatures have largely failed to address blockchain's privacy concerns, emphasising how technology will likely continue to outpace the law, future federal legislation may still offer meaningful solutions. The author extends special thanks to the Centre for American Legal Studies at Birmingham City University.

ABSTRACT

Can the law tackle the legal challenges posed by disruptive technologies, or is the law constantly struggling to keep up with rapid innovation, forcing it into a reactive position? This question lies at the heart of the complex relationship between law and technology. As emerging technologies advance at an unprecedented rate, legal systems often struggle to address the challenges they pose. There is no better example of this in practice than the emergence of blockchain technology, one of the most disruptive innovations of the 21st Century. Blockchain technology refers to a decentralized and encrypted digital ledger enabling secure real-time transactions without a central authority. The applications of blockchain, though predominantly recognized in the financial sector for cryptocurrency, extend to various non-financial domains, including healthcare. Blockchain technology offers transformative opportunities, but also raises legal complexities, particularly regarding individual privacy rights and data protection. While current blockchain scholarship focuses on its criminal use and broad applications in cryptocurrency, this article contributes to the gap by investigating how courts and legislatures at a federal and state level in the United States have responded to the privacy concerns posed by blockchain technology.

First, this article will apply the mosaic theory of privacy as a lens to determine if its application is a) possible, b) likely to be a sensible response to privacy concerns and c) whether case law indicates that arguments based on mosaic theory are likely to find favour with the courts. The mosaic theory, a principle of Fourth Amendment privacy, suggests that even non-intrusive individual data points may, when aggregated, form a detailed mosaic of personal information. Second, this article will address how federal and state legislation in the United States operate to protect individual privacy rights and how adequate these may be. This article focuses on the federal healthcare sector, highlighting blockchain's privacy challenges beyond finance, and the state of California, chosen for its large population and pioneering privacy laws, the California Consumer Privacy Act and the California Privacy Rights Act.

This article concludes that while U.S. courts and legislatures have largely failed to address blockchain's privacy concerns, technology will likely continue to outpace the law, though federal legislation, when eventually enacted, may still offer meaningful solutions to these challenges.

Table of Contents

I. INTRODUCTION

[1] Blockchain technology has emerged as one of the most transformative forces of the 21st Century, fundamentally altering how digital transactions and data storage are managed. Blockchain technology can be understood as a means of real-time record-keeping through a decentralized digital ledger.[1] This ledger is encrypted and distributed, allowing multiple parties to transact securely without relying on a central authority.[2] Over recent years, public adoption of blockchain technology has surged. Forbes magazine, for example, estimated that, by the end of 2021, nearly 300 million people globally would own a form of cryptocurrency, underscoring the technologies growing worldwide impact.[3] Beyond the financial industry, the applications of blockchain technology extend across a broad spectrum of non-financial industries from supply chains to healthcare and identification management, reflecting its potential to affect multiple sectors.[4] Yet, amidst this rapid expansion, concerns regarding privacy and data protection still loom.

[2] As blockchain continues to disrupt industries, important questions emerge about how these transformative capabilities intersect with privacy rights and legal frameworks in the United States. While much of the current blockchain scholarship focuses on its criminal uses,

---

[1] Michael Rennock et al., *Blockchain Technology and Regulatory Investigations,* PRAC. LAW at 35, 36–38 (Feb. 1., 2018), https://www.steptoe.com/a/web/171269/3ZEKzc/lit-febmar18-feature-blockchain.pdf [https://perma.cc/Q64D-7LSU]. *See also* CHRIS JAIKARAN, CONG. RSCH. SERV., R45116, BLOCKCHAIN: BACKGROUND AND POLICY ISSUES 1–2 (2018); *Fintech: Financial Technology Research Guide-Cryptocurrency & Blockchain Technology*, LIBRARY OF CONG., https://guides.loc.gov/fintech/21st-century/cryptocurrency-blockchain [https://perma.cc/3SW8-9TXX].

[2] *Fintech: Financial Technology Research Guide*, *supra* note 1.

[3] Andrew Michael, *Cryptocurrency Statistics 2025*, FORBES (Oct. 8, 2024, 9:19 PM), https://www.forbes.com/advisor/au/investing/cryptocurrency/cryptocurrency-statistics/ [https://perma.cc/6QTU-HQHD].

[4] KRISTEN BUSCH, CONG. RSCH. SERV., R47064, BLOCKCHAIN: NOVEL PROVENANCE APPLICATIONS 20 (2022).

such as money laundering,[5] as well as its broad applications in cryptocurrency,[6] there remains a significant gap in legal and academic discourse regarding the privacy implications of blockchain technology.[7] This article aims to address this gap by investigating how courts and legislatures at both a federal and state level in the United States have responded to the privacy concerns of blockchain technology. This article investigates privacy issues in blockchain technology through two principal approaches: First, it applies the mosaic theory of privacy as a lens to determine if its application is a) possible, b) likely to be a sensible response to privacy concerns, and c) whether case law indicates that arguments based on mosaic theory are likely to find favour with the courts. The mosaic theory, a principle of Fourth Amendment privacy, suggests that even non-intrusive individual data points may, when aggregated, form a detailed mosaic of personal information.[8]

[3] Second, this article aims to address how federal and state legislation in the United States operate to protect individual privacy rights and how adequate these may be. The federal sector of healthcare has been selected for this article to emphasise that the privacy concerns of blockchain technology go beyond the financial sector as blockchain may be used for data management and the handling of sensitive medical information. In addition, the State of California has been chosen, as not only does this state have the largest population in the United States,[9] it

[5] *See, e.g.*, Averie Brookes, *U.S. Regulation of Blockchain Currencies: A Policy Overview*, 9 AM. U. INTELL. PROP. BRIEF. 75, 77–86 (2018).

[6] *See, e.g.*, Sarah Jane Hughes, *Do Blockchain Technologies Make Us Safer? Do Cryptocurrencies Necessarily Make Us Less Safe*? 55 TEX. INT'L L. J. 373, 377 (2020).

[7] *See, e.g.*, Michael Herbert Ziegler et al., *A Systematic Literature Review of Information Privacy in Blockchain Systems*, 5 J. CYBERSECURITY & PRIV. 65, 66 (2025) (emphasizing the fact that multiple systematic review's focus on crypto-currencies and that a review of privacy properties beyond electronic cash is necessary).

[8] Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, *in* SUP. CT. REV. 205, 205–06 (2015).

[9] *U.S. Census Bureau Most Populous,* CENSUS.GOV, https://www.census.gov/popclock/ [https://perma.cc/ZXP2-P757].

has also implemented the "first"[10] and "most comprehensive"[11] state privacy laws to date, the California Consumer Privacy Act[12] and the California Privacy Rights Act.[13]

[4] In the same way that Georges Seurat or Paul Signac, pointillist artists, used countless individual brushstrokes to create a unified scene[14] and the mosaic theory builds understanding from fragments of information, sections I to IV of this paper collectively piece together a complex picture of a legal landscape struggling to keep pace with rapid technological advancement. This assembled landscape reveals significant gaps, particularly in protecting individual privacy rights. While the federal legislature holds the authority to construct a comprehensive framework to address these privacy concerns, the pace of technological innovation suggests that law may always lag slightly behind, perpetually filling in a picture that is never fully complete.[15] Nevertheless, just as each stroke in Seurat's painting ultimately contributes to a cohesive image, even delayed federal legislation could eventually help form a solution to address the privacy concerns raised by blockchain technology.

---

[10] STEPHEN P. MULLIGAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., DATA PROTECTION AND PRIVACY LAW: AN INTRODUCTION (2022).

[11] PRITESH SHAH ET AL., *Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies*, PRAC. LAW (2023).

[12] California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (effective Jan. 1, 2025).

[13] California Consumer Privacy Act of 2018, *amended by*, the California Privacy Rights Act of 2020, CAL. CIV. CODE § 1798.100 (effective Jan. 1, 2023).

[14] Dita Amory, *Georges Seurat (1859-1891) and Neo-Impressionism*, THE MET (Oct. 1, 2004), https://www.metmuseum.org/essays/georges-seurat-1859-1891-and-neo-impressionism [https://perma.cc/Z7ZB-FM28] (explaining Georges Seurat and Paul Signac were French painters well-known for helping to develop neo-impressionism, a style characterized by divisionism, the separation of color through individual strokes of pigment, and pointillism, the application of precise dots of paint that collectively reveal a scene).

[15] *See, e.g.*, *Regulation and Legislation Lag Behind Constantly Evolving Technology*, BL (Sept. 27, 2019), https://pro.bloomberglaw.com/brief/regulation-and-legislation-lag-behind-technology/ [https://perma.cc/7PJC-SUK2].

[5] This article proceeds in four parts. Section I provides a foundational understanding of blockchain technology and its associated privacy concerns in the legal context of the United States. Section I also explores the legislative and constitutional frameworks that underpin individual privacy rights in the United States, providing context for the subsequent sections. Building upon this foundation, Section II explores the mosaic theory of privacy and its application by the courts to technology from its evolution in national security case law[16] to the Supreme Court's decision in *U.S. v. Gratkowski* (2020).[17] Section II also includes a discussion of whether arguments based on the mosaic theory are likely to find favour with the courts. Next, Section III shifts the focus of the article to the healthcare sector, examining the enforcement of privacy rights in relation to blockchain technology and federal legislation such as Health Insurance Portability and Accountability Act 1996[18] and the Health Information and Technology for Economic and Clinical Health Act 2009.[19] Section IV evaluates California's privacy legislation, including the California Consumer Privacy Act[20] and the California Privacy Rights Act,[21] and addresses the adequacy of the 'patchwork' approach to privacy protection.

[16] *See* United States v. Marchetti, 466 F.2d 1309 (4th Cir. 1972); Halkin v. Helms, 598 F.2d 1 (D.C. Cir. 1978); CIA v. Sims, 471 U.S. 159 (1985).

[17] United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020).

[18] Health and Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[19] Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111-5, Div A Title XIII, Div B Title IV, 123 Stat. 226 (2009) (codified in scattered sections of 42 U.S.C.).

[20] California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 *et seq*. (eff. until Jan. 1, 2023).

[21] California Consumer Privacy Act of 2018, *amended by*, the California Privacy Rights Act of 2020, CAL. CIV. CODE § 1798.100 (effective Jan. 1, 2023).

II. AN OVERVIEW OF BLOCKCHAIN TECHNOLOGY, PRIVACY CONCERNS & INDIVIDUAL PRIVACY RIGHTS IN THE U.S.

[6] Prior to any legal analysis, it is necessary to first establish a clear understanding of blockchain technology and its implications for privacy within the United States. This section starts by outlining the core principles and functions of blockchain, then explores its applications and corresponding legal ramifications, with a focus on privacy concerns. Finally, it provides an overview of the legislative and constitutional frameworks that govern privacy rights in the U.S. Ultimately, this context will reveal that as blockchain technology continues to evolve and gain widespread adoption, it is essential for Congress to prioritize addressing privacy challenges through federal legislation to ensure that legal frameworks effectively protect individual privacy rights.

A. What is Blockchain Technology?

[7] In 2008, 'Satoshi Nakamoto' published the White Paper, '*Bitcoin: A Peer-to-Peer Electronic Cash System'* which developed a protocol for a peer-to-peer electronic cash system.[22] This protocol later led to the establishment of 'Bitcoin' the cryptocurrency blockchain network. Cryptocurrency refers to a virtual currency used as payment for goods and services digitally exchanged by users via blockchain technology.[23] It has been argued that Nakamoto's White Paper provides the foundation for distributed ledgers, also known as blockchain, as well as generating the common false perception that blockchain technology is solely associated with cryptocurrency.[24] The applications of blockchain technology span many non-financial industries worldwide

[22] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN (2008) http://satoshinakamoto.me/bitcoin.pdf [https://perma.cc/6HYM-83G4].

[23] *Digital Assets,* IRS, https://www.irs.gov/businesses/small-businesses-self-employed/digital-assets#:~:text=A%20cryptocurrency%20is%20an%20example,real%20currencies%20or%20digital%20assets [https://perma.cc/HAF5-BZ3V].

[24] *Fintech: Financial Technology Research Guide*, LIBRARY OF CONG., https://guides.loc.gov/fintech/21st-century/cryptocurrency-blockchain [https://perma.cc/4JQ2-PFDB].

including healthcare record management, supply chain management as well as identity and credential management.[25] Existing literature provides no singular definition for blockchain technology.[26]

[8] This article proposes that blockchain technology may be explained as a means for real-time record-keeping that uses a digital ledger, which is encrypted, distributed, and allows for parties to transact without the use of a central authority as a trusted intermediary.[27] The information stored and recorded in 'blocks' of data depends on the specific application of the blockchain. The Congressional Research Service (CRS) comments that a blockchain is tamper-resistant as a 'block' of data is cryptographically 'chained' to the previous one.[28] Moreover, the data stored on a blockchain is continually distributed, replicated and synchronised across 'nodes'.[29] The CRS also suggests that blockchain is not a new technology, but rather creates a novel type of database with existing technology including: Asymmetric Key Encryption, Hashes, Merkle Trees, Peer-to-Peer networks, and a Consensus Mechanism.[30]

[9] The type of blockchain will impact both the level of freedom for users to add data to the blockchain and the recorded data's accessibility.

---

[25] BUSCH, *supra* note 4. *See also* U.S. GOV'T. ACCOUNTABILITY OFF., GAO-22-104625, BLOCKCHAIN: EMERGING TECHNOLOGY OFFERS BENEFITS FOR SOME APPLICATIONS BUT FACES CHALLENGES 10-21 (2022).

[26] Within existing literature, each scholar places emphasis on different attributes when defining blockchain technology. *See, e.g.*, Rennock et al., *supra* note 1; JAIKARAN *supra* note 1; *Fintech: Financial Technology Research Guide*, *supra* note 1. *See also,* Sangita F. Gazi, *In Code We Trust: Blockchain's Decentralization Paradox*, 27 VAND. J. ENT. & TECH. L. 59, 61 (2024) (emphasizing that blockchain technology lacks a singular precise definition).

[27] Rennock et al., *supra* note 1. *See also* JAIKARAN *supra* note 1, at 1-3; *Fintech: Financial Technology Research Guide*, *supra* note 1.

[28] BUSCH, *supra* note 4, at 1–3.

[29] *Id.* (defining nodes as individual computer systems or specialized hardware that communicate with each other and store and process data.).

[30] *Id*. at 7; JAIKARAN *supra* note 1, at 1–3.

The literature suggests that whilst a public blockchain is open and accessible to all users, private blockchains are open only to a designated subset such as pre-approved members.[31] Furthermore, a permissionless blockchain allows all members to add data as opposed to a permissioned blockchain which restricts this right to pre-permitted individuals.[32]

[10] The literature importantly comments that the technological components of blockchain mean that all types of blockchain share the following core characteristics: 1) no central authority, 2) immutability, as blockchain records are unalterable, and 3) pseudonymity, as blockchain users do not need to reveal their true identity.[33]

B. The Privacy Concerns of Blockchain Technology

[11] Whilst blockchain's characteristics may be credited as contributing to its popularity, they also pose concerns for individual privacy rights. The CRS notes that blockchain may have ramifications for user privacy and security, as any data added to a public permissionless blockchain, such as healthcare records, which will be viewable to all participating nodes indefinitely as a result of blockchain's immutable nature.[34] Additionally, Pritesh Shah, partner at the law firm Davis Polk, and his co-authors as well as Rebecca Harris, writing in the Loyola of Los Angeles Law Review comment that the immutable nature of blockchain technology, whilst providing the benefit of making information virtually tamper-resistant, presents further individual privacy concerns as this conflicts with California's data privacy laws.[35] These laws include the right to correct and delete

[31] BUSCH, *supra* note 4, at 5–7.

[32] *Id*. at 5-6; PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW, THE RULE OF CODE 31–32 (Harvard University Press, 2019).

[33] BUSCH, *supra* note 4, at 1; DE FILIPPI & WRIGHT, *supra* note 342at 33. *See also* SHAH ET AL., *supra* note 11.

[34] BUSCH, *supra* note 4, at 20.

[35] *See generally* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100, 199; *see also* California Privacy Rights Act of 2020, CAL. CIV. CODE §§ 1798.100-1798.199.100 (eff. from Jan. 1, 2023). *See also California Consumer*

information.[36] Blockchain also increases the risk of the disclosure of sensitive data, such as patient data, and the loss of confidentiality where its encryption is cracked, which has led the Centre for Strategic and International Studies, an American think tank, to state that biometric and personal information should never be stored on the blockchain.[37]

[12] As blockchain is still within the early phase of development, Chris Jaikaran, a cybersecurity policy analyst, has pointed out that legislators possess a limited understanding in relation to the technological applications and functions of blockchain technology.[38] Pritesh Shah and co-authors also suggest that whilst aspects of blockchain seek to protect or mitigate privacy issues, such as the use of encryption and verification of data integrity, legislators have not focused on blockchain technology and its associated technological features when drafting data privacy laws and frameworks.[39]

[13] Within the United States, blockchain technology is commonly used by the public. The Morning Consult Report indicates that one in six U.S. household's own cryptocurrency is secured via blockchain

Privacy Act (CCPA), CAL. OFF. ATT'Y. GEN. (May 10, 2023), https://oag.ca.gov/privacy/ccpa#:~:text=The%20California%20Consumer%20Privacy%20Act,how%20to%20implement%20the%20law [https://perma.cc/A8B4-QFR4].

[36] SHAH ET AL., *supra* note 11, at 6; Rebecca Harris, *Forging a Path Towards Meaningful Digital Privacy: Data Monetization and the CCPA*, 54 LOY. L.A. L. REV. 197, 214 (2020).

[37] William Crumpler, *The Human Rights Risks and Opportunities in Blockchain*, CTR. FOR STRATEGIC AND INT'L STUDIES 5 (Dec. 2021), https://www.csis.org/analysis/human-rights-risks-and-opportunities-blockchain [https://perma.cc/ET6C-E7KD].

[38] *Beyond Bitcoin: Emerging Applications for Blockchain Technology*: *Hearing Before the Subcomm. on Oversight & Subcomm. on Rsch. and Tech. of the H. Comm. on Sci., Space, and Tech.*, 115th Cong. 8–9 (2018) (statement of Chris Jaikaran, Cybersecurity Policy Analyst); *see also* U.S. GOV'T. ACCOUNTABILITY OFF., GAO-22-104625, BLOCKCHAIN: EMERGING TECHNOLOGY OFFERS BENEFITS FOR SOME APPLICATIONS BUT FACES CHALLENGES 20 (2022).

[39] SHAH ET AL., *supra* note 11, at 3. *See also* Laya Aminizadeh, *The Blockchain Technology and Legal Challenges*, 2020 REV. FAC. DREPT ORADEA 139 (2020).

technology.[40] Therefore, the emergence of blockchain technology presents concerns for individual privacy rights which must be tackled by the legal framework of the U.S.

C. Individual Privacy Rights in the U.S.

i. Legislative Protection

[14] The U.S. Constitution establishes a federal system of governance in which the federal government and the government of each state must co-exist. The federal system of governance means that privacy rights legislation is 'patchwork' in manner, meaning at a federal level, the legislation adopted will vary according to sector. For instance, in the healthcare sector, the Health Insurance Portability and Accountability Act 1996[41] operates to ensure privacy standards for individuals' medical records, whereas in the financial sector legislation includes the Bank Secrecy Act 1970.[42] However, at the state level, several states have acted to expand individual privacy protections in response to the federal approach, with California, for example, enacting the Consumer Privacy Rights Act 2020.[43]

ii. Constitutional Protection

[15] The overriding function of the Fourth Amendment of the U.S. Constitution is to protect individuals' right to privacy and freedom from unreasonable government intrusions.[44] The Fourth Amendment provides:

---

[40] Christine Principato et al., *Report: U.S. Public Opinion on Cryptocurrency*, MORNING CONSULT (July 2022), https://pro.morningconsult.com/analyst-reports/state-of-cryptocurrency [https://perma.cc/E89M-G7BM].

[41] Health and Insurance Portability and Accountability Act, *supra* note 18.

[42] Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1118 (1970).

[43] California Privacy Rights Act of 2020, CAL. CIV. CODE §§ 1798.100-1798.199.100 (eff. from Jan. 1, 2023).

[44] 68 AM. JUR. 2D *Searches and Seizures* § 5, Westlaw (database updated May 2025).

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*[45]

The U.S. Supreme Court has evolved its approach to individual privacy protections afforded by the Fourth Amendment and what constitutes a 'search.' Prior to 1928, Fourth Amendment protections were limited to physical trespassing and intrusion on "persons, houses, papers and effects."[46] The Supreme Court held in *Olmstead v. U.S.* (1928) that the wiretapping of public telephones did not constitute a search under the meaning of the Fourth Amendment as conversations were intangible and no physical entry was made to the defendant's property.[47]

[16] However, in *U.S. v. Katz* (1967),[48] the Supreme Court held that the Fourth Amendment protects "people, not places,"[49] thereby representing a shift from earlier jurisprudence. Justice Stewart's majority opinion reasoned that what a person knowingly exposes in public is not afforded Fourth Amendment protection.[50] However, what a person seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[51] Therefore, as demonstrated in *Katz*, the recording of the telephone conversation on a public telephone infringed the defendant's Fourth Amendment rights, as the

[45] U.S. CONST. amend. IV.

[46] *Id.*

[47] Olmstead v. United States, 277 U.S. 438, 466 (1928).

[48] Katz v. United States, 389 U.S. 347 (1967).

[49] *Id.* at 351.

[50] *Id.*

[51] *Id.*

defendant justifiably relied upon privacy while using the telephone booth.[52]

[17] Justice Harlan's concurring opinion in *Katz* introduced a two-part test to determine whether a search has occurred.[53] The test affords Fourth Amendment protection where it is demonstrated that 1) a subjective expectation of privacy exists, and 2) that the expectation is one that society is prepared to recognise as reasonable and legitimate.[54] In *Katz*, Justice Harlan concluded that both prongs of this test were met because society recognised a telephone booth as a place where the occupant has a reasonable expectation of privacy and the defendant subjectively acted to preserve privacy by shutting the booth door.[55] Justice Harlan's two-part 'reasonable expectation' test remains relevant in determining whether an individual's privacy rights may be protected by the Fourth Amendment in relation to technological surveillance.

[18] Following *Katz*, in *U.S. v. Knotts* (1983), the Supreme Court upheld that the use of hidden beepers to monitor a suspect's vehicle did not invade any legitimate expectation of privacy under the Fourth Amendment as a person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy.[56] Later, in *Kyllo v. U.S.* (2001) the Supreme Court held that an unreasonable Fourth Amendment 'search' may occur where the government uses devices not publicly available, such as a thermal imaging device, absent a warrant, to explore details of a private home which are not knowable absent physical instruction.[57]

[19] An exception to Justice Harlan's *Katz* test exists under the third-party doctrine, which proposes that there is no expectation of privacy

[52] *Id*. at 353.

[53] Katz, 389 U.S. 347, 361 (Harlan, J., concurring).

[54] *Id*.

[55] *Id.* at 60–61.

[56] United States v. Knotts, 460 U.S. 276, 280–81 (1983).

[57] Kyllo v. United States, 533 U.S. 27, 40 (2001).

where information is voluntarily provided to others. The Supreme Court first articulated this doctrine in *U.S. v. Miller* (1976), where Justice Powell reasoned that the bank depositor held no Fourth Amendment interest as bank records were negotiable instruments which contained information voluntarily conveyed to the bank and exposed to employees in the ordinary course of business.[58] Moreover, the third party doctrine was held to also apply to telephone records in *Smith v. Maryland* (1979), as a person has no legitimate expectation of privacy in information voluntarily turned over to third parties.[59]

[20] The mosaic theory of privacy emerged within privacy jurisprudence in 2010 as a result of a need to respond to privacy concerns associated with technological advancements in surveillance.[60] The mosaic theory of the Fourth Amendment posits that a person's reasonable expectation of privacy may exist when multiple pieces of public information, which by themselves alone would not be invasive, are combined to produce a mosaic of private information,[61] demonstrating that the "whole is greater than the sum of the individual parts."[62] This theory may be more simply explained as the notion that "the government can learn more from a given slice of information if it can put that information in the context of a broader pattern, a mosaic."[63] Professors Gray and Citron provide a useful example of the mosaic theory when commenting "although a collection of dots is sometimes nothing more than a collection of dots, some collections of dots, when assessed holistically, are a Sunday Afternoon on the Island of La Grande Jatte."[64]

---

[58] United States v. Miller, 425 U.S. 435, 442 (1976).

[59] Smith v. Maryland, 442 U.S. 735, 745 (1979).

[60] *See* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd in part sub nom*., United States v. Jones, 565 U.S. 400 (2012).

[61] Kugler & Strahilevitz, *supra* note 8, at 205.

[62] *Maynard*, 615 F.3d at 558.

[63] Kugler & Strahilevitz, *supra* note 8, at 205.

[64] David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH.

D. Interim Conclusions

[21] Blockchain technology has revolutionized digital transactions, yet it also brings forth notable privacy concerns due to its immutable nature and heightened potential for sensitive data exposure. Therefore, the emergence of blockchain technology presents concerns for individual privacy rights which must be tackled by the legal framework of the U.S. However, the 'patchwork' nature of privacy legislation and evolving interpretation of constitutional protections indicates the complexity of ensuring individual privacy rights in the digital age.

III. THE MOSAIC THEORY OF PRIVACY & BLOCKCHAIN TECHNOLOGY

[22] This section aims to fill a notable gap in the literature by examining the intersection of the mosaic theory and blockchain technology, offering insights into whether the mosaic theory is a) applicable, b) a sensible response to privacy concerns, and c) likely to gain acceptance in the courts. Each of the following sub-sections build upon one another to answer these three questions. Taken together, it is revealed that the reluctance of the U.S. Supreme Court to fully endorse the mosaic theory has divided lower courts, with practical challenges and legislative considerations further undermining its viability as a response to privacy, as evidenced by the recent blockchain ruling of *U.S. v. Gratkowski* (2020).[65]

A. Origins of the Mosaic Theory

[23] The mosaic theory does not originate from Fourth Amendment jurisprudence, but from national security case law. Professor at Columbia Law School, David Pozen, comments that the mosaic theory

381, 415 (2013). 'A Sunday Afternoon on the Island of La Grande Jatte' refers to a painting by Georges Seurat in which individual dots are formed in a way to create a scene when viewed as a whole. *See A Sunday on La Grande Jatte*, ART INST. OF CHI., https://www.artic.edu/artworks/27992/a-sunday-on-la-grande-jatte-1884 [https://perma.cc/HQB6-7U3V].

[65] *See, e.g.,* United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020).

in the context of national security describes when disparate items of information that are individually of limited or of no utility to their possessor are given significance through being combined with other items of information to reveal interrelationships and "analytic synergies" so that the mosaic information is worth the sum of its parts.[66] In particular, Pozen points out that the mosaic theory suggests the potential for an adversary to deduce from independently innocuous facts a strategic vulnerability which is exploitable for malevolent ends.[67]

[24] Since 1972, the courts have favoured arguments based on the mosaic theory in relation to cases involving national security. In *U.S. v. Marchetti* (1972), the mosaic theory was first articulated when the federal government pursued an injunction against the publication of a book by a former C.I.A. agent.[68] The Fourth Circuit upheld the injunction on secrecy grounds.[69] However, Chief Judge Haynsworth's reasoning gave merit to what has become known as the mosaic theory when commenting that the significance that one item of information may provide depends upon the knowledge of many items of information.[70] In particular, what may seem trivial to the uninformed may appear "of great moment" to a person with a broad picture of the scene and put the questioned item into its proper context.[71]

[25] The D.C. Circuit Court in *Halkin v. Helms* (1978) upheld the government's denial of a discovery of information request brought by former Vietnam War protesters on secrecy grounds.[72] However, in justifying this decision, Circuit Judge Robb built upon Chief Judge Haynsworth's opinion in *Marchetti* by expressly likening the business

[66] David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 630 (2005).

[67] *Id.* at 630–31.

[68] *See* United States v. Marchetti, 466 F.2d 1309 (4th Cir. 1972).

[69] *Id.* at 1318.

[70] *Id*.

[71] *Id*.

[72] Halkin v. Helms, 598 F.2d 1, 11 (D.C. Cir. 1978).

of foreign intelligence gathering in the age of computer technology as akin to the construction of a mosaic, thereby associating this theory with the metaphor of a mosaic for the first time.[73]

[26] The mosaic theory "first and last reached"[74] the U.S. Supreme Court in *C.I.A. v. Sims* (1985), a suit which sought for the C.I.A. to disclose individuals and institutions conducting research on a C.I.A. funded project.[75] The Supreme Court has been considered to "endorse" the mosaic theory and "consolidate" *Helms* and *Marchetti* as leading cases[76] when it held that the C.I.A. Director had the authority to withhold "superficially innocuous information" on the grounds it may enable an observer to discover the identity of an intelligence source.[77]

[27] Following *Marchetti*, *Helms and Sims,* Professor Jace Gatewood points out that the mosaic theory gained prominence after the 9/11 terrorist attack on the World Trade Center and that today the mosaic theory has gained an ever-expanding role in national security law.[78] Moreover, Pozen comments that, in the intervening years since the theory's existence, the D.C. District Circuit in *Muniz v. Meese*[79] was the only court on record to reject a government agency's mosaic defence as it was too remote and pretextual to be taken seriously.[80] In the context

[73] *Id*. at 8–9.

[74] Pozen, *supra* note 67, at 643.

[75] CIA v. Sims, 471 U.S. 159, 159–60 (1985).

[76] Pozen, *supra* note 68, at 643.

[77] *Sims*, 471 U.S. at 178.

[78] Jace C. Gatewood, *District of Columbia Jones and the Mosaic Theory—in Search of a Public Right of Privacy: The Equilibrium Effect of the Mosaic Theory*, 92 NEB. L. REV. 504, 524 (2014).

[79] Muniz v. Meese, 115 F.R.D. 63 (D.D.C. 1987).

[80] Pozen, *supra* note 68, at 637.

of the Fourth Amendment jurisprudence, the mosaic theory has been suggested as a "new"[81] and "novel theory."[82]

B. Emergence of the Mosaic Theory & the Fourth Amendment

[28] The mosaic theory first emerged within Fourth Amendment jurisprudence in a decision of the Court of Appeals for the District of Columbia, *U.S. v. Maynard* (2010).[83] The theory resulted from a need to address individual privacy concerns associated with technological advances in surveillance. The D.C. Circuit Court, after holding that none of the appellants' five joint arguments warranted reversal, focused on a separate appeal made by an appellant regarding whether the use of prolonged GPS monitoring, absent a warrant, amounted to a search and if so whether this was reasonable.[84]

[29] Ultimately, in a 3-0 decision, the D.C. Circuit Court held that the use of GPS monitoring, absent a warrant, constituted an unreasonable search which violated the appellants' Fourth Amendment right to a "reasonable expectation of privacy" guaranteed by *Katz*.[85] In reaching this decision, the court distinguished *Maynard* from *Knotts*, arguing that the GPS monitoring, rather than tracking the appellants' movements from only one place to another, instead tracked their movements 24

[81] Orin Kerr, *D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, VOLOKH CONSPIRACY (Aug. 6, 2010, at 2:46 PM), https://volokh.com/2010/08/06/d-c-circuit-introduces-mosaic-theory-of-fourth-amendment-holds-gps-monitoring-a-fourth-amendment-search/ [https://perma.cc/TLU2-YH25].

[82] Madelaine Virginia Ford, *Mosaic Theory and the Fourth Amendment: How Jones Can Save Privacy in the Face of Evolving Technology*, 19 AM. U. J. GENDER SOC. POL'Y & L. 1351, 1365 (2011).

[83] United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd in part sub nom.*, United States v. Jones, 565 U.S. 400 (2012).

[84] *Id*. at 549–55.

[85] *Id*. at 555–58

hours a day for 28 days,[86] leading to the discovery of the totality of the appellants' patterns of movements. Circuit Judge Ginsburg reasoned that the appellants' totality of movements, unlike *Knotts*, was not exposed actually or constructively to the public, as the likelihood of a person witnessing the whole of a person's movements over the course of a month is nil.[87] Circuit Judge Ginsburg introduced the mosaic theory when dismissing the government's arguments that the appellant constructively exposed their movements; similar to a rap sheet in *Freedom of Press,*[88] the whole reveals more than individual movements.[89] Moreover, referencing *Sims* and *Marchetti*, prolonged surveillance will expose types of information not revealed by short-term surveillance.[90]

[30] When reviewing the decision of *Maynard* in *U.S. v. Jones* (2012), the U.S. Supreme Court affirmed that the government's installation of a GPS device and subsequent monitoring, absent a warrant, was a search within the meaning of the Fourth Amendment.[91] However, Justice Scalia's majority opinion stated that Jones' Fourth Amendment rights did not fall within the *Katz* formulation.[92] Instead the court grounded its reasoning in line with the court's earlier Fourth Amendment case law such as *Olmstead* which centred on a trespass-centric approach.[93] Justice Scalia also pointed out that the insistence on *Katz* in the concurrence led the court into "vexing problems," where the *Katz* test is inapplicable and that the differentiation between short and long term surveillance in the concurrence would introduce "yet another

[86] *Id*.

[87] *Id*. at 558.

[88] U.S. Dep't of Just. v. Reps. Comm. for Freedom of the Press, 489 U.S. 749 (1989).

[89] *Maynard*, 615 F.3d at 562.

[90] *Id*. at 562.

[91] United States v. Jones, 565 U.S. 400, 404 (2012).

[92] *Id*. at 406.

[93] *Id*. at 405.

novelty" into jurisprudence.[94] Therefore, the majority opinion of *Jones* suggests cogency to an argument that the Supreme Court is reluctant to find in favour of a mosaic approach in relation to 'new' technology. However, support may be interpreted for the mosaic theory in the concurring opinions of *Jones.*

[31] Justice Sotomayor's concurrence reasons that the majority opinion reflects a "constitutional minimum," as physical trespass is not required in the technological age of surveillance to infringe a person's subjective expectation of privacy.[95] Specifically, Justice Sotomayor's opinion has been considered to voice support for the mosaic theory when stating that GPS monitoring generates a comprehensive record of a person's public movements, and that these attributes of GPS should be taken into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements.[96] Justice Sotomayor stated that they "would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain….political and religious beliefs, sexual habits and so on."[97]

[32] Justice Alito's concurring opinion, joined by Justice Kagan, Justice Breyer, and Justice Ginsburg, also focuses on its rejection of the majority opinion's trespass-centric approach.[98] Justice Alito's comments have been considered to echo the mosaic theory when voicing concern regarding information revealed during long-term surveillance and reasoning that society's expectation is that police will not monitor and catalogue every single movement for a very long period of time.[99]

---

[94] *Id*. at 412.

[95] *Id*. at 414 (Sotomayor, J., concurring).

[96] *Jones*, 565 U.S. at 416–17 (Sotomayor, J., concurring); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012).

[97] *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

[98] *Id*. at 418–31 (Alito, J., concurring).

[99] *Id.* at 430–31 (Alito, J., concurring); Kerr, *supra* note 97, at 313, 327.

[33] The U.S. Supreme Court's docket has been known to include a range of high-profile cases which attract attention and debate from law professors to a general audience of law students and lawyers. *Jones* is such a case.[100] Writing for the Michigan Law Review, Professor Orin Kerr argues that in light of *Jones'* concurrences, the potential adoption of a mosaic theory represents a "Pandora's Box" which the courts should leave closed, and that the theory raises many novel and difficult questions.[101] For instance, what clear and consistent standard would govern the mosaic theory? How should conduct be grouped? How should the court analyse the reasonableness of mosaic searches? What remedies should apply to unconstitutional mosaic searches?[102] Moreover, Kerr comments that the mosaic theory will be difficult to administer effectively due to its departure from existing doctrine and that technology is likely to be outdated by the time that courts have resolved how to address constitutional questions. Furthermore, Kerr opines that the theory may discourage statutory solutions by Congress due to the courts occupying the field.[103] This argument is supported by Madelaine Ford, who suggests that whilst the mosaic theory may be flexible and may adapt to new technology, there is no clear line as to what collectively would amount to a search.[104] Therefore, these arguments suggest that the mosaic theory is not a sensible response to the privacy concerns raised by new technology.

[34] On the other hand, Professor Jace Gatewood, dismissing Kerr's criticisms, comments that the mosaic theory may be a viable solution for protection in the wake of advanced technology by restoring practical limitations as well as balancing society's interest in privacy and the government's interests in investigation.[105]

---

[100] Benjamin J. Priester, *Five Answers and Three Questions after United States v. Jones (2012), the Fourth Amendment "GPS Case"*, 65 OKLA. L. REV. 491, (2013).

[101] Kerr, *supra* note 97, at 329–30, 353.

[102] *Id.* at 329–30.

[103] *Id.* at 346–50.

[104] Ford, *supra* note 83 at 1365–72.

[105] Gatewood, *supra* note 79, at 535–36.

[35] Regardless of whether the literature demonstrates that in the aftermath of *Jones* that the mosaic theory should be adopted or declined, the majority agree that the concurring opinions in *Jones* raise a surprising possibility that a five-justice majority of the Supreme Court are ready to endorse the mosaic theory, thereby inviting lower courts to consider the theories viability.[106]

C. The Mosaic Theory Post-Jones

[36] Fourth Amendment Professor Orin Kerr summarised the aftermath of *Jones* when stating "if anything is clear from the Supreme Court's decision…..in *Jones*, it's that not very much is clear."[107] Jason Medinger commented that in the 365 days since the *Jones* opinion was issued, it had been cited by lower federal and state courts 193 times.[108] Post-*Jones*, subsequent cases indicate that the courts are divided in their application of the mosaic theory to emerging technology and that the courts are likely to remain outpaced by new technology.

[37] In *U.S. v. Graham* (2016), the Fourth Circuit rejected the mosaic theory, holding that the government did not violate the Fourth Amendment by obtaining historical cell-site location information (CSLI) from a cell phone provider absent a warrant.[109] The Court dismissed the defendant's contention based on *Kyllo* and *Jones,* holding that where the government employs technical devices to track

[106] Kerr, *supra* note 9, at 313; RICHARD M. THOMPSON, CONG. RSCH. SERV., R42511, UNITED STATES V JONES: GPS MONITORING, PROPERTY AND PRIVACY 6 (2012).

[107] Orin Kerr, *Why United States v. Jones is Subject to So Many Different Interpretations*, VOLOKH CONSPIRACY (Jan. 30, 2012, at 4:59 PM), https://volokh.com/2012/01/30/why-united-states-v-jones-is-subject-to-so-many-different-interpretations/ [https://perma.cc/2NNL-43BN].

[108] Jason D. Medinger, *Post-Jones: How District Courts are Answering the Myriad Questions Raised by the Supreme Court's Decision in United States v. Jones*, 42 U. BALT. L. REV. 395, 420 (2013).

[109] United States v. Graham, 824 F.3d 421, 424 (4th Cir. 2016).

individuals, it will always invade an individual's right to privacy.[110] Moreover, the Fourth Circuit recognised that whilst technology enables companies to collect vast amounts of customer information, the defendant's argument regarding the amount of information obtained rests on a misunderstanding of the concurrences in *Jones.*[111] Circuit Judge Motz states that *Jones* concerned the government surveillance of an individual, not an individual's voluntary disclosure of information to a third party.[112] The Court reasoned that the third-party doctrine applies as the defendant does not have a reasonable expectation of privacy in the CSLI when information was voluntarily turned over to a third party, the cell phone provider.[113]

[38] The Court in *Graham* also argued that the application of the third-party doctrine does not render privacy an unavoidable casualty of technological progress, as Congress remains free to require greater privacy protection as it is better positioned to respond to changes in technology.[114]

[39] However, *Carpenter v. U.S.*[115] (2018) which has been hailed as the "most important privacy case in a generation,"[116] does appear to endorse the mosaic theory.[117] In the 5-4 decision, the Supreme Court held that, absent a warrant and despite data being held by a third party, accessing CSLI from a phone carrier to reconstruct a record of the

[110] *Id.* at 426.

[111] *Id.* at 434–35.

[112] *Id.* at 435.

[113] *Id.* at 427.

[114] Graham, 824 F.3d at 436.

[115] Carpenter v. United States, 585 U.S. 296 (2018).

[116] Steven Vladeck, *The Supreme Court Phone Location Case Will Decide the Future of Privacy*, VICE (June 16, 2017, 2:00pm), https://www.vice.com/en/article/59zq5x/scotus-cell-location-privacy-op-ed [https://perma.cc/NF4B-YJ2Y].

[117] Paul Ohm, *The Many Revolutions of Carpenter,* 32 HARV. J.L. & TECH. 357, 373 (2019).

suspect's physical location in public spanning at least seven days violated the individual's Fourth Amendment rights and constituted a 'search.'[118] Chief Justice Roberts' majority opinion relied upon *Jones'* concurring opinions when ruling access to historical CSLI violates the individual's reasonable expectation of privacy due to cell-site data's pervasive and non-voluntary nature.[119] The reasoning drew comparison with *Jones,* stating that "much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopaedic, and effortlessly compiled."[120]

[40] Taylor Wilson, writing for the Texas Law Review Online, noted that *Carpenter* introduces a two-step mosaic approach, which asks whether 1) the data when aggregated has the potential to violate a reasonable expectation of privacy by revealing the "privacies of life," then 2) whether the information obtained does so.[121] Moreover, Elle Wang, writing in the Berkley Technology Law Journal, comments that *Carpenter* indicates the Court is moving further away from an historical interpretation of the Fourth Amendment to be more adaptive for the modern era.[122]

[41] On the other hand, Professor Orin Kerr, who filed an amicus brief on behalf of the U.S. in *Carpenter*, suggests that *Carpenter* is only a result of the 'equilibrium adjustment theory' which posits that when new technology threatens to tip the balance of power in favour of the government and away from the citizen, the courts expand legal protections in favour of the latter to restore the prior equilibrium.[123] The

[118] *Carpenter*, 585 U.S. at 311.

[119] *Id.* at 314–315.

[120] *Id.* at 309.

[121] Taylor H. Wilson, *The Mosaic Theory's Two Steps: Surveying Carpenter in the Lower Courts*, 99 TEX. L. REV. ONLINE 155, 163 (2021).

[122] Elle Xuemeng Wang, *Erecting A Privacy Wall Against Technological Advancements: The Fourth Amendment in the Post-Carpenter Era,* 34 BERKELEY TECH. L.J. 1205, 1238 (2019).

[123] Orin Kerr, *Understanding the Supreme Court's Carpenter Decision*, LAWFARE (June 22, 2018, at 1:18 PM), https://www.lawfaremedia.org/article/understanding-

CRS points out that *Carpenter* should prompt the Justices to call for congressional action as the legislative branch is in the best position to balance privacy concerns.[124]

D. The Mosaic Theory Post-Carpenter

[42] Post-*Carpenter,* only 30 cases have used the word "mosaic." Robert Fairbanks, writing in the Berkley Journal of Criminal Law, comments that, whilst the Supreme Court has potentially embraced the mosaic theory for a variety of technologies, this has left lower courts in a "mess" as they cannot agree when to apply the mosaic theory.[125] This is evidenced by cases concerning GPS monitoring and pole-camera surveillance which suggest that lower courts are continuing to be divided as to whether to apply the mosaic theory to new technology.

i. GPS Monitoring

[43] In *U.S. v. Howard* (2019), the District Court for the Southern District of Alabama explicitly declined to apply the mosaic theory when holding that GPS monitoring of a defendant's borrowed truck was not a search.[126] District Judge Watkins began by explaining the general confusion present within Fourth Amendment jurisprudence in relation to searches, and that the mosaic theory has puzzled both federal and state courts. Judge Watkins then made it clear that the court's conclusion "did not rest on the mosaic theory," but rather on fundamental facts and applicable law based on a trespass-centric approach.[127] For instance, that

---

supreme-courts-carpenter-decision#:~:text=The%20court%20ruled%20that%20access,that%20accessing%20those%20records%20requires [https://perma.cc/MD88-S94M].

[124] BEN HARRINGTON, CONG. RSCH. SERV., LSB10157, UPDATE: SUPREME COURT TAKES FOURTH AMENDMENT CASE ABOUT CELL PHONE LOCATION DATA 3 (2018).

[125] Robert Fairbanks, *Masterpiece or Mess: The Mosaic Theory of the Fourth Amendment Post-Carpenter*, 26 BERKELEY J. CRIM. L. 71, 72–73, 75 (2021).

[126] United States v. Howard, 426 F. Supp. 3d 1247, 1256 (M.D. Ala. 2019), *aff'd*, 858 F. App'x 331 (11th Cir. 2021).

[127] *Id.* at 1256.

there was no trespass due to the borrowed truck's owner consenting to the installation of the GPS.[128] Notably, Fairbanks does suggest the court confusingly allowed for the potential application of the mosaic theory when commenting that the surveillance was not for an extended period of time, but rather a 24 hour period.[129]

[44] However, in *U.S. v. Diggs* (2019), the District Court for the Northern District of Illinois appears to support the mosaic approach, holding that the government conducted a search when acquiring a month's worth of a vehicle's GPS data.[130] Specifically, District Judge Feinerman argued that the GPS data fit squarely within the scope of the reasonable expectation of privacy as identified in *Jones'* concurrences, which were reaffirmed by *Carpenter* as the GPS data provides a precise and comprehensive record of Diggs' public movements over the course of a month.[131]

ii. Pole-Camera Surveillance

[45] In *U.S. v. Tuggle* (2021) the Seventh Circuit appears to reject the mosaic approach when holding that the government's warrantless use of pole-camera surveillance for eighteen months to observe the defendant's home did not amount to a search under the Fourth Amendment.[132] Circuit Judge Flaum reasoned that the prolonged and uninterrupted use of pole-camera surveillance was not a search under the mosaic theory; whilst the stationary cameras placed around the defendant's home captured an important sliver of their life, this did not paint an exhaustive picture as in *Jones* or *Carpenter*.[133] The court stated that whilst some judges have relied on mosaic-like reasoning, the Supreme Court has not

[128] *Id.*

[129] Fairbanks, *supra* note 126, at 99.

[130] United States v. Diggs, 385 F. Supp. 3d 648, 649 (N.D. Ill. 2019).

[131] *Id.* at 652.

[132] United States v. Tuggle, 4 F.4th 505, 509 (7th Cir. 2021).

[133] *Id.* at 524.

bound lower courts to apply the mosaic theory.[134] Thus, the mosaic theory has not received the court's full and affirmative adoption leading to a "splintered" approach in lower courts.[135] Moreover, line-drawing issues of the mosaic theory were raised and emphasis was provided that the rise in new technology may be an apt area for Congress to legislate.[136]

[46] However, the state court decision *People v. Tafoya* (2021) appears to support the mosaic approach, holding that surveillance through a pole-camera did indeed constitute a search.[137] The Supreme Court of Colorado reasoned that the defendant demonstrated a subjective expectation of privacy in the area surveilled as this was curtilage and could not be seen by a person standing on the street due to a 6ft privacy fence.[138] Moreover, the privacy fence indicates how the defendant sought to preserve the area as private.[139] Chief Justice Boatright reasoned with reference to *Jones* and *Carpenter* that the duration, continuity, and nature of surveillance matter when considering all the facts and circumstances in a particular case.[140] Therefore, the fact that the pole-camera recorded the curtilage continuously for three months and the police indefinitely stored the footage was problematic. Similar to *Jones,* this creates a precise and comprehensive record of activity which is at least as intrusive as tracking a person's location as a "dot on a map."[141]

[134] *Id.* at 517.

[135] *Id.* at 520.

[136] *Id.* at 526–28.

[137] People v. Tafoya, 494 P.3d 613, 615 (Colo. 2021).

[138] *Id.* at 622.

[139] *Id.* at 623.

[140] *Id.* at 620.

[141] *Id.* at 623.

E. The Mosaic Theory & Blockchain Technology

[47] At the time of writing, a decision of the U.S. Courts of Appeals for the Fifth Circuit, *United States v. Gratkowski* (2020), is the only case that involves blockchain technology and individual privacy rights.[142]

[48] *Gratkowski* held that the defendant lacked a privacy interest in their personal records located within the blockchain and the virtual currency exchange they had voluntarily selected.[143] The defendant was convicted of purchasing child pornography via an online website using the cryptocurrency 'Bitcoin', which operates using a public network, and argued that their Fourth Amendment right to a reasonable expectation of privacy had been violated by the government's tracing using blockchain records.[144] Circuit Judge Haynes stated that the blockchain records containing personal information were akin to those involving bank records and telephone logs, which are not subject to Fourth Amendment protection as a result of the third-party doctrine.[145] This is because the material was not confidential and voluntarily provided to a third party, for instance, a financial institution.[146] Moreover, *Carpenter* was inapplicable because virtual currency is not a pervasive part of daily life and requires affirmative action by the bitcoin address holder.[147]

[49] Therefore, *Gratkowski* provides cogency to the argument that the mosaic theory is likely to be unfavourable with the courts in relation to blockchain technology, as the courts are continuing to favour either a trespass-centric approach or one which sides with the third-party doctrine.

---

[142] United States v. Gratkowski, 964 F.3d 307, 310 n.3 (5th Cir. 2020).

[143] *Id.* at 312.

[144] *Id.* at 309–10.

[145] *Id.* at 310–12.

[146] *Id.* at 311–12.

[147] *Gratkowski*, 964 F.3d at 311–13.

[50] *Gratkowski* has generated discussion amongst scholarship by legal students as to its effect. It is perhaps not surprising that *Gratkowski* has received considerable attention, particularly from scholars, as blockchain regulation is a developing area of law with the implications yet to be fully understood. Yana Kogan, a J.D. student at Columbia Law School, comments that the court applied flawed reasoning as a result of inconsistent distinctions regarding the third-party doctrine and a misunderstanding of blockchain technology.[148] Kogan also suggests that *Gratkowsk*i should be applied narrowly, and a modified reasonable expectation of privacy standard should be implemented, supplementing the existing standard with an additional inquiry into information initially disclosed by individuals.[149]

[51] Taylor Wilson, a J.D. Student from the University of Texas, comments that because of *Carpenter's* "sweeping" language, courts have faced Fourth Amendment challenges to the acquisition of data such as cryptocurrency transactions, and *Gratkowski* indicates the court's emphasis that cryptocurrency ledgers convey limited information, require affirmative action, and are publicly available.[150] Furthermore, although the court in *Gratkowski* did not explicitly address the mosaic theory, there is an acceptance towards *Carpenter's* shift in focus to the nature of information conveyed.[151]

F. Interim Conclusions

[52] Section II has pointed out through a discussion of the mosaic theory's evolution that the Supreme Court is reluctant to provide its full endorsement for the mosaic theory to be applied to cases involving individual privacy rights and new technology. This has led to the division of the lower courts in their application of the mosaic approach.

[148] Yana Kogan, *The Privacy Limits of Transacting in Bitcoin*, 2022 COLUM. BUS. L. REV. 506, 511 (2022).

[149] *Id.* at 542–45.

[150] Wilson, *supra* note 122, at 178.

[151] *Id*.

For instance, following *Jones*[152] and *Carpenter*[153] in GPS monitoring and pole-camera surveillance cases.[154] The literature underscores that the adoption of the mosaic theory by the courts is not a sensible response to privacy concerns of new technology due to practicality issues.[155] For instance, the mosaic theory raises novel questions, technology becomes outdated by the time the courts respond to constitutional questions, and that a ruling would interfere with Congress's legislative role.[156]

[53] Furthermore, the recent case of *Gratkowski* suggests that courts are likely to be unfavourable to arguments rooted in the mosaic theory, particularly in light of the intrusions of blockchain technology not being considered "pervasive" enough to individual privacy rights.[157] It is plausible that as blockchain becomes more ubiquitous, the principles established in *Carpenter*, and thus the applicability of the mosaic theory, could evolve accordingly. However, it is difficult to predict when or if this would occur.

IV. HOW HAS THE FEDERAL LEGISLATURE RESPONDED TO THE PRIVACY CONCERNS OF BLOCKCHAIN TECHNOLOGY IN THE HEALTHCARE SECTOR?

[54] The article will now shift to consider how federal legislation in the United States operates to protect individual privacy rights against blockchain technology and how adequate these protections may be. There has been no federal legislation or recent activity that directly regulates blockchain technology and safeguards individual privacy

[152] *Jones*, 565 U.S. at 400.

[153] *Carpenter*, 585 U.S. at 296.

[154] *See, e.g.,* United States v. Howard, 426 F. Supp. 3d 1247, 1255–56 (M.D. Ala. 2019), *aff'd*, 858 F. App'x 331 (11th Cir. 2021); United States v. Diggs, 385 F. Supp. 3d 648, 649–51 (N.D. Ill. 2019); United States v. Tuggle, 4 F.4th 505, 509 (7th Cir. 2021); People v. Tafoya, 494 P.3d 613, 617 (Colo. 2021).

[155] *See generally* Kerr, *supra* note 97.

[156] *See* Kerr, *supra* note 97; *see also* Ford, *supra* note 83, at 1365–72.

[157] United States v. Gratkowski, 964 F.3d 307, 311–13 (5th Cir. 2020).

rights. Furthermore, scholarship on the federal legislature's response to the privacy concerns raised by blockchain technology is limited. Therefore, Section III aims to explore whether Congress has taken steps to regulate blockchain and protect privacy rights.

[55] In the absence of federal legislation specifically addressing blockchain, this section will examine how existing laws, such as the Health Insurance Portability and Accountability Act (HIPAA) [158] of 1996 and the Health Information Technology for Economic and Clinical Health Act (HITECH) [159] of 2009, may apply to blockchain use in healthcare. This article focuses on the healthcare sector to assert that the privacy concerns of blockchain technology extend beyond the financial sector, particularly in the context of managing sensitive medical data. The section will also explore the ongoing debate in the literature regarding whether these laws adequately address the privacy challenges posed by blockchain technology.

A. Federal Blockchain Privacy Legislation

[56] Victor Wang, professor at Cardozo Law School, comments that currently there are no regulations to govern blockchain technology in the healthcare industry, as not only is blockchain still relatively new, but most existing legal precedents focus on criminal behaviour in relation to blockchain technology's use for cryptocurrency.[160] The Bills introduced by the 118th Congress support Wang's view, for instance, the Blockchain Regulatory Certainty Act Bill, which focuses on financial reporting requirements.[161] Therefore, as no specific privacy legislation exists at a federal level to regulate blockchain technology, this has meant that the state of sector-specific legislation is unclear.

[158] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[159] Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111-5, Div A Title XIII, Div B Title IV, 123 Stat. 226 (2009).

[160] Victor Wang, *Blockchain, the Superhero that the Healthcare Industry Needs*, 40 CARDOZO ARTS & ENT. L.J. 793, 812 (2023).

[161] Blockchain Regulatory Certainty Act, H.R. 1747, 118th Cong. (2023).

[57] Forbes magazine comments that within the healthcare sector, there is an inability to securely share and access sensitive patient data.[162] This aligns with the views of RJ Kraweic, principal in consulting at Deloitte, and his co-authors, who comment in a Deloitte White Paper that the state of healthcare records is disjointed due to a lack of standards allowing for the safe transfer of information.[163] Both Forbes and the Deloitte White Paper suggest that blockchain technology holds the potential to transform and revolutionise the healthcare sector through its unique characteristics and customisable openness.[164] The CRS points out that there have been a variety of proposals for the use of blockchain technology in the healthcare sector, which involve the management of patient information maintained in electronic health records (EHRs), for instance, authenticating patients and healthcare providers on a blockchain to enable the sharing of EHRs.[165] The other uses of blockchain in healthcare include its use for pharmaceutical supply chains and smart contracts.[166] However, despite the potential to revolutionise healthcare, privacy concerns associated with the use of blockchain technology still exist, as raised in Section I.

[58] The CRS states that as blockchain technology may be used for data management and the handling of sensitive medical information, this

[162] José Morey, *The Future of Blockchain in Healthcare*, FORBES (Oct. 25, 2021, at 10:30 AM), https://www.forbes.com/sites/forbestechcouncil/2021/10/25/the-future-of-blockchain-in-healthcare [https://perma.cc/PZ2F-97ET].

[163] *See* RJ Krawiec et al., *Blockchain: Opportunities for Health Care*, DELOITTE (Aug. 2016), https://www2.deloitte.com/us/en/pages/public-sector/articles/blockchain-opportunities-for-health-care.html [https://perma.cc/VFQ6-FDDV].

[164] *Id.* at 3; Morey, *supra* note 164.

[165] JAIKARAN, *supra* note 1, at 6.

[166] *Blockchain For Healthcare*, U.S. DEP'T HEALTH & HUMAN SERV., 16-21 (Jul.10, 2021), https://www.hhs.gov/sites/default/files/blockchain-for-healthcare-tlpwhite.pdf [https://perma.cc/23WQ-XKPE]; U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-104625, BLOCKCHAIN: EMERGING TECHNOLOGY OFFERS BENEFITS FOR SOME APPLICATIONS BUT FACES CHALLENGES 12 (2022).

"implicates"[167] federal privacy legislation such as HIPAA[168] and HITECH.[169]

i. HIPAA

[59] HIPAA is a comprehensive federal law that authorises the U.S. Department of Health and Human Services (HHS) to create national standards that protect sensitive patient health information from being disclosed without the patient's consent or knowledge.[170] The HHS achieved the implementation of HIPAA most notably through issuing the HIPAA Privacy and Security Rules.[171] Within the HHS, the Office for Civil Rights has responsibility for implementing and enforcing the Privacy and Security Rules.[172]

[60] The HIPAA Privacy Rule establishes a set of national standards for the protection of certain health information as well as the protection of individual privacy rights.[173] The major goal of the HIPAA Privacy

[167] JAIKARAN, *supra* note 1, at 6; *Beyond Bitcoin: Emerging Applications for Blockchain Technology*: *Hearing Before the Subcomm. on Oversight & Subcomm. on Rsch. and Tech. of the H. Comm. on Sci., Space, and Tech.*, 115th Cong. 5 (2018) (statement of Chris Jaikaran, Cybersecurity Policy Analyst).

[168] *The Health and Insurance Portability and Accountability Act of 1996 (HIPPA)*, *supra* note 160.

[169] *The Health Information and Technology for Economic and Clinical Health Act of 2009*, *supra* note 161.

[170] *The Health and Insurance Portability and Accountability Act of 1996 (HIPPA)*, CDC (Sept. 10, 2024), https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient%27s%20consent%20or%20knowledge [https://perma.cc/RQZ2-AWPP].

[171] 45 C.F.R. §§164 (2000); *The Health and Insurance Portability and Accountability Act of 1996 (HIPPA)*, *supra* note 160.

[172] STEPHEN REDHEAD, CONG. RSCH. SERV., R43991, HIPAA PRIVACY, SECURITY, ENFORCEMENT, AND BREACH NOTIFICATION STANDARDS 1-2 (2015).

[173] *The HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERV. (Sept. 27, 2024), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html [https://perma.cc/ZW5R-9KJS].

Rule is to ensure individuals' health information is properly protected whilst allowing the flow of health information needed to provide and promote high-quality healthcare and to protect the public's health and well-being.[174]

[61] The HIPAA Privacy Rule applies to "covered entities" and "business associates" who transmit health information in electronic form in connection with transactions protected under HIPAA.[175] A "covered entity" includes every healthcare provider that electronically transfers health information in connection with certain transactions, health plans, as well as healthcare clearinghouses.[176] Moreover, a "business associate" is a person or organisation other than a member of the "covered entities" workforce who performs certain functions, activities or services on behalf of or to a "covered entity" that involves the use or disclosure of individually identifiable health information.[177] A business associate agreement is required where a "covered entity" uses a contractor or other non-workforce member to perform "business associate" activities.[178] This agreement imposes written safeguards on individually identifiable health information disclosed to "business associates."[179]

[62] The Privacy Rule seeks to protect any "individually identifiable information," also known as protected health information (PHI), that is transmitted or maintained in any form or medium by "covered entities" or its "business associates."[180] PHI includes information such as demographic data that relates to the individual's past, present, or future health condition, the provision of healthcare, as well as information which identifies the individual or for which there is a reasonable basis

[174] *The Health and Insurance Portability and Accountability Act of 1996 (HIPPA)*, *supra* note 160.

[175] 45 C.F.R. §§ 160.102, 106.103 (2013).

[176] 45 C.F.R. §§ 160.103, 164.500 (2013).

[177] 45 C.F.R. §160.103 (2013).

[178] 45 C.F.R. §§ 164.502(e),164.504(e) (2024).

[179] *Id*.

[180] 45 C.F.R. § 160.103 (2024).

to believe it can be used to identify the individual.[181] Common identifiers include names, addresses, and social security numbers.[182] There are no restrictions on the use or disclosure of de-identified health information.[183] This is health information that neither identifies nor provides a reasonable basis for identification.[184] The Privacy Rule includes the "safe harbour" method to achieve "de-identification", requiring the removal of 18 specified types of identifiers.[185]

[63] The Privacy Rule standards, which protect an individual's PHI, include those that limit the circumstances for its use or disclosure.[186] For instance, "covered entities" must not disclose or use PHI, except where required by the Privacy Rule, such as in HHS investigations, or where the individual who is the subject of the information has given authorisation in writing.[187] The Privacy Rule also highlights instances in which permitted uses and disclosures of PHI may be made without an individual's authorisation, such as for the treatment activities of any healthcare provider.[188] A "covered entity" must also limit its uses and disclosures of PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure.[189]

[64] The Privacy Rules standards, which protect individual privacy rights in respect to their health information, include the right to inspect

[181] *Id*.

[182] *Summary of the HIPAA Privacy Rule*, U.S. DEP'T HEALTH & HUMAN SERV. (Mar. 14, 2025, at 5:22 PM), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html [https://perma.cc/SF9T-NZ6H].

[183] *Id*.

[184] 45 C.F.R. §§ 164.502(d)(2), 164.514(a)–(b) (2013).

[185] 45 C.F.R. § 164.514(b) (2025); *see also* REDHEAD, *supra* note 174, at 5.

[186] 45 C.F.R. § 164.502(a) (2024); *see also Summary of the HIPPA Privacy Rule*, *supra* note 184.

[187] *See Summary of the HIPPA Privacy Rule*, *supra* note 184.

[188] 45 C.F.R. § 164.502(a)(1)–(5) (2025).

[189] 45 C.F.R. §§ 164.502(b) (2024), 164.514(d) (2013).

and retain copies of medical information,[190] the right to amend or correct inaccurate information,[191] and the right to an accounting of certain types of information disclosure.[192] Each "covered entity" with certain exceptions must also provide notice of its privacy practices.[193]

[65] The major goal of the HIPAA Security Rule is to protect the privacy of individuals' health information whilst allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care.[194] The HIPAA Security Rule operationalises the protections afforded in the Privacy Rule, addressing the administrative, physical, and technical safeguards that organisations called "covered entities" must put in place to secure individuals' "electronic protected health information" (e-PHI).[195] Those who are subject to the Security Rule remain the same as the Privacy Rule.[196]

[66] Specifically, to comply with the HIPAA Security Rule, "covered entities" must 1) ensure the confidentiality, integrity, and availability of all e-PHI, 2) detect and safeguard against anticipated threats to the security of the information, 3) protect against anticipated impermissible

[190] 45 C.F.R. § 164.524 (2025).

[191] 45 C.F.R. § 164.526 (2025).

[192] 45 C.F.R. § 164.528 (2002).

[193] 45 C.F.R.§ 164.520 (2024).

[194] *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERV. (Mar. 14, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html [https://perma.cc/VZ9D-Y3J8].

[195] 45 C.F.R. §§ 164.308, 164.310, 164.312 (2013); *see also The Security Rule,* U.S. DEP'T HEALTH & HUMAN SERV. (Oct. 20, 2022), https://www.hhs.gov/hipaa/for-professionals/security/index.html [https://perma.cc/V8C8-VLFH].

[196] *Summary of the HIPAA Security Rule,* U.S. DEP'T HEALTH & HUMAN SERV. (Dec. 30, 2024), https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html [https://perma.cc/96HJ-789S].

uses or disclosures that are not allowed by the rule, and 4) certify compliance by their workforce.[197]

ii. The HITECH Act

[67] The HITECH Act,[198] enacted as part of the American Recovery and Reinvestment Act of 2009,[199] was signed into law to promote the adoption and meaningful use of health information technology.[200] HITECH includes a series of provisions associated with electronic health information designed to expand and address the HIPAA Privacy and Security Rules.[201] Specifically, its provisions include those which strengthen the civil and criminal enforcement of HIPAA's rules,[202] incentives for the use of electronic health records,[203] and provisions that allow individuals a right to receive electronic copies of their PHI.[204] HITECH also expanded the responsibilities of "business associates" under the HIPAA Security Rule, making them directly liable and subject to penalties for non-compliance.[205]

---

[197] 45 C.F.R. § 164.306(a) (2025); *see also Health Insurance Portability and Accountability Act of 1996 (HIPPA)*, *supra* note 160.

[198] *The Health Information and Technology for Economic and Clinical Health Act of 2009*, *supra* note 161.

[199] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009).

[200] *HITECH Act Enforcement Interim Final Rule*, U.S. DEP'T OF HEALTH & HUMAN SERV. (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html [https://perma.cc/6KA6-KNR5].

[201] REDHEAD, *supra* note 174, at 15.

[202] *Id.* at 15–16.

[203] Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, § 3011, 123 Stat. 115, 246 (2009).

[204] Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, § 13405, 123 Stat. 115, 264 (2009).

[205] 45 C.F.R. §164.514(e) (2013).

iii. HIPAA Breach Notification Rule

[68] The HIPAA Breach Notification Rule,[206] established pursuant to HITECH, requires HIPAA "covered entities" and their "business associates" to notify all individuals affected by a breach of unsecured protected health information without unreasonable delay, but no later than 60 days.[207]

iv. Omnibus Rule

[69] The final Omnibus Rule amends and extends the privacy and security provisions of HIPAA whilst implementing several provisions from the HITECH Act.[208] Key provisions include alterations to the breach notification rule's definition of breach, deletion of the definition "compromises the privacy or security" of PHI, where data breaches occur, this must be notified within 60 days of discovery, and expands the right to an electronic copy of PHI to a right to a copy of the individual's designated record subset.[209]

[70] It should be noted that since the Omnibus Rule, a notice of proposed rulemaking has been issued in relation to HIPAA.[210] However, this relates to reproductive health rights, not blockchain technology.[211]

---

[206] 45 C.F.R. §§ 164.400-414 (2025).

[207] *Id. See also Breach Notification Rule*, U.S. DEP'T OF HEALTH & HUMAN SERV., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html [https://perma.cc/7HDW-RGPM]. REDHEAD, *supra* note 174, at 17.

[208] Press Release, U.S. Dep't of Health & Human Serv., New Rule Protects Patient Privacy, Secures Health Information (Jan. 17, 2013).

[209] *Id*. *See also* Rebecca L. Williams et al., *New Omnibus Rule Released: HIPAA Puts on More Weight,* DAVIS WRIGHT TREMAINE (Jan. 23, 2013), https://www.dwt.com/insights/2013/01/new-omnibus-rule-released-hipaa-puts-on-more-weigh [https://perma.cc/3BEG-32CT].

[210] *HIPAA Privacy Rule Notice of Proposed Rulemaking to Support Reproductive Health Care Privacy Fact Sheet*, U.S. DEP'T OF HEALTH & HUMAN SERV. (Apr. 25, 2023), https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/hipaa-reproductive-health-fact-sheet/index.html [https://perma.cc/J4CL-N8YD].

[211] *Id*.

B. HIPAA, HITECH & Blockchain

[71] There is an ongoing debate within the literature regarding whether HIPAA and HITECH are adequate to regulate blockchain technology and address associated privacy concerns, or if updates are necessary.[212] The following literature suggests that federal privacy legislation is inadequate to accommodate the development of blockchain technology, as the law is likely to be outpaced by new technology. Attorney Roy Wyman argues that HIPAA reflects an "antiquated view"[213] and that change is desperately needed, for instance, a broad privacy rule that includes HIPAA and governs all business entities.[214] This is required, as HIPAA's vague distinctions between 'covered entities' and 'business associates,' which have access to an individual's data, must be eliminated to reduce structural issues, allowing two companies holding the same information to be treated differently depending on contractual relations.[215] Wyman also suggests that HIPAA has been proven imperfect from its conception, not ageing well in the face of technological development.[216] Specifically, technology makes it likely that HIPAA's method for "de-identifying" information may still lead to the identification of individuals through other available

[212] *See* Roy Wyman, *Can HIPAA be Saved? The Continuing Relevance and Evolution of Healthcare Privacy and Security Standards*, NELSON MULLINS (Aug. 17, 2020), https://www.nelsonmullins.com/storage/GiffvCERcGZ36N9rzYYKQsy4aMHATVu76CBkaHgk.pdf [https://perma.cc/9SXP-RTD6]; Devon Connor-Green, *Blockchain in Healthcare Data*, 21 U.S.F. INTELL. PROP. & TECH. L.J. 93 (2017); Wang, *supra* note 162; Zachary L. Catanzaro & Robert Kain, *Patients as Peers: Blockchain Based EHR and Medical Information Commons Models For HITECH Act Compliance*, 44 NOVA L. REV. 289 (2020); Kathryn Bennett, *Healthtech: How Blockchain Can Simplify Healthcare Compliance*, 25 WASH. & LEE J. CIVIL RTS. & SOC. JUST. 287 (2018); Les Wilkinson et al., *Blockchain Meets Healthcare: Understanding the Business Model and Implementing Initiatives*, ACC DOCKET (Sept. 1, 2017), https://docket.acc.com/blockchain-meets-healthcare-understanding-business-model-and-implementing-initiatives [https://perma.cc/WX46-JL27].

[213] Wyman, *supra* note 214, at 19.

[214] *Id*. at 5.

[215] *Id*. at 8.

[216] *Id*. at 7.

information, besides the 18 identifiers.[217] Moreover, whilst HIPAA does not preclude blockchain technology, legislation should be sensitive to technology as changes in the law may limit its use.[218]

[72] Attorney Devon Connor-Green agrees with Wyman, pointing out that HIPAA's language must be updated and expanded.[219] Connor-Green reasons this is necessary as blockchain is evolving the ways it stores and collects data, meaning that it will soon fall outside of HIPAA's scope.[220] Victor Wang, professor at Cardozo Law School, also supports the need for an update in the current approach to regulating blockchain technology.[221] Wang points out that blockchain will have difficulty becoming HIPAA compliant as a result of blockchain's characteristics, such as immutability and decentralisation, meaning that conflict occurs with not only HIPAA's security rule but also its authority requirement.[222] Wang discusses a possible solution in that blockchain technology must develop further to become HIPAA compliant.[223] However, Wang concludes that because technology is advancing at a quicker rate than legal updates, legislators need to consider updating the entirety of HIPAA into a new piece of law to ensure privacy and security of PHI.[224]

[73] On the other hand, Professor Zachary Catanzaro and Attorney Robert Kain support the view that the federal legislation of the U.S. is adequate.[225] They argue that blockchain, by virtue of its technological components, complies with HITECH incentives reporting requirements

[217] *Id*. at 9.

[218] Wyman, *supra* note 214, at 11.

[219] Connor-Green, *supra* note 214, at 103–06.

[220] *Id*. at 103.

[221] Wang, *supra* note 162.

[222] *Id.* at 813–14.

[223] *Id.* at 816–20.

[224] *Id.* at 824.

[225] Catanzaro & Kain, *supra* note 214.

and HIPAA in most respects.[226] Moreover, they comment that blockchain compliance with HIPAA is possible through the implementation of technical policies and procedures to allow only authorised personnel access to electronic health records.[227] Katheryn Bennett agrees with the view that federal legislation is adequate, commenting that it offers a comprehensive system that not only complies with HITECH and HIPAA but also offers healthcare providers efficiency, ease, and relative cost neutralisation.[228]

[74] Alternatively, Professor Jason Epstein and co-authors take a nuanced approach. On one hand, they acknowledge that the structure of laws and regulations, such as the administrative simplification rules of HIPAA, did not envision blockchain technology.[229] On the other hand, they also state that blockchain requires the application of pre-existing legal constructs with an eye to new issues and that a well-designed blockchain structure may avoid many of the pitfalls found within federal privacy laws.[230] Furthermore, the adoption of transformative technology will take time, and whilst slow, the law does eventually respond.[231]

C. Interim Conclusions

[75] This section has revealed that significant gaps exist within the current legal framework of the U.S., as there is an absence of specific federal legislation dedicated to governing blockchain technology and protecting individual privacy rights. Therefore, section III focused on identifying federal legislation in the healthcare sector that may be

[226] *Id.* at 315.

[227] *Id.* at 325.

[228] Bennett, *supra* note 214, at 12.

[229] Les Wilkinson et al., *supra* note 214.

[230] *Id*.

[231] *Id*. at 64.

implicated by blockchain's management of sensitive information, HIPAA[232] and HITECH.[233]

[76] This section also examined the wider scholarly debate surrounding whether the aforementioned legislation is adequate to address the privacy concerns of blockchain technology. In particular, the literature identified that HIPAA and HITECH are inadequate to address the privacy concerns of blockchain, due to provisions being outdated in comparison to new technology and conflicting with blockchain's core characteristics.[234] It is proposed that federal legislation lacks updated provisions that are broad and sensitive to technology.[235] However, the feasibility of federal legislation containing the suggested updates remains to be seen, as technology will likely continue to outpace the law.

V. HOW HAS THE STATE OF CALIFORNIA'S LEGISLATURE RESPONDED TO THE PRIVACY CONCERNS OF BLOCKCHAIN TECHNOLOGY?

[77] As established in Sections I and III, the U.S. approach to data privacy regulation is 'patchwork' in a manner that has meant that sector-specific legislation is adopted at a federal level. The federal approach of the U.S. to data privacy regulation has led some states, including California and Colorado, to put in place additional privacy laws.[236] However, as Rebecca Harris's research indicates, there is no state legislation specifically regulating blockchain technology.[237] This view

[232] *The Health Insurance Portability and Accountability Act of 1996 (HIPPA)*, *supra* note 160.

[233] *The Health Information and Technology for Economic and Clinical Health Act of 2009*, *supra* note 161.

[234] Wyman, *supra* note 214, at 19; Connor-Green, *supra* note 214, at 103–06; Wang, *supra* note 162, at 813.

[235] Wyman, *supra* note 214, at 19.

[236] California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (effective Jan. 1, 2025); California Consumer Privacy Act of 2018, *amended by*, the California Privacy Rights Act of 2020, CAL. CIV. CODE § 1798.100 (effective Jan. 1, 2023).

[237] Harris, *supra* note 36, at 226.

is reinforced by the National Conference of State Legislatures' findings, which indicate that New Hampshire is the only state with pending privacy legislation that takes into consideration blockchain technology through its privacy rights Bill, which prohibits the use of currency (including digital currencies) that may be detrimental to an individual's privacy rights.[238]

[78] Attention shall now be directed to considering how state legislation in the United States operates to protect individual privacy rights, and how adequate these protections may be. The focus will be on California as it has the largest population in the United States[239] and has implemented the "most comprehensive"[240] state privacy laws to date, the California Consumer Privacy Act (CCPA)[241] and the California Privacy Rights Act (CPRA).[242] California does not have legislation to regulate privacy that is specific to blockchain technology.[243] This section will examine whether the CCPA and CPRA are adequate to address privacy concerns related to blockchain technology and will touch upon the broader debate about the adequacy of the fragmented federal and state approach to the protection of individual privacy rights.

[238] H.B. 225, 2023 Leg. (N.H. 2023); *Cryptocurrency 2023 Legislation*, NAT'L CONF. STATE LEG., https://www.ncsl.org/financial-services/cryptocurrency-2023-legislation [https://perma.cc/77QJ-3UP7].

[239] *U.S. Census Bureau Most Populous*, *supra* note 9.

[240] SHAH ET AL., *supra* note 11; Marissa Wong, *Revising U.S. Privacy Laws: New Laws Are Required to Fill in the Gaps of Current and Proposed Legislation to Account for New Technology and Future Emergencies*, 16 BROOK. J. CORP. FIN. & COM. L. 305, 309 (2021).

[241] California Consumer Privacy Act of 2018, CAL. CIV. CODE. § 1798.100 et seq. (eff. until Jan 1, 2023).

[242] California Consumer Privacy Act of 2018, *amended by*, the California Privacy Rights Act of 2020, CAL. CIV. CODE § 1798.100 (effective Jan. 1, 2023).

[243] *See, e.g.,* SHAH ET AL., *supra* note 11.

A. CCPA

[79] As the first state to enact a data breach notification law in 2003,[244] and the first to provide consumers with comprehensive privacy protections through the enactment of the CCPA,[245] the State of California is known to be a leader in the U.S. for protecting California residents' privacy rights. The CCPA is a landmark law that gives consumers more control over their personal information collected by businesses and secures new privacy rights for California consumers.[246]
[80] The CCPA regulates "for-profit businesses" that conduct business in California and collect consumers' personal data.[247] These businesses must meet one of the jurisdictional thresholds: 1) an annual gross revenue that exceeds $25 million, 2) the selling and sharing of the personal information of 100,000 or more consumers annually, or 3) derive 50% or more of its annual revenue from selling, sharing, or purchasing personal data.[248] Common exceptions to those included under the CCPA are "non-profit entities" and entities regulated by other sector-specific laws, such as healthcare, which is regulated by HIPAA.[249]

[81] According to state regulations, as of September 1, 2017, the CCPA defines a consumer as any resident of California.[250] Further

[244] Kamala D. Harris, CAL. OFF. ATT'Y GEN., *California Data Breach Report*, 1–2 (Oct. 2014), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf [https://perma.cc/L5N4-T5GX].

[245] California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (effective Jan. 1, 2025).

[246] *California Consumer Privacy Act (CCPA)*, CAL. OFF. ATT'Y GEN., (May 10, 2023), https://oag.ca.gov/privacy/ccpa [https://perma.cc/HWD7-QXPE].

[247] CAL. CIV. CODE §1798.140(d)(1) (West 2025).

[248] *Id*.

[249] CAL. CIV. CODE §§ 1798.140(d), 1798.145 (West 2025); *see also California Consumer Privacy Act (CCPA/CPRA) Quick Facts: Overview*, PRAC. LAW (Westlaw 2025).

[250] CAL. CIV. CODE § 1798.140(i) (West 2025).

definitions provided include personal information, which is broader than federal legislation and refers to information that identifies or may be reasonably capable of being linked with a particular consumer, such as geolocation data and Internet browsing history.[251] Sensitive Information is also defined, for instance, as a consumer's social security number.[252]

[82] Most notably, the CCPA secures new privacy rights for California consumers regarding their personal information.[253] These include: the right to know about personal information a business collects from them and how it is shared,[254] the right to delete personal information collected from them,[255] the right to opt-out of the sale or sharing of their personal information,[256] as well as the right to non-discrimination for exercising their CCPA rights.[257] The CCPA also requires businesses to act upon and respond to a consumer's request to exercise their personal information rights.[258] Moreover, the CCPA provides consumers with the potential mechanism to sell their personal data as businesses may offer financial incentives, including payment for the compensation of collecting personal data.[259]

[251] *Id.* § 1798.140(v)(1).

[252] CAL. CIV. CODE §§ 1798.140(v)(1)(L), (ae) (West 2025).

[253] *See* CAL. CIV. CODE §§ 1798.100–1798.125 (West 2025); *see also California Consumer Privacy Act (CCPA)*, CAL. OFF. ATT'Y GEN., https://oag.ca.gov/privacy/ccpa [https://perma.cc/3HP9-UHYU].

[254] CAL. CIV. CODE §§ 1798.100, 1798.110, 1798.115, 1798.130 (superseded on Jan. 1, 2023); CAL. CODE REGS. tit. 11, §§ 7024, 7031 (superseded on Mar. 29, 2023).

[255] CAL. CIV. CODE § 1798.105 (superseded 2023).

[256] CAL. CIV. CODE § 1798.120(a) (superseded 2023).

[257] CAL. CIV. CODE § 1798.125(a)(1)(A) to (D) (superseded on Jan. 1, 2023); CAL. CODE REGS. tit. 11, §§ 7080-7081 (superseded on Mar. 29, 2023).

[258] *See California Consumer Privacy Act (CCPA)*, *supra* note 256.

[259] CAL. CIV. CODE §§ 1798.120(c–d), 1798.125 (b)(1–3) (superseded 2023); *see also* Harris, *supra* note 36, at 229.

B. CPRA

[83] California voters subsequently amended the CCPA by passing a ballot initiative, also known as Proposition 24, to enact the CPRA.[260] The CPRA expands the scope of the CCPA whilst introducing new privacy rights to protect the interests of consumers.[261] The CPRA establishes a new enforcement body, the California Privacy Protection Agency, which commenced enforcement of the CPRA on the 1st July 2023.[262] Most notably, the CPRA means that California consumers now have the right to request the correction of inaccurate personal information that a business possesses about them[263] and the right to limit the use and disclosure of sensitive information collected about them.[264]

C. CCPA, CPRA & Blockchain

[84] Whilst there is a dearth of literature examining the compatibility of the CCPA and CPRA to blockchain technology, Rebecca Harris, Attorney Roy Wyman, and Attorney Pritesh Shah point out that blockchain technology and the CCPA could fundamentally conflict due to being drafted in a way that is insensitive to developing technology and blockchain's characteristics.[265] Specifically, Harris and Shah comment that blockchain's immutable nature is incompatible with the

[260] California Consumer Privacy Act of 2018, *amended by*, the California Privacy Rights Act of 2020, CAL. CIV. CODE § 1798.100 (effective Jan. 1, 2023); *see also Laws & Regulations*, CAL. PRIV. PROT. AGENCY, https://cppa.ca.gov/regulations/ [https://perma.cc/299K-JNU8].

[261] *Laws & Regulations*, *supra* note 263.

[262] CAL. CIV. CODE §§ 1798.185(d), 1798.199.10–40, 1798.199.95 (West 2025); CAL. CIV. CODE §§ 1798.199.45–85, 1798.199.100 (West 2025); CAL. CODE REGS. tit. 11, § 7300–04 (2025); *see also Laws & Regulations*, *supra* note 263.

[263] CAL. CIV. CODE § 1798.106(a); CAL. CODE REGS. tit. 11, § 7023 (2025); *see also California Consumer Privacy Act (CCPA)*, *supra* note 249.

[264] CAL. CIV. CODE § 1798.121 (West 2025); CAL. CODE REGS. tit. 11, § 7027 (2025); *see also California Consumer Privacy Act (CCPA)*, *supra* note 249.

[265] Harris, *supra* note 36, at 226; Wyman, *supra* note 214, at 11; SHAH ET AL., *supra* note 12, at 6.

CCPA's 'right to be forgotten' provisions, which require user data to be deleted on request.[266] Furthermore, Shah identifies that individual rights provided by the CCPA and CPRA, such as the right of correction, the right to opt-out, and the right to limit use and disclosure of sensitive information, may also facilitate an identical issue and conflict with blockchain technology.[267]

[85] Gustavo Alza, writing in the Santa Clara High Technology Law Journal, takes a different approach, suggesting that whilst the CCPA's right to deletion will conflict with blockchain technology, businesses should adapt blockchain to comply with the CCPA, such as developing blockchain in a way that personal information is not collected and alterations can be made, as this builds consumer trust.[268] Therefore, Alza comments that ultimately the CCPA does not outlaw blockchain technology, and that permissioned blockchains should be developed where responsibility can be specifically assigned. [269]

[86] Professor Michele Benedetto Neitz takes a nuanced stance, commenting that in relation to state legislative efforts, the law always moves more slowly than technology, and California's slow method of law-making is contributory to a lack of blockchain legislation.[270] However, Neitz also suggests that California's measured approach to blockchain legislation may lead to a more balanced and successful legislative scheme in the long run.[271]

[87] Therefore, it might be considered that the protection afforded by the CCPA and CPRA is inadequate, as they conflict with the

[266] Harris, *supra* note 38, at 226; SHAH ET AL., *supra* note 11, at 6.

[267] SHAH ET AL, *supra* note 11, at 6.

[268] Gustavo Alza, *Blockchain & CCPA*, 37 SANTA CLARA HIGH TECH. L.J. 231, 252 (2021).

[269] *Id*. at 255.

[270] Michele Benedetto Neitz, *How to Regulate Blockchain's Real-Life Applications: Lessons from the California Blockchain Working Group,* 61 JURIMETRICS J. *185*, 192, 212 (2021).

[271] *Id*. at 214.

fundamental characteristics of blockchain technology. There are suggestions that the development of blockchain technology should be adapted to suit the slow pace of lawmakers;[272] however, the feasibility of this suggestion may be debated.

D. State v. Federal Privacy Legislation

[88] Due to the 'patchwork' nature of privacy legislation in the U.S. as a result of both federal and state legislative efforts, there is a question within the literature as to whether the current U.S. approach to privacy legislation is adequate. Literature overwhelmingly argues that the current U.S. legal framework to protect an individual right to privacy is inadequate and reflects how the law is on the backfoot to regulating developing technology.

[89] Attorney Marissa Wong comments that the current "scatter-shot" of sector and state-based privacy laws is ineffective as loopholes still exist, including "big tech" companies that argue they do not sell data but simply share it.[273] Moreover, different privacy laws lead to confusion among consumers as well as businesses.[274] Furthermore, state residents such as those in California cannot be assured that the data protections provided by their state laws, such as the CCPA, will remain protected from state to state.[275] Wong suggests that a comprehensive federal privacy framework that pre-empts state law and provides redress would unify data protection enforcement, make the application of privacy laws more consistent, and relieve the burden of trying to ensure compliance with not just multiple state laws, but across different sectors.[276]

[272] *See* Alza, *supra* note 271, at 255.

[273] Wong, *supra* note 243, at 305, 310.

[274] *Id*. at 308.

[275] *Id*. at 309.

[276] *Id*. at 309.

[90] The argument in favour of a comprehensive federal privacy law is also supported by Michael Beckerman, president and chief executive of the D.C. based lobbying group, the Internet Association, who suggests that a federal law is needed to set consistent standards, regardless of where the individual lives, because Americans cannot be confident that their data remains confidential when they travel from state to state.[277] Moreover, Beckerman points out that, ironically, to ensure compliance with certain state laws, online services must choose between applying the standard of one state or collecting further personal information.[278] This might require, for instance, choosing whether to treat all individuals as California residents or ascertaining further information to confirm a person is a resident of California.[279]

E. Interim Conclusions

[91] The State of California does not have specific legislation that responds to the privacy concerns of blockchain technology, meaning that California's comprehensive privacy laws, the CCPA[280] and the CPRA[281] may be applicable. The literature indicates that the CCPA and CPRA are inadequate to address the privacy concerns of blockchain technology due to being drafted in a way that conflicts with blockchain's fundamental characteristics.[282] For instance, the immutability of blockchain conflicts with the right to deletion and correction.[283] Some suggestions support the view that blockchain technology should be developed and adapted to comply with the existing state laws, or that the

[277] Michael Beckerman, *Americans Will Pay a Price for State Privacy Laws*, N.Y. TIMES (Oct. 14, 2019), https://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html [https://perma.cc/L6N6-X8SM].

[278] *Id*.

[279] *Id*.

[280] California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (effective Jan. 1, 2025).

[281] CAL. CIV. CODE §§ 1798.100–.199.100 (West 2023) (effective Jan. 1, 2023).

[282] Harris, *supra* note 36, at 226; SHAH ET AL., *supra* note 11.

[283] Harris, *supra* note 36, at 226; SHAH ET AL., *supra* note 11.

state law will eventually become balanced in the long run.[284] However, the practicality of these suggestions remains to be explored.

[92] Section IV also indicates that the 'patchwork' response of the U.S. towards the protection of individual privacy rights is inadequate. The 'patchwork' response may be considered inadequate as there is a lack of legislative consistency, which allows for loopholes to be exploited by "big tech" companies.[285] It is proposed in the literature that the U.S. is missing a comprehensive federal privacy law to ensure a unified approach to privacy legislation.[286] However, similar to suggestions made regarding the CCPA and CPRA, it is difficult to predict if an updated and new federal legislation would be achievable.

VI. CONCLUDING REMARKS

[93] This article has examined the responses of the courts and legislatures at the federal and state levels, to the privacy concerns raised by blockchain technology. The overall conclusion that may be drawn is that the courts and legislatures in the U.S. have not responded to the privacy concerns of blockchain technology and that the approaches taken to date to protect individual privacy rights at the federal and state levels have been inadequate. Specifically, Sections II to IV all reveal that the law remains on the backfoot to technological advancements such as blockchain technology and that it is ultimately for the federal legislature to decide if they wish to respond to these privacy concerns, as they are in the best position to do so. However, as this article has suggested, technology is likely to remain one step ahead of the law, which means that the law will continue to play a game of catch-up. In the end, federal legislation may eventually be drafted. While this response may come later than desired, it could still pave the way for meaningful solutions to the privacy concerns raised by blockchain technology.

---

[284] Alza, *supra* note 271, at 255; Neitz, *supra* note 273, at 214.

[285] Wong, *supra* note 243, at 305, 310.

[286] Wong, *supra* note 243, at 309; Beckerman, *supra* note 281.