




Spring 2024

Fitting a Block into a Sphere Mold: The Inadequacy of Current Data Privacy Regulations in Protecting Data Privacy within the Blockchain Space

Jenny Yang

Washington and Lee University School of Law, yang.j24@law.wlu.edu

Follow this and additional works at: <https://scholarlycommons.law.wlu.edu/crsj>

 Part of the [Civil Rights and Discrimination Commons](#), [Computer Law Commons](#), [Human Rights Law Commons](#), [Privacy Law Commons](#), and the [Science and Technology Law Commons](#)

Recommended Citation

Jenny Yang, *Fitting a Block into a Sphere Mold: The Inadequacy of Current Data Privacy Regulations in Protecting Data Privacy within the Blockchain Space*, 30 Wash. & Lee J. Civ. Rts. & Soc. Just. 377 (2024). Available at: <https://scholarlycommons.law.wlu.edu/crsj/vol30/iss2/11>

This Note is brought to you for free and open access by the Washington and Lee Journal of Civil Rights and Social Justice at Washington and Lee University School of Law Scholarly Commons. It has been accepted for inclusion in Washington and Lee Journal of Civil Rights and Social Justice by an authorized editor of Washington and Lee University School of Law Scholarly Commons. For more information, please contact christensena@wlu.edu.

Fitting a Block into a Sphere Mold: The Inadequacy of Current Data Privacy Regulations in Protecting Data Privacy within the Blockchain Space

Jenny Yang*

Abstract

Despite global imposition of data privacy laws and regulations, data privacy is a nonexistent luxury amongst the data-charged world we live in. Data privacy has long been established as a fundamental right. Entities have successfully established robust methodologies around existing data privacy laws and regulations to utilize past consumer behavior to predict, impact and manipulate current and future consumer behaviors. This phenomenon has been commonly coined as “corporate surveillance.” Emerging spaces arising through technological developments have greater access into consumer data to impact economic choices. Specifically, the blockchain space, through its unique open-source and permanent traits, has been able to skirt around data privacy laws and regulations through its nonconventional decentralized nature. Current data privacy regulations are geared towards centralized systems, thus not readily applicable to decentralized blockchains. While most blockchain spaces boast of increased security, the danger lies within the increased volume and access into data collection itself that is not regulated, prompting greater invitation

* J.D. Candidate, May 2024, Washington and Lee University School of Law. I would like to extend my sincerest appreciation to everyone who helped me throughout the Note writing process – I could not have done this without my village of supporters. Thank you to my faculty advisor, Professor Joshua A. Fairfield, and my mentor, Professor Michael Bombace, for the continuous insights, direction, and advice that allowed me to transform my ideas into this Note. Thank you to my partner Alex Lim, my family (specifically Jason Yang and Jody Yang), and friends who listened, encouraged, and supported me through each step of the process.

for bad actors. Countries, especially the United States, should impose stricter data privacy regulations to impact the blockchain space to provide consumers greater data protection within emerging new technological spaces. Blockchain spaces should also have minimum data privacy protection mechanisms such as the usage of zero-knowledge proofs and integration of data privacy regulations at the system’s foundation. Through the combination of establishing necessary requirements and heightened regulations, consumer data and privacy can be better protected as a fundamental right.

Table of Contents

I. Introduction 379

II. Capitalist Economy Promotes Surveillance Capitalism
Through Manipulating Economic Choice 383

 A. The Necessity of Economic Freedom on Market Efficiency 384

 B. The Rise and Power of Surveillance Capitalism 388

III. Privacy is a Recognized Fundamental Right 394

 A. Protection of Data Privacy 396

IV. Current Data Privacy Regulation 398

 A. State Data Privacy Laws and Regulations 402

 B. Global Data Privacy Laws and Regulations 404

V. Understanding Blockchain Technology, Benefits, Uses, and
Data Retention 406

 A. Building Blocks of Blockchain 407

 B. Data Retention and Traceability on Blockchains 411

 C. Blockchain Usages 415

VI. Application of Current Data Privacy Regulations 420

 A. Corporations Are Skirting Around Current Data Privacy
Regulations 421

 B. Non-Applicability of Existing Regulations on Blockchain . 423

VII. The Necessity for Standardized Data Privacy Regulations for
Blockchains and Emerging Data Collecting Technologies 429

 A. Required Implementation of Zero-Knowledge Proofs 430

B. Call for Standardized Blockchain Regulations.....	434
VIII. Conclusion	437

I. Introduction

You are being tracked.¹ Your every online click, statement, and movement has been recorded somewhere amongst the ether for corporations to predict and manipulate your *next* click, statement, and movement.² Your data is more valuable than gold, and it is being collected and utilized by corporations as *you* pay for services and goods.³ This phenomenon is the epitome of modern-day online blind bargains.

Corporations have long utilized past human behavior data to heavily influence future human behavior of similar kinds.⁴ Due to the immense power and storytelling data allows, it has been leveraged across every industry to not only maximize profit but also to dominate markets.⁵ If you have ever purchased something online, opened a bank account, signed up for a subscription, researched a topic or anything else online, you have been subjected

1. See Alicia Shelton, *A Reasonable Expectation of Privacy Online: “Do Not Track” Legislation*, 45 U. BALT. L.F. 35, 35 (2014) (establishing the inherent nature of tracking on all online activities).

2. See Dave Davies, *How Tech Companies Track Your Every Move and Put Your Data Up for Sale*, NPR: FRESH AIR (July 31, 2019, 1:29 PM) (outlining areas of data corporations collect on web browsers despite people thinking their activities and information are private) [perma.cc/R76M-EKLJ].

3. See Jeff Tyler, *How Hard is it to Opt Out of Third-Party Data Collection*, MARKETPLACE (May 22, 2013) (recognizing the incredibly difficult mechanisms corporations have implemented to opt-out of data collection for consumers, which work in the corporations’ favor because consumers go with the status quo) [perma.cc/T739-WRLV].

4. See 6 *Inspiring Examples of Data-Driven Companies (Key Takeaways Included)*, UNSCRAMBL (June 15, 2021) (explaining how data-driven companies such as McDonald’s, Google, Coca-Cola and banks utilize collected data from prior consumer activities to produce insights that are then readily integrated to optimize future operations) [perma.cc/8CAP-T9AB].

5. See *id.* (suggesting that using data is a corporation norm amongst major companies because it allows them to predict and direct their marketing tactics and products amongst consumers who will be most receptive to their goods and services).

to a form of corporate surveillance.⁶ The usage of data to understand and control both monumental and minute decisions has been deeply interwoven through almost all types of forums consumers utilize in their day-to-day life.⁷

While the rise of technological advances has allowed greater access to a greater assortment of consumer goods and products, it has also created greater ease of accessibility for entities to collect data and influence consumers' decisions.⁸ Specifically, the introduction of blockchains and various cryptocurrencies have allowed this to be done in a decentralized fashion.⁹ Protocols and platforms, either utilizing existing blockchains or building new ones to accomplish their wide array of missions, allow data to be collected in a new approach promoted to be more efficient, faster, and have greater connectivity to one another.¹⁰ Blockchains are able to bridge the gap between socio-economic conditions that traditionally set specific groups apart.¹¹ The ease of use and accessibility allows anyone with internet connectivity to be interconnected with those of similar missions.¹² However, as with

6. See Shelton, *supra* note 1, at 35–36 (listing common, everyday actions which leave a digital footprint which can be tracked).

7. See *id.* (arguing that the use of technological advances, such as blockchain technologies, has greatly enhanced businesses' ability to utilize data more effectively and efficiently).

8. See *How Technology is Revolutionizing Data Collection*, FORMPLUS BLOG (last updated July 27, 2023) (stating that rapid technological advances contribute to transforming the process of collection, storage, and analysis of data to allow businesses to leverage real-time data in their decision-making processes) [perma.cc/U9Y6-ENJH].

9. See Nadav Roiter, *How Data Collection Networks Are Powering a Silent Blockchain-Like Revolution*, BRIGHT DATA (Feb. 23, 2021) (explaining how the collaborative and accessible nature of blockchains can allow business communities to gather more data to advance the free market theory) [perma.cc/EXH9-ZUX9].

10. *Benefits of Blockchain*, IBM [perma.cc/E3NJ-294A].

11. See Nathan Reiff, *How Blockchain Can Help Emerging Economies*, INVESTOPEDIA (last updated Oct. 26, 2021) (noting that the strongest appeal of blockchain technologies amongst different societal groups lies within its ability to be easily accessible, especially for banking services for the underbanked across the globe) [perma.cc/J6AV-T7DC].

12. See *id.* (“With blockchain technology, users across the globe could access banking services where they otherwise wouldn’t have the opportunity. Particularly, individuals in emerging economies where there are not standard

all new spaces, regulations are lacking in providing sufficient applicable guidance and protection for consumers whose data privacy rights are at even greater risk.¹³

The United States' federalist structure enabled the oversight of data privacy by both federal agencies and state governments, but is currently majorly regulated at the state level, ranging from robust to nonexistent.¹⁴ Both federal and state consumer data privacy regulations are inadequate against conglomerate corporations who understand how to navigate around the vague regulations in place.¹⁵ In addition, current regulations are largely geared towards centralized systems surrounding data.¹⁶ The inadaptability and vast data privacy regulation differences amongst states results in a lack of comprehensive data protection regulations to encompass the blockchain and decentralized finance (DeFi) space, leaving consumers' data privacy at high risk of being misused.¹⁷

The benefits of blockchain and lure of data immutability should not be at the price of infringing upon the fundamental human right to one's data privacy. This Note will focus on the increased need for limitations of this power to be placed through

banks readily accessible could make use of blockchain technology to access these services.”).

13. See Aditya Narain & Marina Moretti, *Regulating Crypto*, INT'L MONETARY FUND (Sep. 2022) (explaining that the growth in market capitalization of crypto assets significantly increased financial regulations to work on policies to regulate the space, but it is hard for regulations to apply or develop new policies because crypto is evolving too fast) [perma.cc/5CGV-V56K].

14. See Kristin M. Hadgis et al., *Data Privacy: Evolving Updates to the Global Landscape*, MORGAN LEWIS (Sep. 14, 2022) (outlining all the different types of state regulations relating to data privacy that span from robust to bare minimum since there is no federal data privacy law to set the minimum) [perma.cc/9VZJ-P7QX].

15. See *id.* (reiterating the importance for a comprehensive federal data regulation to ensure data privacy can be protected through corporation's data collection and usage).

16. See Pritesh Shah et al, *Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies*, THOMSON REUTERS: PRACTICAL LAW 3 (2019) (defining the primary tension between current data privacy laws and blockchain as the former's focus on a centralized controller of data retention and usage that is inherently nonexistent in blockchain infrastructure) [perma.cc/WT5Q-9EBV].

17. See *id.* (discussing how legislators' lack of focus on how blockchain technology and its unique features impact data privacy can contribute to a higher risk of unprotected data usage) [perma.cc/WT5Q-9EBV].

uniform federal regulations that are readily adaptable within the blockchain space or any new industry arising in the future that interacts with data. This is required to ensure consumers' data are not exploited by large corporations and emerging technologies. Through the rapid speed this space develops and changes, regulations have to be flexible to adapt.

Part II of this Note will introduce the foundations of today's capitalist society: the basics of economic choice and surveillance capitalism.¹⁸ These two concepts are crucial to understand how corporations today are operating through data utilization and the impact data plays in business decisions.¹⁹

Part III provides the fundamental background into privacy.²⁰ It is important to understand what is at risk when corporations are infringing upon a coveted established human right through exploiting or manipulating human behavior with data collection. Data or information data is a subsection of privacy that has been recognized as crucial to protect for consumers.²¹

Part IV delves into existing data privacy laws to outline the effects of federalist application and the division of regulations based on industry and data type.²² The brief history of these laws will provide insight into their deficiency in protecting consumers not only in the blockchain space, but any potential new industries that will be collecting large masses of data in the future. This Part will also provide a brief glimpse into state's efforts to ensure consumer data is protected and global examples of how data is protected in other countries.

Part V introduces blockchain through providing a glimpse into how the technology operates, a brief history of its rise, popularity, usage, and how various protocols and platforms have integrated

18. Discussion *infra* Part II.

19. See ANNA BERNASEK & D. T. MONGAN, ALL YOU CAN PAY 112 (2015) (discussing the specificity with which companies can track individual's data and preferences).

20. Discussion *infra* Part III.

21. See *What Is Data Privacy*, CLOUD FLARE ("Data privacy is the protection of personal data from those who should not have access to it and the ability of individuals to determine who can access their personal information.") [perma.cc/C6MB-9YG8].

22. Discussion *infra* Part IV.

usage to their advantage.²³ The interwoven push and pull of data immutability and lack of data privacy is illustrated by the underlying framework of data collection on typical blockchain technologies.

Part VI explains how blockchain's data integration and retention combats traditional data privacy regulations and laws to render them inapplicable due to their lack of adaptability.²⁴ Current data privacy regulations are proven to even be ineffective against corporations curtailing the fine lines of data usage, much less on new technologies.

Part VII proposes a framework of required federal regulations for blockchains and any new arising industry that collects data.²⁵ Additionally, this Part provides insight into currently proposed federal legislations and features global examples that will be beneficial to consumers in the long run. While blockchains are inherently more secure than traditional means of data ledgers and have implemented advanced technologies such as zero-knowledge proofs, they may still fall short in the long-run if government regulations and laws cannot keep up with new developments. Implementing zero-knowledge proofs across every blockchain is the minimum for meaningful data privacy. The United States should also create a new inclusive data privacy legislation to protect personal data.

II. Capitalist Economy Promotes Surveillance Capitalism Through Manipulating Economic Choice

A majority of economies today are classified as mixed capitalist economies where market movements are largely controlled and impacted by private actors with profitability as the ultimate goal.²⁶ Governments interject to correct market failures

23. Discussion *infra* Part V.

24. Discussion *infra* Part VI.

25. Discussion *infra* Part VII.

26. See Sarwat Jahan & Ahmed Saber Mahmud, *What Is Capitalism?*, INT'L MONETARY FUND: FIN. & DEV. (explaining how owning and controlling private capital assets allow for capitalist economies to operate independently of government intervention under the notion of rational self-interest) [perma.cc/E92P-ZHW2].

such as public safety, social welfare, pollution, and monopolization.²⁷ At the core of mixed capitalist economies are consumers who possess economic freedom, which includes the interaction of “(1) personal choice, (2) voluntary exchange coordinated by markets, (3) freedom to enter and compete in markets, and (4) protection of persons and their property from aggression by others.”²⁸ In essence, people engage in economic activity at their own free will. Empirical data consistently show a direct positive correlation between greater economic freedom and greater economic growth.²⁹ It is this foundation that promotes economic choice amongst consumers and provides the gateway to surveillance capitalism.³⁰

A. *The Necessity of Economic Freedom on Market Efficiency*

What are you willing to pay for a bottle of water? Well, it depends on your financial situation, location, ease of convenience to obtain the good, and totality of your resources. It could be a negligible cost at home where you can get tap water. It could be \$2 if you were out running errands and needed a drink on the way. It could be \$5 if you were on a road trip in the middle of nowhere and stopped at a gas station. Increase it to \$10 at an airport when you forgot to bring a reusable bottle. Probably infinite if you were stranded in a desert and in dire need of water.

27. See Sean Ross, *Is the United States a Market Economy or a Mixed Economy?*, INVESTOPEDIA (Dec. 16, 2023) (“A mixed economic system protects some private property and allows a level of economic freedom in the use of capital, but also allows for governments to intervene in economic activities in order to achieve social aims and for the public good.”) [perma.cc/4JGH-42GR].

28. *Economic Freedom Basics*, FRASER INST [perma.cc/SA7T-U964].

29. See Robert A. Lawson, *Economic Freedom*, LIBR. ECON. & LIBERTY (presenting data showing economic freedom’s impact on several factors within a nation such as GDP per capita and economy size) [perma.cc/B6GL-2DG2].

30. See *The Benefits of Mixed Economies*, LUMEN LEARNING (detailing the advantages of mixed economies for both sides of a transaction where consumers have a choice on what they wish to purchase while private businesses have a choice on how to run their businesses through production, pricing, employment, and marketing) [perma.cc/5J6X-86P2].

Scarcity is the backbone of economics.³¹ The balance of preferences and resources available allows for both individuals and businesses to make economic decisions.³² Sufficient resources, including time and finances, would realistically allow one to purchase any water bottle due to convenience; the opportunity cost of alternatives would simply not compare to resources available.³³ Individuals with limited financial resources render searching for product, such as tap water, within their purchasing power.³⁴ Essentially, there is a difference between how much one is willing to pay for something due to need versus what they would actually pay in the current market given the specific conditions.³⁵ This is economic surplus.³⁶

Free markets are able to operate efficiently through economic surplus, the economic measurement of consumer benefits resulting from market competition.³⁷ Total economic surplus is made up of

31. See *Scarcity*, NAT'L GEOGRAPHIC SOC'Y (Oct. 19, 2023) (affirming the importance of scarcity to impact supply and demand in markets which allows for limitations on consumer choice based on one's resources) [perma.cc/AEK7-X64X].

32. See *id.* ("Certain limits of scarcity can be balanced by taking resources from one area and using them somewhere else . . . This is done by trying to strike a balance between what consumers need or want, what the government needs, and what will be an efficient use of resources to maximize profits.").

33. See Jason Fernando, *Opportunity Cost: Definition, Calculation Formula, and Examples*, INVESTOPEdia (Oct. 31, 2023) ("Opportunity cost represents the potential benefits that a business, an investor, or an individual consumer misses out on when choosing one alternative over another. While opportunity costs can't be predicted with total certainty, taking them into consideration can lead to better decision making.") [perma.cc/KJE2-JC8Y].

34. See BERNASEK & MONGAN, *supra* note 19, at 3 (explaining the ability of businesses to engage in different marketing tactics within an industry of similar products due to understanding consumers' needs and wants, such as creating a more luxurious sparkling water like Pierre aimed at specific economic groups who want or have a higher standard of living).

35. See *id.* (providing an example of air being a free resource but one would be willing to pay any amount if they are drowning underwater, requiring balances of needs and wants).

36. See Melanie Lockert, *What Is Economic Surplus and How Does It Work?*, BUS. INSIDER: PERS. FIN. (last updated July 21, 2022, 10:29 AM) ("Economic surplus refers to the respective gains that a consumer or producer gets within an economic activity and is the combined benefit, sometimes referred to as 'total welfare.'") [perma.cc/Z8JL-W8R5].

37. See *Economic Surplus Formula: How to Calculate and Example*, SHOPIFY (June 16, 2023) (demonstrating how market forces from both consumers and

consumer surplus and producer surplus.³⁸ Producer surplus is the profit businesses realize through the sale of their good or services.³⁹ If the market value is higher than the producer price (consumers are willing to pay more than what producer is charging) then producers reap an economic benefit.⁴⁰ Producer surplus' existence allow for increased utility on both the consumer and producer sides; this gap promotes fairer market prices through price competition and consumers' ability to shop the market.⁴¹ On the other hand, there is consumer surplus, which is the surplus captured by the consumer via the maximum price one is willing to pay for a good or service and the price they actually pay.⁴² Maximizing enjoyment for consumers means paying less but getting more, while businesses are doing the opposite by charging more and delivering less to maximize profits.⁴³ Market competition is produced by keeping the exact price a consumer is willing to purchase a good or service a mystery, which provides the most efficient price to satisfy both the producer and consumer.⁴⁴ A fair market rests on minimalizing the information parties know of each other's surplus. This dynamic is at risk due to the knowledge gap

producers enable a constantly changing equilibrium of economic surplus efficiency) [perma.cc/857E-WPYN].

38. See *id.* (providing the economic surplus equation and various ways it can be changed to figure out market equilibrium given set data).

39. See BERNASEK & MONGAN, *supra* note 19, at 4 (emphasizing this is just a simple profit analysis for businesses with all other factors equal).

40. See Chris B. Murphy, *Consumer Surplus Definition, Measurement, and Example*, INVESTOPEDIA (last updated Sep. 1, 2022) (explaining market surplus is usually a balance of consumer or producer surplus unless there is perfect equilibrium between all prices, which is rare in a competitive market) [perma.cc/UJ3L-MT8T].

41. See BERNASEK & MONGAN, *supra* note 19, at 176 (describing the ability of larger corporations to adapt and utilize this consumer behavior to their advantage to enable the highest level of producer surplus).

42. See *id.* (integrating the water pricing example again to demonstrate an individual with more resources will be able to purchase more readily available commodities).

43. Irena Asmundson, *Supply and Demand: Why Markets Tick*, INT'L MONETARY FUND [perma.cc/3L4D-4RNR].

44. See *What Is the Consumer Surplus Formula?*, CB INSIGHTS (illustrating surplus through the example of a consumer's willingness to buy a car at \$25,000 and a car dealership is willing to sell a car for \$25,000 where both parties are satisfied through finding a market equilibrium of supply and demand) [perma.cc/59AM-93H3].

the use of data creates because producers can pinpoint consumer surplus without disclosing their own.

Many factors, such as personal preferences and financial ability, are relevant when it comes to the satisfaction derived from a good or service, which impacts the price one is willing to pay.⁴⁵ Businesses will utilize consumer surplus gaps to find prices that consumers are willing to pay based on these known preferences.⁴⁶ Within a free market where producers are competitive in goods and service, price is a device utilized to secure market share.⁴⁷ For markets to be truly competitive, everyone can pay the same market-clearing price, even if there are groups of individuals who are willing to pay more.⁴⁸ This is especially important for low socio-economic classes that rely on price elasticity to conduct their consumer decisions.⁴⁹

As the markets move from traditional mass markets to segmentation, not only has efficiency increased, but the ability for businesses to sell the *same* goods and services to *different* socio-economic classes also significantly increased.⁵⁰ Segmentation is

45. See *Consumer Surplus*, CORP. FIN. INST. (last updated Nov. 26, 2022) (recognizing personal preferences and financial ability are key factors in calculating satisfaction and worth within a good or service) [perma.cc/JTB4-UAQC]; see also BERNASEK & MONGAN, *supra* note 19, at 4 (“The difference between what something is worth to you and what you actually give in exchange for it can be very personal. Surplus varies from person to person, time to time and from situation to situation.”).

46. See BERNASEK & MONGAN, *supra* note 19, at 110 (discussing the disguise of mass customization as personal customization to consumers to give off the impression they are personally catering to one’s needs and can price accordingly *after* discovering *exactly* what is wanted).

47. See Murphy, *supra* note 40 (showcasing more competitive markets are usually met with lower prices as consumers are easily able to shop around to find the best price match, meaning consumer surplus will also increase).

48. See BERNASEK & MONGAN, *supra* note 19, at 17 (explaining how producers base consumers’ willingness to pay for a good or service on marketing and research, which translates to bigger brands charging the average of what they think a majority of consumers will pay, in turn resulting in both consumer and producer surplus).

49. See *id.* at 204 (showing that utilizing new technologies can help corporations break through unnecessary noise and promote ease of prediction).

50. See *id.* at 34 (expounding upon how market segmentation allows for more choices for consumers, but it directly increases the range of prices and captures more consumer surplus over time, which blurs the line of what is considered to be fair for a good or service).

the separation of markets on similar items that have different prices resulting from corporations successfully capturing consumer surpluses to reflect each consumer's ability to pay.⁵¹ It is a key aspect of reinforcing social inequality since without open disclosure of fair pricing, price encapsulates everything at a single point for each individual's decision making.⁵² Capturing greater producer surplus through usage of new technological forces and collection of consumer datapoints allows for a greater knowledge gap between consumers and producers within the market.⁵³ This motive has become both the cause and effect of surveillance capitalism.

B. *The Rise and Power of Surveillance Capitalism*

The complexity and marketability of data has allowed companies to utilize personal data to predict and dictate consumers' behaviors.⁵⁴ The airline industry is a prime example to help illustrate this phenomenon.⁵⁵ Airline corporations utilize the knowledge gained from real-time data collection on current consumers across various platforms and apply it to future consumers.⁵⁶ Picture two New York based individuals researching a flight to Paris. One has a net worth of \$100 million, while the

51. *See id.* at 33 (emphasizing the break-even cost for producers is not as important as the consumer's willingness to pay price, which is gathered through datapoints).

52. *See id.* (adding another negative factor about segmentation—those prices do not reflect real costs and decreases consumers' power over time).

53. *Id.* at 34.

54. *See id.* at 154 (illustrating how only ten major data giants have become the middlemen on transactions that cover goods and services of every aspect of life to match specific buyers with sellers and the data will allow data giants to start predicting consumers' wants and needs).

55. *See* Shoshana Zuboff, *You Are Now Remotely Controlled*, N.Y. TIMES (Jan. 24, 2020) (exemplifying Delta Airlines' pilot of a new biometric data system at the Atlanta airport that allowed passengers to easily opt-in to facial recognition technologies, which provided Delta more information about their customer base) [perma.cc/W6PM-NRFF].

56. *See How Airlines Are Using Big Data*, MEDIUM (Apr. 10, 2017) (explaining that leveraging data insights provides companies a greater competitive edge and corporations within the airline industry are experts in utilizing their consumer data through the process of formulating personalized customer experiences and successful loyalty programs) [perma.cc/9ZRF-T5UV].

other has \$100,000. Through a collection of their past online activities, including search histories, purchases, banking affiliations, social media relationships or IP addresses, major online search platforms and airlines companies are able to purchase all of this data to create a personalized story for each individual to understand their price tolerance.⁵⁷ While pricing is an art involving various factors, all other factors are held constant in this simple scenario to better understand the effect and power of data.⁵⁸ The data collected through past activities provides insight to not only reveal each individual's *ability* to but also their *willingness* to pay through details, like the frequency of their searches, to obtain a sense of urgency.⁵⁹ Simultaneously, the corporations are collecting *more* data for future references.⁶⁰ Ultimately, not only does the data insights allow the airline to charge the \$100 million individual more for the *same seat* than the \$100,000 individual, the airline is also able to price the seat at a level closest to each individual's *willingness* to pay.⁶¹ This directly leads to an increase of producer surplus and a decrease of consumer surplus. Price personalization reduces consumer choice

57. See *id.* (explaining that tracking information like search history, purchase history, checked luggage, departure and arrival times, destinations, in-flight food choices, rentals, number of travelers, credit card is the norm for airlines).

58. See Desirae Odjick, *How to Price a Product in 3 Simple Steps (2023)*, SHOPIFY (Oct. 10, 2022) (explaining that choosing the correct pricing is crucial to a business model and can directly impact crucial future business decisions, thus companies expend a great deal of time and resources in creating the perfect pricing strategy for their goods and/or services) [perma.cc/CDA2-WPLD].

59. See BERNASEK & MONGAN, *supra* note 19, at 164–68 (using an example of a restaurant that customizes their prices to the consumer to illustrate the massive amount of information a corporation can obtain on its costumers and the way the data can be used to maximize profit).

60. See *id.* at 168 (discussing how the collection of data accumulates to an economy in which “natural monopolies flourish and immense economic power is overwhelmingly concentrated in the hands of a few”).

61. See *id.* at 127 (stating that United Airlines has over thirty-eight different types of airline tickets, which is the norm for airlines as they usually have different fare fees, rules, and flyer rewards to reflect customers' *willingness to pay* and to cover such activities); see also Alexandra Twin, *What Is Price Discrimination and How Does It Work?*, INVESTOPEDIA (last updated June 13, 2022) (pricing is based on consumers' price elasticity where consumers in a relatively inelastic market will pay higher prices compared to consumers in elastic markets) [perma.cc/ZQZ3-NBM8].

when situations are dire, while maximizing profits for corporations within each clientele group.⁶² The pricing tactics utilized in the airline ticket example is not special to the airline space. In fact, this exact methodology is utilized across everything consumers purchase to ensure price maximization. That is the true power of data and how it has become the primary force behind surveillance capitalism.

Surveillance capitalism, coined by Shoshana Zuboff, is a modern-day phenomenon of capitalizing human experience into behavioral data.⁶³ The data collected can be employed to improve the product or services offered, but it is most often used in machine-learning or artificial intelligence (AI) algorithms to create predictions anticipating consumer behavior for future markets.⁶⁴ This methodology allows corporations to not only predict future behavior but also influence consumer behavior towards more profitable outcomes.⁶⁵ Consumers are tracked both online and offline through their online blueprint and the persistent tracking methods to paint a full picture of one's consumption behavior.⁶⁶ Surveillance capitalism is on the rise due to the asymmetric power between those with the data information and those without.⁶⁷

62. See *Price Discrimination*, STUDYSMARTER (highlighting ways some monopolies can take advantage of price discrimination tactics to capture a greater market share, which initiates a higher barrier to entry for other companies while simultaneously limiting product choices for consumers) [perma.cc/GHZ4-QN2C].

63. See SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER* 8 (2018) (warning of data's power to manipulate consumers' behavior).

64. See *id.* (pointing out that the competitive dynamics of new markets drive surveillance capitalists to acquire ever-more-predictive sources of behavioral surplus such as our voices, personalities, and emotions to ensure they are at the forefront of their industries).

65. See *id.* (elucidating that competitive pressures produced from the shift in data directly correlates with the rise of machine processes that not only know our behavior but also can shape our behavior, transforming knowledge into power in order to have some level of control over consumers).

66. See Joshua A.T. Fairfield, "*Do-Not-Track*" as Contract, 14 VAND. J. ENT. & TECH. L. 545, 549 (2012) ("[C]orporations can often gain detailed pictures of where consumers go in real space and can correlate that information with consumers' online behaviors. In short, there is no longer any place to hide, online or off.").

67. See BERNASEK & MONGAN, *supra* note 19, at 178 (explaining that fine print on most contracts relating to consumer/producer relationships can hide a

Businesses utilize data collection systems within platforms aimed at consumers without sufficient disclosure.⁶⁸ Companies are able to easily collect our data insofar as they are complying with relevant laws and regulations, while consumers are no longer able to protect their data easily due to the lack of resources compared to corporations.⁶⁹ While there are multiple bills in front of Congress to provide different options for consumers to withdraw from being tracked, there are currently no concrete protections in place.⁷⁰

Corporations selling and buying personal data to utilize in their business decisions has long been an established phenomenon amongst twenty-first century markets where consumers usually are predisposed to automatically waive all rights when online.⁷¹ Consumer data holds sufficient power for modern-day corporations because it is essential for businesses to make impactful and profitable decisions.⁷² There are various types of data collected: personal, engagement, behavioral, and attitudinal.⁷³ The types of

firm's true intentions in collecting whichever data they desire as most consumers do not take the time to read agreements).

68. See ZUBOFF, *supra* note 63, at 11 (describing companies' ability to accumulate vast amounts of new knowledge from consumers via data collection to predict our futures to contribute to their gains).

69. See BERNASEK & MONGAN, *supra* note 19, at 62 (explaining that increasingly available data collection mechanisms lead to increased consumer vulnerability).

70. See *Consumer Data Privacy Laws*, BLOOMBERG L. (2024) ("The U.S. does not yet have a comprehensive federal consumer data protection law that covers all varieties of private data. But it does have several federal laws that protect specific data sets, such as the U.S. Privacy Act of 1974, HIPAA, COPPA, and the Gramm-Leach-Bliley Act.") [perma.cc/KL5L-KFQM].

71. See *id.* at 554 (stating usage of cookies and other tracking devices on various platforms allow ease of access into data and tracking activities).

72. See Petar Todorovski, *How Do Sales of Personal Data Work and How to Protect Yourself*, PRIV. AFFS. (Aug. 8, 2022) (revealing the immense industry and power data brokerages inherently hold as samples include a 2019 sale resulting in a \$4.4 billion acquisition of a data broker called Epsilon) [perma.cc/S4PS-TTS4].

73. See Max Freedman, *How Businesses Are Collecting Data (And What They're Doing with It)*, BUS. NEWS DAILY (last updated Jan. 23, 2023) [perma.cc/7NSK-QRW6].

1. Personal data. This category includes personally identifiable information such as Social Security numbers and gender, as well as nonpersonally identifiable

data collected does not only encompass personally identifiable information (PII) such as names, social security, email addresses, home addresses or phone numbers but also one's political views, online behavior, family life, and more.⁷⁴ A study showed a data broker has over 3,000 items of information on every consumer in the United States.⁷⁵

Technological advances have been the main driving force behind the ability for businesses and institutions to collect consumer data.⁷⁶ Companies use a combination of data collection methods, sources, and software to capture consumer data.⁷⁷ Through the development of machine learning algorithms and other forms of AI, data analytics are not only powerful but also fast to acquire and implement immediately.⁷⁸ The most important usages of this data are to structure marketing campaigns and impact consumer experience.⁷⁹ Data's strong predictive analysis traits enable engineers to understand the *why's*, which will directly allow them to make an extremely educated guess of what is wanted

information, including your IP address, web browser cookies and device IDs (which both your laptop and mobile device have).

2. Engagement data. This type of data details how consumers interact with a business's website, mobile apps, text messages, social media pages, emails, paid ads and customer service routes.

3. Behavioral data. This category includes transactional details such as purchase histories, product usage information (e.g., repeated actions) and qualitative data (e.g., mouse movement information).

4. Attitudinal data. This data type encompasses metrics on consumer satisfaction, purchase criteria, product desirability and more.

74. *Id.*

75. See BERNASEK & MONGAN, *supra* note 19, at 55 (highlighting that there is little to no information consumers can hide from data collection companies).

76. Freedman, *supra* note 73.

77. See *id.* (discussing direct collection of data from customers, data from indirect tracking, and integration of third party sources of customers).

78. See *id.* ("As machine learning algorithms and other forms of AI proliferate and improve, data analytics becomes an even more powerful field for breaking down the sea of data into manageable tidbits of actionable insights.").

79. See *id.* ("Contextualized data can help companies understand how consumers are engaging with and responding to their marketing campaigns, and adjust accordingly. This highly predictive use case gives businesses an idea of what consumers want based on what they have already done.").

or needed next.⁸⁰ While this data is supposedly used by major corporations to ensure consumers are provided with a more personalized online experience, a lot of the data is utilized to maximize their own profits via advertising and other product placements.⁸¹ Mass customization shifts consumers' focuses to wants rather than needs that are specifically tailored to their personal data.⁸² Segmentations of consumers is due to different purchase abilities.⁸³

Dynamic pricing is exacerbated with the rise of technological forces that are created solely to navigate utilizing data to price discriminate.⁸⁴ Price discrimination arises when consumers receive the same product or service, but pay different prices determined by the seller.⁸⁵ It centers on the premise of consumers' inability to pinpoint the true value of a good or service, whereas businesses are able to obtain more surplus from the knowledge gap.⁸⁶ Through new technology such as cookies and site trackers, businesses are now able to directly track your personal information and provide a customized price that they believe YOU should pay.⁸⁷ Some corporations curtail the requirements to provide consumers a chance to opt-out by requiring data or cookie trackers in exchange for the entrance and usage of the actual site. Utilization of modern tracking techniques are employed without requiring

80. See BERNASEK & MONGAN, *supra* note 19, at 60 (explaining that a power shift occurs when producers are able to price goods and services based on *all* that one is able to pay instead of what one is willing to pay).

81. See *id.* at 98 (noting that corporations use data from consumers' search history, purchase ability, and desires to determine which advertisements will most likely trigger the next spend).

82. See *id.* at 108 (highlighting that this customization kills mass markets because everything can now be unique and catered towards each consumer's datapoints without a singular fair price).

83. *Id.* at 32–33.

84. See *id.* at 79 (describing how changing the price of a good or service based on immediate data sources is now possible with immediate data collection and analysis).

85. *Id.*

86. *Id.* at 74.

87. See *id.* at 91 (stating that it is nearly impossible to protect financial and personal information given the speed of technological advances that are geared towards meeting corporation's demands to track and utilize consumer personal data).

access to one's device.⁸⁸ Majority of services and goods today are backed by online corporate contracts that allow computers to obtain a glimpse into one's online blueprint with no clear boundaries.⁸⁹ There is a general lack of self-help solutions for consumers within the legal realm, as current data privacy laws do not provide sufficient protection in new spaces or techniques utilized to collect and exploit one's data.⁹⁰ This phenomenon has one of the most pernicious influence upon consumers' access to adequate data protection.

III. *Privacy is a Recognized Fundamental Right*

The right to privacy has been long established within American jurisprudence.⁹¹ The Supreme Court of the United States first recognized the right to privacy in *Griswold v. Connecticut*⁹² in 1965, where the court held that privacy is an individual's right to be left alone.⁹³ Only two years after *Griswold*, the court in *Katz v. United States*⁹⁴ established that individuals are

88. See Fairfield, *supra* note 66, at 559 (explaining that movements online are tracked through the changes in URL addresses without having to put a direct code on one's computers and warning that corporations gain user approval for these tracking devices by putting information in fine print on their goods or services page.).

89. See *id.* at 560 (noting corporate contracts allowing corporations to utilize this collected data place them in a "hacker realm" where they are enabled to see relevant data without legal bounds).

90. See Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—and How to Change the Game*, BROOKINGS (July 12, 2018) ("This is where we are with data privacy in America today. More and more data about each of us is being generated faster and faster from more and more devices, and we can't keep up. It's a losing game both for individuals and for our legal system.") [perma.cc/PJ8H-NAHE].

91. See *Right to Privacy*, CORNELL LEGAL INFO. INST. (June 2022) (providing the basics of how the right to privacy has been established within the United States) [perma.cc/R4ZA-RCJL].

92. See *Griswold v. Connecticut*, 381 U.S. 479, 484 (1965) (applying the languages of various Amendments, a right of privacy is a constitutional right that should be extended to all individuals).

93. See *id.* at 485 ("[T]he right of privacy which presses for recognition here is a legitimate one.").

94. See *Katz v. United States*, 389 U.S. 347, 350 (1967) (finding that the Fourth Amendment extends further than protecting individual privacy against government intrusions, but also general right to be left alone and have a zone of personal privacy left to themselves against other people).

able to have reasonable zones of privacy, applicable within new spaces.⁹⁵ Although it is not explicitly codified in the United States Constitution or any federal law, courts and the general public have consistently deemed it to be a protected fundamental right that requires utmost protection.⁹⁶ Courts have stated the right to privacy is implicitly contained within the Constitution through combining the First, Third, Fourth, Fifth, and Ninth Amendments, which together creates a zone of personal privacy.⁹⁷ Over time, privacy has been defined to be free of “unwarranted publicity,” which reserves a zone of freedom away from others and may be influenced by factors such as property law and societal understandings.⁹⁸

Since the early 1970s, the emergence of different government agencies and regulatory groups helped navigate privacy in various areas.⁹⁹ The right to privacy has extended to several other facets

95. See *id.* at 361. (Harlan, J., concurring) (establishing a two-pronged test to determine the reasonableness of privacy zones, which balances an individual’s subjective expectation of privacy and society’s reasonable acceptance of the area to be deemed private).

96. See Cameron F. Kerry & John B. Morris, *Framing a Privacy Right: Legislative Findings for Federal Privacy Legislation*, BROOKINGS (Dec. 8, 2020) (exploring the legal and moral history of privacy in America) [perma.cc/YM6R-XK46].

97. See *Privacy*, CORNELL LEGAL INFO. INST. (Jun. 2022) (expressing the long and evolving history behind courts’ establishment of privacy as a recognized fundamental right through utilizing the implications provided through the Constitution) [perma.cc/5Q3D-PT4K]; see also *Griswold v. Connecticut*, 381 U.S. 479, 483–87 (1965) (extrapolating a right to privacy based on protections afforded in the Bill of Rights).

98. See 77 C.J.S. *Right of Privacy and Publicity* § 1 (Mar. 2024) (stating the zone of privacy can include freedom from both person and place); see also Ashley N. Longman, *The Future of Blockchain: As Technology Spreads, It May Warranty More Privacy for Information Stored with Blockchain*, 23 N.C. BANKING INST. 111, 114 (2019) (outlining the Harlan Standard from *Katz* to protect individuals’ zone of privacy rather than places of privacy).

99. See *History of Privacy Timeline*, U. MICH.: INFO. & TECH. SERVS. SAFE COMPUTING (listing several legislations and regulatory materials emerging since the realization of privacy as a human right) [perma.cc/4S5H-UH7A].

of our lives: contraceptives,¹⁰⁰ abortion,¹⁰¹ publicity,¹⁰² personal information, and data.¹⁰³ Internationally and in the United States, privacy is recognized to be a fundamental human right requiring upmost protection because it underpins human dignity and highlights key values of freedom of speech and association.¹⁰⁴

A. Protection of Data Privacy

A sub-sector of privacy at large is data or informational privacy, which is especially essential within the modern digital age where information is readily interchanged and collected.¹⁰⁵ Through *Katz*, courts have recognized individual's data to be a reasonable zone of privacy.¹⁰⁶ It encompasses the protection of data

100. See *Eisenstadt v. Baird*, 405 U.S. 438, 444–46 (1972) (holding the constitutional right to privacy is contained with the individual to make autonomous decisions for themselves).

101. See *Roe v. Wade*, 410 U.S. 113, 158–60 (1973) (stating that the right of privacy derived from the Fourteenth Amendment includes personal liberty); *but see Dobbs v. Jackson Women's Health Org.*, 142 S. Ct. 2228, 2240 (2022) (overturning *Roe v. Wade* and the concept of applying privacy to abortion decisions).

102. RESTATEMENT (SECOND) OF TORTS § 652C cmt. A (AM. BAR ASS'N 2022).

103. See *Right to Privacy*, *supra* note 91 (identifying several of the recognized zones of privacy).

104. See Matthew Rosenquist, *What is Privacy and Why Does it Matter?*, HELP NET SECURITY (July 28, 2020) ("Privacy is a basic right and a necessary protection in the digital age to avoid victimization and manipulation.") [perma.cc/N4FS-AZSP]; see also *What is Privacy?*, PRIVACY INT'L (Oct. 23, 2017) (establishing the notion that privacy creates barriers into unwarranted inferences and is key to negotiate how we protect ourselves and interact with the world and institutions who may wield their power unjustly) [perma.cc/MQN9-XA2C]. See Philip Kushmaro, *Why Data Privacy is a Human Right (And What Businesses Should Do About It)*, FORBES (June 7, 2021 7:10 AM) (identifying access to the internet is even a recognized human right, but upon the internet, everything is magnified with communications and data collection, increasing the need for data privacy) [perma.cc/M9FK-QEQD].

105. See Stephen J. Bigelow, *Data Privacy (Information Privacy)*, TECH TARGET (last updated Aug. 2022) (illustrating data privacy to not be one-dimensional, but rather can evolve and develop as rules, practices, guidelines, and tools interact) [perma.cc/JC6T-UG4M]; see also *About the IAPP*, IAPP ("Information privacy is the right to have some control over how your personal information is collected and used.") [perma.cc/94DC-U4DG].

106. See *Katz*, 389 U.S. at 359 (determining that the Fourth Amendment protects an individual from surveillance under certain circumstances).

“storage, access, retention, immutability and security of sensitive data” and “proper handling personal and confidential data.”¹⁰⁷ Democratic countries around the world have employed Fair Informational Practice (FIP) upon automated data system, outlining a set of foundational standards: no secret personal-data record-keeping system, individuals should be able to find out what records are kept and how it is used, consent for data usage, withdrawal of data mechanisms, and assurance of reliability of data for intended use with reasonable precautions against misuse.¹⁰⁸ The Privacy Act¹⁰⁹ and Fair Credit Reporting Act¹¹⁰ were the initial attempts at guaranteeing data is processed fairly and individuals received notice on how their data is applied.¹¹¹

Data is shaping up to be the new oil with its power to predict human behaviors.¹¹² Utilization of cookies and IP address tracking provide corporations the insights into consumers’ preferences and information.¹¹³ Protecting data privacy is crucial to ensuring corporations are not exploiting consumers.¹¹⁴ Creating a shield with data privacy regulations and laws will curtail businesses from abusing their power and becoming too invasive with the

107. Bigelow, *supra* note 105.

108. Neil M. Richards, *Why Data Privacy Law is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1506 (2015).

109. 5 U.S.C. § 552a (2014).

110. See 15 U.S.C. § 1681 (2023) (defining the purpose of the law as “requir[ing] that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer”).

111. See Richards, *supra* note 108, at 1510 (describing both laws as early attempts to embody fair information practices).

112. See Rosenquist, *supra* note 104 (“Our digital fingerprints are everywhere. They tell a story of where we go, what we do, who we like or dislike, and what we think When that data is aggregated, it can provide tremendously powerful insights about a person or community”).

113. See *How Websites and Apps Collect and Use Your Information*, FED. TRADE COMM’N (Sept. 2023) (advising consumers to partake in safe online practices to protect their data against the multitude of integrated methodologies companies engage in to collect and utilize their data) [perma.cc/6CBV-NFKS].

114. See Rosenquist, *supra* note 104 (stating that as institutions collect more information through consumers’ online activities, they are able to better “pull people into desired behaviors”).

information they retain and utilize.¹¹⁵ While some federal regulations and laws are in place to prevent some abuses of captured datapoints, the majority are insufficient to protect against corporations creating unfair markets that further prejudice consumers.¹¹⁶

Within the international realm, data privacy was declared by the United Nations to be a protected basic human right under the 1948 Universal Declaration of Human Rights (UDHR).¹¹⁷ Within individual countries in the European Union and states within the United States, data privacy as a recognized fundamental right has been codified into statutes and regulations.¹¹⁸

IV. Current Data Privacy Regulation

There are a few general federal regulations in place to protect the collection of data, but not a principal regulation or law that can impact the blockchain space to ensure consumer data privacy is thoroughly protected.¹¹⁹ Currently, a combination of federal and

115. See *id.* (“Protecting privacy is not about hiding information. It is about the ability to be free from *unwanted* influence[.]”) (emphasis added).

116. See *Privacy & Technology*, AM. CIV. LIBERTIES UNION (“Technological innovation has outpaced our privacy protections. As a result, our digital footprint can be tracked by the government and corporations in ways that were once unthinkable.”) [perma.cc/936P-VXFL].

117. See G.A. Res. 217 (III) A, Universal Declaration of Human Rights, at 12 (Dec. 10, 1948) (enshrining the freedom from being subjected to “arbitrary interference with [one’s] privacy”); see also Ryan Moshell, . . . *And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH L. REV. 357, 364–88 (2005) (describing various European nations’ and the United States’ shifts towards implementing data-protection laws after they recognized the importance of regulating the data privacy space).

118. See Rosenquist, *supra* note 104 (learning from past lack of protection in data privacy, more states have implemented data privacy statutes and regulations to be a shield against unjust victimization); see also *Privacy*, *supra* note 97 (describing the United States Supreme Court’s evolving recognition of a fundamental right to privacy); *Which States Have Consumer Data Privacy Laws?*, BLOOMBERG L. (last updated Nov. 23, 2023) (listing the US states that enacted comprehensive data privacy laws) [perma.cc/QN59-BRSL].

119. See Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (and Why It Matters)*, N.Y. TIMES (Sept. 6, 2021) (“The United States doesn’t have a singular law that covers the privacy of all types of data. Instead, it has a mix of laws that go by acronyms like HIPAA, FCRA, FERPA, GLBA, ECPA, COPPA, and VPPA.”) [perma.cc/6QYS-D5YM].

state laws are utilized to govern online data protection.¹²⁰ Federal-level data protection was first initiated by courts' interpretation of the Constitution.¹²¹ However, a comprehensive federal law governing data privacy does not exist.¹²² Insufficient online data protection can be traced to a lack of federal oversight on data collection and usage; any regulations pertaining to data are sectorial. Through time, sectorial federal laws have proliferated, including the Family Educational Rights and Privacy Act¹²³ for student education records privacy; the Privacy Act¹²⁴ for federal agencies' collection and maintenance of personally identifiable data; the Telephone Consumer Protection Act¹²⁵ to allow consumers to opt out of telemarketing calls; the Health Insurance Portability and Accountability Act¹²⁶ for medical data; the Children's Online Privacy Protection Act¹²⁷ for data collection of children, Gramm Leach Bliley Act¹²⁸ for private data in financial institutions, and E-Government Act¹²⁹ for governments to conduct

120. See F. Paul Pittman et al., *Data Protection Laws and Regulations USA 2022-2023*, GLOB. LEGAL GRP. (Aug. 07, 2022) ("In parallel to the federal regime, state-level statutes protect a wide range of privacy rights of individual residents. The protections afforded by state statutes often differ considerably from one state to another") [perma.cc/DQ7S-RTRQ].

121. See *Privacy*, *supra* note 97 (tracing evolving jurisprudence regarding the right to privacy in the US).

122. See *Data Privacy Laws: What You Need to Know in 2023*, OSANO (Dec. 14, 2022) (stating that in the absence of a comprehensive federal law regulating data privacy, states have instituted hundreds of their own data privacy and data security laws that impact the types of rights consumers have and the type of consent required for data collection) [perma.cc/LCW5-SQPK].

123. See 20 U.S.C. § 1232g (2013) (providing guidelines for the protection and release of educational records).

124. See 5 U.S.C. § 552a (2014) (establishing the conditions under which government agencies can store and release information about individuals).

125. See 47 U.S.C. § 227 (2019) (restricting whom could be called using automated telephone technology).

126. See 42 U.S.C. § 1320d-6 (2009) (criminalizing the wrongful disclosure of individually identifiable health information and setting penalties for such violations).

127. See 15 U.S.C. §§ 6501–6506 (2023) (limiting what personal information can be collected about child users of the internet).

128. 15 U.S.C. § 6801 (2011).

129. 44 U.S.C. § 3501 (2002).

tests on new technologies.¹³⁰ Digital footprints are effortless to create, but nearly impossible to expunge.¹³¹ Companies engaged in data activities outside of these sectors are largely left to regulate themselves.¹³²

The United States Federal Trade Commission (FTC), an independent U.S. law enforcement agency created via the Federal Commission Act in 1914,¹³³ attempts to ensure consumers are protected against unfair and deceptive practices through enforcement of privacy and data regulations.¹³⁴ They are the central agency for data privacy across various industry sectors and is primarily responsible for emerging technological advances that affect consumers.¹³⁵ Over the years, the FTC, as enforcers of consumer protection, have provided a general outline of ways data can be collected, used, disclosed, sold, and handled.¹³⁶ The most notable enforcement areas include maintaining reasonable data security measures, producing self-regulatory principles of the industry, requiring adherence to self-published privacy policies for

130. See *Data Privacy Laws: What You Need to Know in 2023*, *supra* note 122 (listing the patchwork of laws that address privacy in the federal government and across the states).

131. See *Internet Privacy Laws Revealed - How Your Personal Information Is Protected Online*, THOMSON REUTERS (“Your PI may be shared in ways you don’t expect or are unaware of. Your information may be at some risk because even the best information security programs are not 100% guaranteed.”) [perma.cc/B9SU-NBDZ].

132. See Klosowski, *supra* note 119 (“The data collected by the vast majority of products people use every day isn’t regulated. Since there are no federal privacy laws regulating many companies, they’re pretty much free to do what they want with the data . . .”).

133. 15 U.S.C. § 41.

134. See Pittman, *supra* note 120 (“The FTC has taken the position that ‘deceptive practices’ include a company’s failure to comply with its published privacy promises and its failure to provide adequate security of personal information, in addition to its use of deceptive advertising or marketing methods.”).

135. See FED. TRADE COMM’N, *PRIVACY & DATA SECURITY 2* (updated 2018) (“The FTC uses a variety of tools to protect consumers’ privacy and personal information. The FTC’s principal tool is to bring enforcement actions to stop law violations and require companies to take affirmative steps to remediate the unlawful behavior.”) [perma.cc/V4J2-3965].

136. 16 C.F.R. § 314 (2002).

accurate privacy and security representations, and ensuring proper collection, process or sharing of consumer information.¹³⁷

The Gramm-Leach-Bliley Act protects personal information collected by banks and financial intuitions.¹³⁸ Under the Gramm-Leach-Bliley Act, “financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – must explain their information-sharing practices to their customers and to safeguard sensitive data.”¹³⁹ The FTC is responsible for all entities that are not under Gramm-Leach-Bliley Act, but who are still engaged in activities financial in nature or incidental to financial activities under Bank Holding Act¹⁴⁰ and under FTC federal jurisdiction.¹⁴¹

With the wide-usage of modern-day technologies, ensuring data privacy across individual’s online activities is increasingly important.¹⁴² The limited protections and overhead regulations within the data privacy space has hindered complete integration of new technologies like blockchain.¹⁴³ With increased technological usage and companies’ entrenchment into the nuance activities of everyday life, data privacy laws are utilized to protect the important information of our generation.¹⁴⁴ Due to the

137. See *Data Privacy Laws: What You Need to Know in 2023*, *supra* note 122 (indicating various other acts that govern different areas of privacy laws such as children’s online privacy protection act, collection of minors’ information, health insurance portability and accounting act, collection of health information, and family education rights and privacy acts).

138. See *id.* (governing personal information collection by banks and financial institutions).

139. 15 U.S.C. § 6801 (2011).

140. 12 U.S.C. § 1843(k) (2010).

141. See Klosowski, *supra* note 119 (describing the FTC’s role in data privacy laws).

142. See Jacky Goh, *Crypto 101: Data Privacy and Security on Cryptocurrency Platforms*, EMERGING TECH (Feb. 28, 2022, 5:00 AM) (highlighting people’s higher expectation for increased security measures to protect personal information online) [perma.cc/WP23-XAEX].

143. See Rita Esposito, *Lack of Federal Data Privacy Legislation Leaves US Agencies to Provide Guidance*, THOMSON REUTERS (July 15, 2022) (“Navigating the choppy waters of US federal data privacy policy can be difficult, primarily because a lack of policy development on the federal level has led to state — rather than federal — legislatures taking the lead on recent consumer privacy laws.”) [perma.cc/5FG2-8Q4A].

144. See Kerry, *supra* note 90 (stating despite the existence of regulations and laws in place to curtail data collection by corporations, companies like Facebook

ambiguity of how companies collecting data can be regulated, they are largely left to regulate themselves in the day-to-day data activities.

A. State Data Privacy Laws and Regulations

Data regulation oversight of private entities is predominantly vested within the states.¹⁴⁵ At the time of writing this Note, only thirteen states have successfully passed comprehensive data privacy laws with only around four currently effective.¹⁴⁶ The most robust data protection is California’s Consumer Privacy Rights Act (CPRA),¹⁴⁷ which is viewed as the industry standard for strong and effective data privacy regulations.¹⁴⁸

There are various states that have utilized CRPA as a model to shape their own state regulations. As of the beginning of 2023, many states have either engaged in changing their data privacy laws to be more vigorous or is shaping entirely new legislation to encompass the changing data sphere.

Data privacy protections are enacted at the state level where states have autonomy to control as much or as little as they seem fit.¹⁴⁹ Therefore, there exists a wide range of data privacy

are still able to collect an abundance of consumer data, which have caught public attention).

145. See Klosowski, *supra* note 119 (existing disparate state data regulations result in consumers’ data to be collected without any oversight in some states).

146. See F. Paul Pittman, *US Data Privacy Guide*, WHITE & CASE (Dec. 26, 2023) (listing California, Virginia, Colorado, Connecticut, Utah, Iowa, Indiana, Tennessee, Texas, Florida, Montana, Oregon, and Delaware as stated that passed the laws, but only California, Colorado, Connecticut, and Virginia to be in effect) [perma.cc/R4GC-NPCP].

147. CAL. CIV. CODE § 1798.100 (2023).

148. See Klosowski *supra* note 119 (“The experts we spoke to referred to California’s privacy protections as the strongest in the US, since the regulations include a limited “private right of action”—the ability to sue a company—against certain types of data breaches.”).

149. See *Data Privacy Laws: What You Need to Know in 2023*, *supra* note 122 (asserting that states have taken it upon themselves to initiate protection measures, instead of waiting for the federal government to produce a singular data privacy law).

protections as one moves from state to state.¹⁵⁰ As a sampling of some data privacy state laws in place, this Note will discuss the two most robust states: California and Virginia.¹⁵¹

California's CPRA has been deemed to be the most comprehensive and consumer-friendly data privacy regulation.¹⁵² CPRA was first introduced in 2018 and has been amended over the years, with the latest update created in January of 2023.¹⁵³ Since the CPRA is a state law, it only protects California-based residents.¹⁵⁴ It provides consumers with more autonomy to control their data collection when interacting with online sites and provides businesses with guidance and rules on how to implement the regulations.¹⁵⁵ Key elements include consumers' rights to mandatory user opt-outs, privacy notices, ability to correct incorrect personal information, limit the usage and disclosure of their sensitive information, increased fines for breaches of specific categories of data, and use restrictions on certain data.¹⁵⁶

Virginia was the second state to pass a robust set of privacy laws in March 2021, enacted in January 2023, called Virginia's Consumer Data Protection Act (CDPA).¹⁵⁷ Similar to California's data privacy laws, Virginia enacted CDPA to ensure businesses are handling consumer data properly and applies to Virginian residents or those who conduct business within the state.¹⁵⁸ Its key elements include allowing consumers to opt out of data processing,

150. *See id.* ("The U.S. has hundreds of sectoral data privacy and data security laws among its states.").

151. *Id.*

152. *See id.* (suggesting California was the state that started the domino effect of implementing stronger data privacy laws for its residents at the state level after the federal government failed to implement a comprehensive one).

153. *California Consumer Privacy Act (CCPA)*, STATE CAL. DEPT. JUST. OFF. ATTY GEN. (Jan. 20, 2023) [perma.cc/R4X9-3F9K].

154. *See id.* (defining a California resident as either a natural person residing in California even if the person is temporarily outside of the state).

155. *Id.*

156. *Meet the California Privacy Protection Agency (CPPA)*, OSANO (July 27, 2022) [perma.cc/4MUQ-M8TR].

157. *See Data Privacy Laws: What You Need to Know in 2023*, *supra* note 122 ("It grants Virginia consumers certain rights over their data and requires companies covered by the law to comply with rules on the data they collect, how it's treated and protected, and with whom it's shared.").

158. *Id.*

providing clear privacy notices, disclosing if data will be sold, and how sensitive data is to be processed.¹⁵⁹

Other notable states that have either passed or enacted data privacy laws include Colorado, Utah, and Connecticut.¹⁶⁰ Each state has drafted a different version to best fit their state's needs and what they deem to be most important to protect. The different regulations amongst the states can impact consumers in various jurisdictions, but with the nature of business today, it is difficult to not follow the most robust data privacy laws as a corporation because those goods and services will eventually reach those states.¹⁶¹

B. Global Data Privacy Laws and Regulations

There have been global concerns surrounding data protection with over 71% of countries enacting data-related legislation and an additional 9% of countries have initiated drafting legislation.¹⁶²

On the international scale, Europe's General Data Protection Regulation (GDPR)¹⁶³ has set a strong standard for how data privacy regulations should be structured.¹⁶⁴ Deemed to be the "toughest" privacy law in the world, it imposes its obligations on corporations within the European Union and corporations who conduct any business with EU citizens, creating a wide-arching

159. *Id.*

160. *See id.* (recognizing each of these states as the first states in the country to have implemented strong data privacy security measures for corporations who interact with their associated residents and have positively impacted other states to follow suit).

161. *See Data Privacy Laws by State: Comparison Charts*, BLOOMBERG L. (Feb. 2, 2022) (providing comparison charts of protections afforded by states with the top sufficient data privacy laws in place) [perma.cc/S59Z-P85F].

162. *See Data Protection and Privacy Legislation Worldwide*, U.N. CONF. ON TRADE & DEV. ("As more and more social and economic activities have place online, the importance of privacy and data protection is increasingly recognized. Of equal concern is the collection, use and sharing of personal information to third parties without notice or consent of consumers.") [perma.cc/3PTZ-G5BT].

163. Commission Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

164. *See generally Data Privacy Laws: What You Need to Know in 2023*, *supra* note 122.

impact worldwide.¹⁶⁵ It encompasses protection and reach over personal data, data processing, data subject, data controller, and data processor.¹⁶⁶ From required consent of data collections to how data is transferred and stored, the GDPR imposes high levels of penalties up to 20 million euros or 4% of the company's revenue if a company defaults.¹⁶⁷ While thoroughly robust, GDPR's regulations are still in question when it comes to blockchain application since it is geared towards centralized institutions.¹⁶⁸

The People's Republic of China (PRC) published some of the first national-level laws, addressing data privacy protection in 2017 with continual updates to withstand new data collection techniques.¹⁶⁹ Data protection spans three large categories: Personal Information Protection Law (PIPL), Cybersecurity Law (CSL), and Data Security Law (DSL).¹⁷⁰ Within the past five years, the PRC also released various federal-level guidances and standardization materials to streamline data regulation across

165. See Ben Woford, *What is GDPR, The EU's New Data Protection Law?*, GDPR.EU (establishing a strong focus and goal on protecting the rights of their citizens against unwarranted usage of data has set the standard for data privacy laws across the globe) [perma.cc/4UCF-4KUN].

166. *Id.*

167. See *The European Union (EU) General Data Protection Regulation (GDPR)*, UNIV. PITT. HUM. RSCH. PROT. OFF. (last updated Feb. 13, 2023) (listing several helpful answers to common questions that will guide companies conducting businesses in the EU to be compliant with strict EU data privacy rules) [perma.cc/57WT-N932].

168. See *GDPR & Blockchain: At the Intersection of Data Privacy and Technology*, BDP (focusing on GDPR's requirement for entities to instill a "right to be forgotten" implementation, which is at odds with blockchain because all records are forever kept on the chain) [perma.cc/9XBT-T6DR].

169. See *Data Protection of the World*, DLA PIPER (last updated Jan. 03, 2023) [perma.cc/DP6D-JK83].

On June 1, 2017, the CSL came into effect and became the first national-level law to address cybersecurity and data privacy protection. Draft Amendments to the CSL were issued on September 12, 2022, proposing enhanced liabilities for violating obligations of general network operation security, security protection of critical information infrastructure, network information security and personal information protection.

170. See *id.* ("There is not a single comprehensive data protection law in the People's Republic of China (PRC). Instead, rules relating to personal information protection and data security are part of a complex framework and are found across various laws and regulations.").

various industries.¹⁷¹ Violators face not only civil penalties but criminal ones as well.¹⁷² In terms of blockchain, China's Ministry of Public Security spearheaded RealDID in 2023 to allow citizens to utilize blockchain technology without linking their personal information.¹⁷³ This is the first national-level usage of blockchain technology for government identity purposes.¹⁷⁴

The GDPR and PCR case studies reflect implementation of legislation at the federal level to enable cohesive regulation of data privacy. These are great starting points for the United States to learn and adapt in creating more inclusive data protection regulations.

V. *Understanding Blockchain Technology, Benefits, Uses, and Data Retention*

Blockchain technology first arose within the mainstream sphere in 2008 with Satoshi Nakamoto's introduction of Bitcoin and its integration of blockchain technology.¹⁷⁵ The blockchain space is a continuous and quickly evolving technological paradigm.¹⁷⁶ Blockchain technology has risen in popularity through its multi-functional use applications, which enables it to

171. *Id.*

172. See Dora Luo & Yanchen Wang, *China – Data Protection Overview*, DATA GUIDANCE (Oct. 2023) (illustrating various penalties the People's Republic of China implemented on companies since these regulations have been implemented) [perma.cc/D2YU-U5UX].

173. See Sam Reynolds, *China to Verify Citizens' Identifies with New Blockchain-Based Platform*, COINBASE (Dec. 12, 2023) ("The RealDID service launch will enable users to register and log in to websites anonymously using DID addresses and private keys, ensuring that business data and transactions remain disconnected from personal information.") [perma.cc/HE3Q-Q7MW].

174. *Id.*

175. See Ravikiran A S, *What is Blockchain Technology? How Does Blockchain Work?*, SIMPLILEARN (last updated Jan. 29, 2023) (highlighting Satoshi Nakamoto's important role in increasing blockchain's popularity through using the hashcash-like method, which is crucial to the Bitcoin network) [perma.cc/TK5R-XP7U].

176. See *Cryptos On The Rise 2022*, THOMSON REUTERS (bridging the analysis on how blockchains are increasingly growing, which means regulatory agencies have to keep up or be left behind in protecting necessary rights) [perma.cc/M5AR-G89U].

be utilized in a majority of industries today.¹⁷⁷ Keep in mind that Bitcoin and blockchain are not synonymous; Bitcoin is a form of cryptocurrency built *with* blockchain technology.¹⁷⁸

A. *Building Blocks of Blockchain*

Blockchain is a “form of record-keeping” employing decentralized distributed ledger technology (DLT) amongst a network of computer nodes with no central authority, allowing for secure and immutable records.¹⁷⁹ Blocks of data are created with new movements within the software or platform, whether it is the initial input of information, a transfer, additional supporting information, or change of any form.¹⁸⁰ Every change creates a new

177. See David Rodeck & Benjamin Curry, *What is Blockchain?*, FORBES: ADVISOR (last updated Apr. 28, 2022) (“While cryptocurrency is the most popular use for blockchain presently, the technology offers the potential to serve a very wide range of applications.”) [perma.cc/VBC8-34GK]; see also Sam Daley, *Blockchain. What is Blockchain Technology? How Does it Work?*, BUILT IN (last updated Sep. 1, 2022) (utilizing blockchain technology includes food supply chains, healthcare, gaming, real estate, finance, creative spaces) [perma.cc/2EP6-GYUU]; see also *Types of Blockchain*, GEEKS FOR GEEKS (last updated Aug. 2, 2022) (listing potential real world problems blockchains can solve such as voting management system, supply chain management, real estate projects, NFT markets, avoiding copyright and original content creation, and more) [perma.cc/3NGJ-FDKA].

178. See Ankush Jain & Dheeraj Vaidya, *Bitcoin vs Blockchain*, WALLSTREETMOJO (2024) (comparing the major differences between Bitcoin and blockchains including each respective use, main aim, trade, scope, strategy and status, with the main takeaway that blockchain is a technological advancement utilized as a foundation of Bitcoin’s usage).

179. See Adam Sulkowski, *Blockchain, Business Supply Chains, Sustainability and Law: The Future of Governance, Legal Frameworks, and Lawyers?*, 43 DEL. J. CORP. L. 303, 308 (2010) (simplifying the explanation of blockchains into a series of blocks and chains with data recorded throughout and the ability for the entire blockchain to work through self-executing smart contracts to continuously keep the blockchain running during changes); see also Rodeck & Curry, *supra* note 177 (stating that blockchain’s uniqueness comes from its totally decentralized structure where as soon as a block is added to the chain, all underlying transactions are recorded on the ledger and the block is now stored across nodes of the network).

180. See Daley, *supra* note 177 (explaining every chain has multiple blocks with each block consisting of the data, nonce, and hash where once a block has been created with the change in data, the nonce automatically creates the cryptographic hash which solidifies the data into the chain forever).

block, which is then added to the overall existing blocks already created to be “chained” together cryptographically to persist the sequence of transactions.¹⁸¹ As soon as a block is created and added to the existing chain, all nodes across the network will update to reflect the new chain.¹⁸² The use of a distributed ledger allows all information to be transmitted electronically and automatically recorded via a public ledger.¹⁸³ Every node, computer in the system, has access or view to each transaction, which makes it almost impossible for individuals to copy assets or engage in fraudulent transactions.¹⁸⁴ A single actor cannot enter into the system to change, duplicate or lie about prior transactions as each movement is captured in a block indefinitely.¹⁸⁵

The three indispensable elements of blockchain include the distributed ledger technology, immutable records, and smart contracts.¹⁸⁶ A distributed ledger allows for all users to have access and a copy to the data without duplication of transactions.¹⁸⁷ All records, once on the blockchain cannot be repudiated, which means corrections can be added with subsequent blocks.¹⁸⁸ The

181. See CAMPBELL R. HARVEY ET AL., *DEFI AND THE FUTURE OF FINANCE* 18 (John Wiley & Sons, Inc., 2021) (providing a basis framework of blockchain technology).

182. See Rodeck & Curry, *supra* note 177 (stating that new blocks are essential to why blockchains are very secure because of the necessity for majority of the nodes to verify and confirm the legitimacy of the new data prior to the block being added to the new chain).

183. See *id.* (recording transactions on a public ledger is similar to a bank’s balance sheet where each transaction is readily recorded, but note it is on a decentralized and distributed public ledger).

184. See *id.* (“Blockchain is the innovative database technology that’s at the heart of nearly all cryptocurrencies. By distributing identical copies of a database across an entire network, blockchain makes it very difficult to hack or cheat the system.”).

185. *Id.*

186. See *What is Blockchain Technology?*, IBM (making clear the combination of all three elements enable blockchains to be successfully and appealing to those who wish for better ways to navigate data retention) [perma.cc/GEU2-5FSD].

187. See *id.* (“All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that’s typical of traditional business networks.”).

188. See *id.* (“No participant can change or tamper with a transaction after it’s been recorded to the shared ledger. If a transaction record includes an error,

foundation of parties utilizing blockchains stem from smart contracts stored on the blockchain that self-execute when predetermined conditions are met.¹⁸⁹

Blockchain encompasses three main technologies to ensure a high-level of security: cryptographic hashes, asymmetric encryption, and digital signatures to enable secure record-keeping.¹⁹⁰ Hashing requires application of an algorithm on the input of information to produce a seemingly randomized output called the “hash.”¹⁹¹ A hash is almost computationally impossible to retrieve the original value due to its one-way function.¹⁹² Information contained within each block is hashed to obscure the original datapoint to protect against manipulation.¹⁹³ Due to the autonomous accessibility, transferability, decentralization, and speed, actual blocks on the chain can only be added to the overall blockchain if the majority of the nodes confirm the data movement to create a single-source of truth.¹⁹⁴ “Truth” of the information is

a new transaction must be added to reverse the error, and both transactions are then visible.”).

189. See Morgan N. Temte, *Blockchain Challenges Traditional Contract Law: Just How Smart Are Smart Contracts?*, 19 WYO. L. REV. 87, 94–96 (2019) (“Codifiers write the terms of a smart contract in blockchain computer code rather than in English or another traditional language. No individual or program can override or change the ledger. Once the parties meet conditions as stated in the ledger, the contract executes automatically without interjection from a third party.”).

190. See Paul Belonick, *Transparency is the New Privacy: Blockchain’s Challenge for the Fourth Amendment*, 23 STAN. TECH. L. REV. 114, 125 (2020) (combining these three technologies allows for exchanges between strangers to be secured and impossible to tamper with, increasing people’s confidence in blockchain technologies).

191. See Andrew Loo, *Hash Function*, CORP. FIN. INST. (defining hashing as an algorithm that converts any messages or values into a hash value set by the system) [perma.cc/M66G-VPR2].

192. See *Explained: What is Hashing in Blockchain?*, BYBIT (hashing safeguards data through deterministic outputs, preimage resistance and collision resistance meaning while inputs produce hash to verify data consistency but enables to determine original input from the hash) [perma.cc/NNF4-W7HP].

193. See Daley, *supra* note 177 (“The math problems involving matching nonces and hashes is almost impossible to change later — the record of previous actions on the blockchain is highly accurate and secure from manipulation.”).

194. See *id.* (noting all changes to the blockchain are documented and added to all nodes across the network allows the blockchain to be the integrity of the truth and transparency).

verified through consensus mechanisms.¹⁹⁵ A consensus mechanism is “a program used in blockchain systems to achieve distributed agreement about the ledger’s state.”¹⁹⁶ There are various forms of consensus mechanisms deployed across blockchains: Proof of Work (PoW)¹⁹⁷, Proof of Stake (PoS),¹⁹⁸ Proof of Capacity (PoC),¹⁹⁹ Proof of Activity (PoA),²⁰⁰ Proof of Burn (PoB),²⁰¹ and Proof of History (PoH)^{202,203} However, as with all technology, it is only as good and truthful as the people utilizing it and the data contained.²⁰⁴ To simplify the blockchain process, these are the general steps:

195. See HARVEY, *supra* note 181 (“Blockchains are possible because of *consensus protocols* – sets of rules that determine what kinds of blocks can become part of the chain and thus the ‘truth.’”).

196. Jake Frankenfield, *What Are Consensus Mechanisms in Blockchain and Cryptocurrency?*, INVESTOPEDIA (Feb. 17, 2023) [perma.cc/8FRQ-FQWW].

197. See *id.* (“The proof of work (PoW) is a common consensus algorithm used by the most popular cryptocurrency networks like Bitcoin and Litecoin. It requires a participant node to prove that the work done and submitted by them qualifies them to receive the right to add new transactions to the blockchain.”).

198. See *id.* (“The proof of stake (PoS) is another common consensus algorithm that evolved as a low-cost, low-energy consuming alternative to the PoW algorithm. It involves allocating responsibility in maintaining the public ledger to a participant node in proportion to the number of virtual currency tokens held.”).

199. See *id.* (“Proof of Capacity (PoC) which allow sharing of memory space of the contributing nodes on the blockchain network. The more memory or hard disk space a node has, the more rights it is granted for maintaining the public ledger.”).

200. See *id.* (“Proof of Activity (PoA), used on the Decred blockchain, is a hybrid that makes use of aspects of both PoW and PoS.”).

201. See *id.* (“Proof of Burn (PoB) requires transactors to send small amounts of cryptocurrency to inaccessible wallet addresses, in effect “burning” them out of existence.”).

202. See *id.* (“Proof of History (PoH) was developed by the Solana Project. It is similar to Proof of Elapsed Time (PoET), which encodes the passage of time itself cryptographically to achieve consensus without expending many resources.”).

203. See *id.*

Consensus mechanisms verify data inputs and outputs, which translates to automatically auditing the digital transactions that are common today—without human oversight or intervention. They create an environment where you don’t need to trust that the other party in a transaction is honest because they ensure the information is unalterable and secure.

204. See *What is Blockchain?*, MCKINSEY & CO. (Dec. 5, 2022) (“A motivated group of hackers could leverage blockchain’s algorithm to their advantage by

1. A transaction is initiated, which is communicated to the network of computers, called nodes, within the system. The information is automatically hashed using a secure hashing algorithm.
2. The network of nodes validates the transaction through the blockchain's form of consensus mechanism.
3. The validation creates a single source of truth leading to the creation of a new block containing all this information, which is then attached to the existing blockchain.
4. The transaction is complete and now immutable.²⁰⁵

Blockchain technology boasts of greater efficiency, security, opacity, and trust.²⁰⁶ This is largely due to blockchain's decentralization, which makes it more difficult to falsify transactions or hack into a system consisting of a plethora of validators.²⁰⁷

B. Data Retention and Traceability on Blockchains

The appeal of blockchain technology is having a readily available ledger with all single-truth datapoints collected since the beginning of its creation.²⁰⁸ Data collected, whether it is the actual datapoints involved in the transaction itself or a hash is stored

taking control of more than half of the nodes on the network. With this simple majority, the hackers have consensus and thus the power to verify fraudulent transactions.”) [perma.cc/VL3J-BSV9].

205. See Scott Likens, *Making Sense of Bitcoin, Cryptocurrency and Blockchain*, PWC (simplifying blockchain's process into a six-step diagram to highlight blockchain's potential applications) [perma.cc/4EA8-FWG7].

206. See *Benefits of Blockchain*, *supra* note 10 (addressing problems in traditional record-keeping, such as vulnerability to fraud, slow speed resulting from increasing transaction volumes, and limited transparency).

207. See *Friel v. Dapper Labs, Inc.*, 657 F. Supp. 3d 422, 427–28 (S.D.N.Y. 2023) (“To reach consensus, embedded in each blockchain platform is a software protocol, or consensus mechanism, which provides governance standards over how information is added to the blockchain.”).

208. See Adam Hayes, *Blockchain Facts: What is It, How It Works, and How It Can Be Used*, INVESTOPEDIA (last updated Sept. 27, 2022) (“For all of its complexity, blockchain's potential as a decentralized form of record-keeping is almost without limit. From greater user privacy and heightened security to lower processing fees and fewer errors, blockchain technology may very well see applications beyond those outlined above.”) [perma.cc/WB95-W7BL].

indefinitely on the chain.²⁰⁹ The traceability of this data also means activity and information on blockchains are not as secure as individuals are led to believe.²¹⁰

A core concept of every blockchain activity involves the difference between anonymity and pseudonymity.²¹¹ Almost all public blockchain activities are said to be conducted anonymously, meaning the individual or entity is able to “operate in a way that makes them unidentifiable.”²¹² On the surface, this seems to be beneficial to users who may be able to relax concerns over data traceability because the only readily available information is the public blockchain address that conducted the transaction.²¹³ However, this is hardly the reality. All blockchain activities adopt a pseudonymous identity, meaning one is “operating in a way in which they can be identified, but their identification shields who they actually are.”²¹⁴ In essence, blockchain activities, while difficult to trace due to the innate encryptions and hashing, *are* traceable with the right analytics and tools.²¹⁵ Transparency within public ledgers have become a double-edge sword that allows trained individuals or entities to directly pinpoint activities

209. *See id.* (contributing to blockchain’s popularity is its ability to be a secure and immutable ledger).

210. *See* Diego Geroni, *A Comprehensive Guide on Blockchain Traceability*, 101 BLOCKCHAIN (Sept. 7, 2021) (“The use of public, private, and hybrid blockchain could introduce traceability, transparency, and accountability in the movement of assets.”) [perma.cc/YZP9-AGWH].

211. *See Anonymity vs. Pseudonymity in Crypto*, CRYPTOPEDIA (last updated May 17, 2021) (“Many in the crypto community employ some level of anonymity or pseudonymity for security and privacy purposes or as a means of working toward self-sovereignty. Anonymity and pseudonymity provide different, but equally important, protections.”) [perma.cc/J77A-PGJA].

212. *Id.*

213. *See* Shah, *supra* note 16 (reiterating that while pseudonymization can better protect identifications, it is not a path away from complying with necessary regulations).

214. *See* GDPR, *supra* note 163, at art. 4 (“[T]he processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is . . . not attributed to an identified or identifiable natural person.”).

215. *See Is Bitcoin Traceable?*, CHAINALYSIS (Apr. 11, 2022) (taking advantage of collected datapoints from blockchain activities, Chainalysis is able to analyze activities and successfully track criminal or suspicious activities) [perma.cc/FP6L-XDAY].

associated with specific encryption keys.²¹⁶ Governments and entities have continuously utilized these methods to halt suspicious activities or gain insight into their users.²¹⁷

Despite blockchain arising under the notion of privatization and championing for greater security, consumers' information are still collected at an exponential rate compared to traditional regulation-protected sectors.²¹⁸ Although the foundational appeal includes its public but safe ledgers, the increased popularity of blockchain also breeds increased opportunities for abuse by hackers and scammers who set up scams that not only steal individual's money but also their personal information.²¹⁹ Some protections currently in place, including know-your-customer (KYC) checks on users, hinge upon preventing child trafficking and integration with major criminal networks.²²⁰ However, KYC methods, inherent security holes within blockchains, and data clustering, allow for users' real identities and related information to be discovered, almost defeating the initial purpose of blockchain.²²¹ Blockchain data is even more entrenched in

216. See Christian Vos, *Are Bitcoin Transactions Anonymous and Traceable?*, COIN TEL. (Sept. 3, 2022) ("When trading from Bitcoin wallets whose identity is not known, transactions can be traced quickly, but it can take time to find out the identity.") [perma.cc/JQ7Z-CHYL].

217. See Dani Haston, *Cryptoasset Realization: How Cryptocurrencies Are Frozen, Seized, and Forfeited*, CHAINALYSIS (Apr. 29, 2022) (addressing suspicious activity within a blockchain is necessary for government agencies to capture any bad actors) [perma.cc/H2X2-X5Y5].

218. See Anna Baydakova, *How Binance, Coinbase and 22 Other Crypto Exchanges Handle Your Data*, COINDESK (Jan. 27, 2022 9:11 AM) (noting all types of personal data that are being collected by blockchains due to ease of use and trust within the platforms, such as bank account information, personal identifications, tax IDs, and more) [perma.cc/V2CX-4NVG].

219. See Goh, *supra* note 142 (stating that over 7,000 people lost more than \$80 million to crypto-based scams, which is a 1100% increase from previous years).

220. See *id.* ("All major crypto services these days are subject to laws and regulations obliging them to perform know-your-customer (KYC) checks on any new client.").

221. See Electric Coin Company, *Linda Xie on Bitcoin Transparency*, YOUTUBE (Sept. 6, 2018) (working with law enforcement on compliance investigations through tracing blockchain transactions allowed Linda Xie to understand how funds move through the blockchain and realize blockchains are not anonymous as techniques like clustering for pattern recognition are easily utilized to trace movements) [perma.cc/VY7L-ZF8V].

collecting crucial personal data, such as gaining insight into past trade activities, cryptocurrency addresses used to deposit or withdraw funds and other related activities.²²² A lot of information can be revealed through free online wallet transactions sites or past court cases where addresses are revealed for larger schemes.²²³ Since data is connected through chains, exposing one block along the chain can reveal all transactions related to a specific wallet or address, which could paint a clearer picture of one's financial situation or preferences.²²⁴

Most blockchain platforms also operate under traditional business models to retain and attract more users, which means purchasing third-party data through outside data brokers.²²⁵ Some platforms are required to partner with third-party services to aid users in completing the transactions offered, such as in a payment process, meaning the blockchain data is now shared with business partners to ensure a seamless transaction.²²⁶ Ultimately, data living within the blockchain space usually have a real-world match or correspondence.²²⁷ Since most blockchain networks will not disclose or many not even know the purpose or means of how their data is processed, where it will go next, or tracked, it is difficult to apply existing regulations onto this space.²²⁸

222. See Baydakova, *supra* note 218 (“Platforms also routinely gather technical information about the devices users are logging in from, including operating systems, browser details, IP addresses, and the location and time zone settings of computers and phones their clients use to trade.”).

223. See *id.* (indicating the average person can start predicting trends and cluster data to see where they fall within the transactions).

224. See *The Beginning of a New Era in Technology: Blockchain Traceability*, VISIOTT TRACEABILITY SOL. (explaining how to sterilize a product and trace its journey through a consumer lifecycle) [perma.cc/59H6-RMGW].

225. See Baydakova, *supra* note 218 (“This might include companies affiliated with the platform via common owners; third-party providers of identity verification and other technology; banks; government organizations; social networks and other sources.”).

226. See *id.* (maintaining a cryptocurrency platform requires a substantial number of moving pieces to keep the site running and those additional partners are, for the most part, not decentralized and collect data in their own fashion, increasing risk).

227. See Hayes, *supra* note 208 (existing blockchain data has a one to one match with a real-world data point, whether it is the an identity, product, action, or indirect movement of information).

228. See Shah, *supra* note 16 (pointing out that even if blockchains do understand how partners are utilizing and processing their data, it does not

C. Blockchain Usages

Through usage of blockchains, people have greater ease of access to be interconnected with those around the world with a similar purpose or need.²²⁹ The most common uses of blockchains have been in fields of decentralized finance (DeFi), including cryptocurrency and banking, ensuring wider access of social welfare outreach, advancement of technological methodologies, and new record-keeping systems used in domains such as the scientific field.²³⁰

DeFi is an ecosystem of finance systems and services built with blockchain technology.²³¹ Traditional centralized finance involves third parties, such as banks, to facilitate financial transactions between parties.²³² DeFi allows these same transactions without the need for third parties or centralized institutions, which reduces transaction times and costs while increasing access to financial services.²³³ DeFi has emerged as a crucial technological advancement, especially within the cryptocurrency space.²³⁴ Cryptocurrencies are decentralized digital

sufficiently apply the decentralized nature of keeping data safe for the entirety of the data's life cycle).

229. See Shruti Kaushik, *How Blockchain is Connecting Humans*, FXEMPIRE (updated Nov. 27, 2018) (integrating blockchain's intrinsic technology and trust systems has allowed humans to connect in transformed ways through changing ways social interactions occur such as exclusive control over their content and the removal of middlemen) [perma.cc/3RV2-N7SW].

230. See Sam Daley, *35 Blockchain Applications and Real-World Use Cases*, BUILTIN (last updated Nov. 27, 2023) ("Blockchain is especially popular in finance for the money and time it can save financial companies of all sizes. By eliminating bureaucratic red tape, making ledger systems real-time and reducing third-party fees, blockchain can save the largest banks lots of money.") [perma.cc/X8A9-CQ7C].

231. See Rakesh Sharma, *What is Decentralized Finance (DeFi) and How Does it Work?*, INVESTOPEDIA (last updated Sep. 21, 2022) ("Decentralized finance uses the blockchain technology that cryptocurrencies use.") [perma.cc/7RMF-H7QV].

232. See *id.* (facilitating transactions usually involve a centralized network to clear the initiated transaction and another to accept the transaction).

233. See *id.* ("Decentralized finance eliminates the need for a centralized finance model by enabling anyone to use financial services anywhere regardless of who or where they are. DeFi applications give users more control over their money through personal wallets and trading services that cater to individuals.").

234. See Jackson Wood, *Understanding DeFi and Its Importance in the Crypto Economy*, COINDESK (Nov. 27, 2023) (illustrating defi's ease of adapting to various

assets utilizing open-source blockchains and technologies to allow individuals or entities to buy, sell or trade amongst each other on a publicly recorded ledger.²³⁵ There are several appeals to substituting fiat currencies with cryptocurrencies: heightened security, low entry barriers to create ease of accessibility and availability, public ledger of transactions, divisibility, durable, fungible, and more.²³⁶ Since Bitcoin's rise to fame, many other cryptocurrencies have arisen for various needs, goals, concerns, and values.²³⁷ As of 2023, there has been over 21,000 cryptocurrencies created across over 1,000 different blockchains, not solely for currency use but also for causes that span ending poverty in third-world countries to increasing accessibility to banking.²³⁸ Its increased popularity over the past decade has motivated the emergence of new platform technologies to support new coins.²³⁹ The most popular amongst these are Bitcoin,

financial uses such as the lending and borrowing space where blockchain's technology can drastically help increase services and products available) [perma.cc/R9LF-EGKE].

235. See *What is Cryptocurrency?*, COINBASE (listing familiar cryptocurrencies such as Bitcoin, Ethereum, Litecoin to showcase the increasingly popular usage of digital assets since Bitcoin's launch in 2008) [perma.cc/D344-CNHC]; see also Andy Rosen, *Cryptocurrency Basics: A Guide for Beginners*, NERD WALLET (last updated Feb. 14, 2023) (utilizing assets without direct monetary intervention from the government or banks, unlike traditional fiat which are usually heavily controlled by national governments, is cryptocurrencies' main appeal) [perma.cc/P2VG-F7YG].

236. See Mark Leon Goldberg, *Cryptocurrency Isn't All Bad*, FOREIGN POL'Y (June 22, 2021) ("Of great significance to the global development community, many of these new-generation DeFi platforms are being built specifically for users in the developing world who have traditionally been denied low-cost financial services or have been excluded from these services entirely.") [perma.cc/8UAD-N2UK].

237. See Daley, *supra* note 177 (stating cryptocurrencies' market cap has reached over \$1 trillion and is rising exponentially to meet increasing demands of its application).

238. See Coryanne Hicks, *Different Types of Cryptocurrencies*, FORBES ADVISOR (last updated Dec. 7, 2022) (capitalizing around \$850 billions of the market, various types of crypto represent the vast array of technological, financial, economics, and innovative advances catered towards consumers' desires) [perma.cc/AV5X-BCJC].

239. See Goldberg, *supra* note 236 ("The demonstrated potential of blockchain combined with the limited utility of Bitcoin and its destructive environmental costs gave rise to a new generation of blockchain technologies. Rather than just

Ethereum, and Tether.²⁴⁰ As they continue to garner attention, adoption rates will also increase.²⁴¹ The combination of these new coins and platforms allows crypto to readily adapt to modern needs and to be utilized in almost every aspect of our lives from purchasing goods and services to incentivizing social change.²⁴²

The appeal of blockchains and this new online space lies in its seemingly more accessible features.²⁴³ A strong focus behind DeFi is allowing lower income individuals, who traditionally have been denied financial services, a leveraged economic playing field.²⁴⁴ The major reason for around 20% of Americans being unbanked is due their inability to meet minimum balance requirements and ease of access to bank branches.²⁴⁵ DeFi has huge potential to assist in decreasing the 1.7 billion “unbanked” individuals around the world who lack access to traditional modern financial

sending and receiving a cryptocurrency, newer iterations of blockchain technology can support applications layered on top of it.”).

240. See Nicholas Rossolillo, *Types of Cryptocurrency*, MOTLEY FOOL (last updated June 28, 2022 5:51 PM) (listing and providing background on the top five most popular cryptocurrencies) [perma.cc/7SXZ-H99K].

241. See Keegan Francis, *Crypto Mass Adoption: A Matter of When, Not If*, NASDAQ (Jan. 24, 2022 10:20AM) (implying adoption of cryptocurrencies is inevitable and a matter of when the timing is) [perma.cc/AZ5B-QKL2].

242. See Jake Frankenfield, *Cryptocurrency Explained with Pros and Cons for Investment*, INVESTOPEDIA (last updated Feb. 04, 2023) (reiterating crypto provides the much-needed equality of opportunity regardless of demographic, economic class or geographic location) [perma.cc/RAE4-UWEM].

243. See Hayes, *supra* note 208 (describing how blockchains are the newly coveted form of data ledgers due to its decentralized, transparent, and secure features which may be the future of how data can be recorded without worry about immutability).

244. See Goldberg, *supra* note 236 (explaining many cryptocurrencies have been utilized in underdeveloped nations to incentive economic growth and financial education, which have been easier to implement due to the low transaction costs and easier access to the capital); see also Weng Cheong, *Here Are All the Ways Bitcoin Could Help Address Income Inequality in the 2020s*, BUS. INSIDER (Dec. 20, 2019) (noting Bitcoin’s purpose was to bridge the global wealth gap during the Great Recession of 2008 by fighting centralized currency manipulation by the few in powers of fiat monetary policies) [perma.cc/44W5-EW2X].

245. See René Bennett, *6 Reasons to be Unbanked or UnderBanked*, BANKRATE (Feb. 13, 2023) (pointing to factors like past financial behavior, lack of trust in banking institutions, meeting minimum balance requirements, avoiding banking fees, and escaping debt collectors can impact and produce greater numbers of unbanked individuals in the United States) [perma.cc/PHQ3-4L9M].

services.²⁴⁶ The availability of cryptocurrencies will provide low-income individuals more opportunities to own assets beyond fiat, to expand their wealth, or to take greater control of their financial wellbeing.²⁴⁷ The potential for cryptocurrency to impact these groups is massive due to the ease of access and low barrier costs; most individuals today have a cell-phone connected to the internet, helping them connect to any blockchain or cryptocurrency technology.²⁴⁸ There can be higher trust built within these systems because the value is not tied to a specific government or institution who may fail overnight and the portability aspect provides greater access to one's funds at any moment in time.²⁴⁹ Integrated payment plans, availability of credit, process for saving, and access to insurance are all ways blockchain can impact low-socio economic groups.²⁵⁰ This will allow low-socio economic groups to have a better chance of accessing much-needed capital to promote personal financial growth.²⁵¹ Since traditional centralized

246. See Goldberg, *supra* note 236 (highlighting that “banking the unbanked” has always been a global development goal to promote financial inclusion under anti-poverty work and wider economic development efforts and utilizing DeFi is more scalable and easier to access than instilling traditional financial institutions in areas of low-income).

247. See Cheong, *supra* note 244 (explaining that new cryptocurrency technologies help distribute wealth and widen investor demographics because individuals are able to use cryptocurrencies in common business transactions, such as taking out loans through credit building).

248. See *id.* (accessing the interconnected world of cryptocurrencies now only requires basic internet connection, meaning that the new technology can reach large groups of the traditionally financially illiterate).

249. See Frankenfield, *supra* note 242 (discussing cryptocurrency's ability to operate independent of major global monetary intermediaries, which provides users with greater flexibility and control over their finances).

250. See Cecilia Chapiro, *Working Toward Financial Inclusion with Blockchain*, STAN. SOC. INNOVATION REV. (Nov. 24, 2021) (“Four ways blockchain technology is beginning to help people in countries such as Kenya and Argentina build more resilient and prosperous lives through greater access to financial services.”) [perma.cc/6VCJ-WZDF].

251. See *How Does Bitcoin Help the Poor?*, GUARDIAN NIGERIA (Feb. 17, 2022 3:19PM) [perma.cc/6MRP-L7VQ].

Governments in developing nations implement laws and regulations restricting capital flow in and out of geographical borders. As such, many individuals in such countries lack adequate capital access. Bitcoin's decentralization protects it from such restrictions. Thus, such governments can't prevent the poor in their countries from accessing the much-needed capital.

financial systems are generally geared towards the elite and wealthy, DeFi creates access to modern-banking products in a secure environment regardless of economic class.²⁵²

Vast applications of blockchain and DeFi products in developing countries have enabled individuals to adopt the technology within different sectors.²⁵³ The Indian government has partnered with ConsenSys,²⁵⁴ to help with land titling, supply chains, health records, and blockchain education to help create a standardized record-keeping to combat common issues like bribery, identification requirements, and tax evasion tactics.²⁵⁵ IBM also implemented a crop-yielding blockchain in India that supports increasing yield and working closely with India's central bank, Reserve Bank of India, to formulate better farm-to-store supply chains.²⁵⁶ IBM worked with Twiga Foods in Africa to extend micro-finance loans to vendors who traditionally have credit-worthiness barriers.²⁵⁷ This greatly improves the efficiency of loan-processing, allowing more vendors to begin their businesses.²⁵⁸ Other examples include pharmaceutical companies utilizing

252. See *Banking the Unbanked: How DeFi Can Help the Low-Income Population*, COINTELEGRAPH (integrating blockchain to handle digital asset trading, lending protocols, community and money connections, and yield farming, are just a few ways blockchain technologies can positively impact low socio-economic classes) [perma.cc/N44S-4FA6].

253. See Kevin Werbach, *How the Blockchain Brings Social Benefits to Emerging Economies*, KNOWLEDGE WHARTON (Nov. 28, 2018) (providing examples of how developing nations are using blockchain technology differently) [perma.cc/EW2H-E3ZA].

254. See *ConsenSys Is a Market-Leading Blockchain Technology Company*, CONSENSYS ("ConsenSys is the leading Ethereum software company. We enable developers, enterprises, and people worldwide to build next-generation applications, launch modern financial infrastructure, and access the decentralized web.") [perma.cc/AX89-HZUV].

255. See Werbach, *supra* note 253 (integrating ConsenSys increases protection from data manipulation in the supply chain and the housing industry where bribery is especially rampant due state officials having the power to easily change records in response checks).

256. See *id.* (deepening insights into crop yields can further prepare markets for upcoming seasons and by gathering data on crucial factors such as weather, farmers are better informed of what insurance they require).

257. See *id.* (expediting the entire loan process through blockchain smart contracts that compile mobile device data and implement machine learning algorithms to predict creditworthiness).

258. *Id.*

sensors to ensure medications are stored at the right temperatures before they are sold to protect consumers from defective products, river cleanup initiatives utilizing blockchain technology to monitor toxin levels in local waters, and insurance companies managing workers' compensation claims through identity verification to expedite the process.²⁵⁹

Overall, blockchains have immense social impact through its transparency, identification, compliance, legitimacy, and trust.²⁶⁰ Beyond impacting reduction in poverty and providing accessibility into centralized systems that were previously designed towards the wealthy, there are increasing ways blockchain can aid in reducing discrimination and financial exclusion.²⁶¹ Blockchains have immeasurable potential to be adopted quickly, but data privacy laws are enabling complete integration.

VI. Application of Current Data Privacy Regulations

A regulation's existence does not automatically mean adherence. Corporate surveillance, both promoted and hindered by economic choice, is able to thrive despite data privacy regulations across various spaces. Technological advancements within both traditional data collection and blockchain has diminished the effects of these regulation efforts. Under the public interest theory of economic regulation,²⁶² governments should respond to public demands of implementing certain regulations to create more

259. *Id.*

260. See generally *Blockchain for Social Impact: The Good, Bad, and in Between*, TERRAPASS (Nov. 1, 2021) [perma.cc/TQ3C-9GUW].

261. See Nir Kshetri, *Potential Roles of Blockchain in Fighting Poverty and Reducing Financial Exclusion in the Global South*, 20 J. GLOB. INFO. TECH. MGMT. 201, 202 (2017).

Disadvantaged groups' lack of access to financial services has become one of the main problems that the world is facing today. What is new in blockchain is the combination of decentralized access and immutability, which makes it difficult to engage in opaque transactions that take place between companies, individuals, and institutions.

262. See *Public Theory of Regulation*, BODY KNOWLEDGE INFRASTRUCTURE REGUL. ("Explains government intervention in markets and associated regulatory rules as responses to market failures and market imperfections. This theory argues that regulation promotes the general welfare rather than the interests of well-organized stakeholders.") [perma.cc/MD87-PHZB].

efficient market prices or practices.²⁶³ Even with the E-Government Act of 2002, which limits data collection, management, and usage by corporations, corporations have been able to navigate away from the fine print of the Act to incorporate disclosures and fine-print agreements that readily sign away one's rights to any data privacy.²⁶⁴ If current regulations cannot curtail corporations' data usage for corporate surveillance, then they definitely cannot impact blockchain.

A. Corporations Are Skirting Around Current Data Privacy Regulations

Studies have consistently shown corporations have increasing abilities to utilize consumer data to their advantage through new technological advances that promote more efficient tracking and treading the fine lines between regulations and laws.²⁶⁵ The danger lies in the lack of universal regulation or standard for collecting, disclosing, sharing, and utilizing the data companies have collected from users.²⁶⁶ The autonomy of online contract formation has been the key for corporations to skirt around current data privacy regulations.²⁶⁷

263. See Brian Seamus Haney, *Blockchain: Post-Quantum Security & Legal Economics*, 24 N.C. BANKING INST. 117, 142 (2020) (combatting blockchain's volatile nature, government involvement can be seen as necessary to regulate large parts of the market to allow for more efficiency and fairness).

264. *E-Government Act of 2002*, U.S. DEP'T JUST. BUREAU JUST. ASSISTANCE [perma.cc/93BV-HKNV]; see also Joseph Turow et al, *Americans Can't Consent to Companies' Use of Their Data*, UNIV. OF PA. ANNENBERG SCH. OF COMM'N (Feb. 2023) [perma.cc/5DBF-MPPF] (identifying the lack of knowledge consumers have over which sites and corporations collect their data through common marketing practices because consumers fail to realize what constitutes as adequate consent)

265. See Frederik Zuiderveen Borgesius & Joost Poort, *Online Price Discrimination and EU Data Privacy Law*, 40 J. CONSUMER POL'Y 347, 349 (2017) ("New data analysis technologies, often summarized as "big data," give new possibilities for tailored pricing.").

266. See Baydakova, *supra* note 218 (lacking universal data security disclosure standards enables some crypto services to passively claim they are taking necessary measures to ensure consumers' data security, while other platforms implicate and integrate specific tech solutions into their systems).

267. See Fairfield, *supra* note 66 (showing that companies track consumers both online and offline in order to better understand their users' consumption behaviors).

Corporations have several methodologies to gather qualitative and quantitative data.²⁶⁸ The top three include asking consumers directly for use of their data, indirectly tracking online activity through usage of mechanisms, like cookies, and purchasing data from other sources.²⁶⁹ Companies require the exchange of some form of data to access their sites. The non-existence of standard regulations to regulate how data is collected combined with consumers' overt consent employed through online contracts in forms of terms of service agreements, failing to opt out of do-not-track messages, not reading a website's fine print, accepting cookies, and simply utilizing a site as a means of exchange for your information has led to continual data exploitation.²⁷⁰ In essence, collection, usage, and selling of your data is completely legal. Most consumers are unaware of corporate surveillance, therefore, providing greater data privacy regulations can help provide more transparency in this space.

Companies like Zoom, Equifax, SkyMed, and Uber all have been penalized with fines and restrictions by government agencies to enable greater data protections.²⁷¹ The FTC is notable in bringing several actions against corporations that failed to adhere to data privacy standards.²⁷² Facebook, a common data-privacy

268. See Freedman, *supra* note 73 (“Some collection methods are highly technical, while others are more deductive The bottom line, though, is that companies are using a cornucopia of collection methods and sources to capture and process customer data on metrics, with interest in types of data ranging from demographic data to behavioral data . . .”).

269. See *id.* (suggesting that “a robust business strategy needs all three” methodologies).

270. See Jennifer Horton, *Companies Are Tracking Your Personal Data Without Your Consent, What You Need to Know*, WBRC (Oct. 5, 2021) (“We haven’t passed a meaningful consumer privacy law in the United States in over twenty years, we are so far behind We rely heavily at the federal level on the Federal Trade Commission to help regulate and police this space, but that agency is woefully underfunded and its mandate is way too broad.”) [perma.cc/6N6A-H2DD].

271. See *Privacy and Security Enforcement*, FED. TRADE COMM’N (2024) (emphasizing that the FTC has brought legal actions against companies that violate the privacy rights of their consumers or mislead them by not maintaining the proper security for sensitive consumer information) [perma.cc/5YU6-RWJQ].

272. See *id.* (demonstrating that the FTC often charges defendant-companies with violating Section 5 of the FTC Act, “which bars unfair and deceptive acts and practices in or affecting commerce”).

offender due to the enormous consumer data they collect, had a \$5 billion penalty and new privacy restrictions in 2019 after the continual violation of FTC's 2012 order against the company through misrepresenting users' control over their personal information, failure to implement reasonable programs to ensure consumer privacy, and deceptive use of consumer phone numbers through two-factor authentication for targeted advertisements.²⁷³ The penalty was considered to be an anomaly; it was the largest imposition assessed worldwide with unprecedented restrictions requiring Facebook to restructure their privacy mechanisms and compliance channels.²⁷⁴ FTC's impositions had a didactic purpose to enable greater compliance. This form of compliance should be the status quo of all corporations utilizing consumer data and for emerging technologies like blockchains.

B. Non-Applicability of Existing Regulations on Blockchain

The more pressing issue is the non-applicability of existing regulations and laws on the emerging and ever-changing blockchain space.²⁷⁵ Traditional data privacy regulations and laws are applied towards a *centralized* controller-based framework.²⁷⁶

273. See *United States v. Facebook, Inc.*, 456 F. Supp. 3d 115, 119–21 (D.D.C. 2020) (noting the imposed remedial steps, including ceasing misrepresentations, clearly disclosing the sharing of users' personal information and obtaining express consent, the timely deletion of users' personal information, obtaining users' consent before implementing facial recognition technology, and undertaking an annual certification of compliance with the order and any FTC investigation); see also *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FED. TRADE COMM'N (July 24, 2019) ("The \$5 billion penalty against Facebook is the largest ever imposed on any company for violating consumers' privacy and almost 20 times greater than the largest privacy or data security penalty ever imposed worldwide.") [perma.cc/Q6VB-9CLP].

274. See Horton, *supra* note 270 (demonstrating that the lack of federal privacy laws to regulate this type of activity allows "data collection" to be framed as targeted advertising when the practice is actually far more invasive").

275. See Mike Davis, *US Must Catch Up With Rest of the World on Data Privacy*, ROLL CALL (Oct. 14, 2021, 6:00 AM) ("The U.S. is woefully behind the rest of the world in enacting universal, comprehensive data privacy laws that protect consumers. A messy patchwork of disjointed and woefully outdated laws leaves Americans vulnerable to attacks on their private data.") [perma.cc/V2B8-8G5H].

276. See Shah, *supra* note 16 (regulating blockchains with existing EU or US laws are at odds with what the regulations and laws are set out to accomplish,

Unlike traditional data collection systems, which are usually backed by government or monetary institutions, blockchain hinges upon the concept of *decentralization* and typically has no entity backing.²⁷⁷ This means blockchain has more functional flexibility outside of conventional and existing intermediaries and regulations that cannot be readily applied.²⁷⁸ For instance, the Right to Financial Privacy Act²⁷⁹ cannot provide any privacy protection within the blockchain space because blockchain entities do not fall within the limited scope of protected institutions.²⁸⁰ Existing regulations' impact on the blockchain space is still a large grey area filled with questions.²⁸¹ Since 2019, various government agencies have started paying more attention to DeFi applications of the blockchain phenomenon to aid in developing regulations and applications of law to protect consumers.²⁸² The majority of the financial agencies within the United States are either imposing existing regulatory standards on blockchain and DeFi activities or

since blockchains lack core components of a centralized system outlined in these regulations or laws).

277. *See id.* (highlighting the difficulty surrounding the legal status of cryptocurrencies due to their lack of backing from public and private entities in comparison with Fiat currencies, which derive their authority from government or monetary authorities).

278. *See id.* (“It has been difficult to make a case for their legal status in different financial jurisdictions throughout the world. It doesn’t help matters that cryptocurrencies have largely functioned outside most existing financial infrastructure. The legal status of cryptocurrencies has implications for their use in daily transactions and trading.”).

279. 12 U.S.C. § 3401 (2010).

280. *See id.* at (1) (defining a financial institution as a “bank, savings bank, card issuer . . . industrial loan company, trust company, savings association, building and loan, or homestead association (including cooperative banks), credit union, or consumer finance institution”).

281. *See* Kurt Woock, *Crypto Regulation: What’s New and What Investors Need to Know*, NERDWALLET (Dec. 19, 2022) (“Crypto is regulated by many government bodies but lacks one unifying framework. This regulatory wiggle room enables crypto businesses to experiment and grow quickly — but it also means that risky practices leaving consumers exposed can go unchecked.”) [perma.cc/44NM-YMBR].

282. *See* Frankenfield, *supra* note 242 (“In June 2019, the Financial Action Task Force (FATF) recommended that wire transfers of cryptocurrencies should be subject to the requirements of its Travel Rule, which requires AML compliance.”).

creating limited regulations and laws to adapt to the new technology.²⁸³

Due to the nature of blockchain, there are no exchanges of *traditional* sensitive private information when utilizing cryptocurrency, including name, age, or financial history, which provides some insulation of private personal information from being sold to third-parties.²⁸⁴ However, a digital trail is still left within the blockchain as each transaction is publicly recorded within the blockchain and specific entities can trace the general information through utilizing anti-money laundering (AML) efforts required under the Bank Secrecy Act (BSA)²⁸⁵ to combat terrorism.²⁸⁶ Most blockchains are also tied to traditional entities that collect user information prior to entry into the system, such as usage of third-party payment systems or banks.²⁸⁷ The newness of the cryptocurrency space and vagueness of regulations and laws has caused crypto platforms to have a wide range of disclosures and privacy practices.²⁸⁸ Most importantly, most policies mention collecting bank account numbers and trading history.²⁸⁹ In the

283. *See id.* (revisiting the SEC's treatment of Bitcoin, Ethereum, and similar crypto through its introductions, where the SEC did not deem them to be securities under their definitions, but shifted towards the end of September 2022 when SEC began to view crypto differently and deem them to be securities).

284. *See id.* (discussing the general greater protection of privacy safety on cryptocurrency platforms, since sensitive information is not required to utilize the systems, directly lowering the risk of information being compromised or a person's identity being stolen).

285. *See* 12 U.S.C. § 1951 (1970) ("It is the purpose of this chapter to require the maintenance of appropriate types of rec-ords and the making of appropriate reports by such businesses in the United States where such records or reports have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings.").

286. *See* Frankenfield, *supra* note 242 (comparing pseudonymous to anonymous transactions; since all crypto activities are pseudonymous, the actual individual's information is protected, while all other information can still be traced and utilized to understand geographic location, illegal activities, and more).

287. *See* Shah, *supra* note 16, at 3 (describing the role of third-party data collectors within the blockchain).

288. *See* Frankenfield, *supra* note 242 (listing out several cryptocurrency platforms and their associated disclosures).

289. *See id.* (stating BlockFi had the longest list of banking data it collects, while a lot of other exchanges like Binance and BitMex did not disclose what banking data is collected).

United States, the world of cryptocurrency is currently most regulated by the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), and Financial Crimes Enforcement Network (FinCEN).²⁹⁰ These efforts requiring blockchain entities to collect user details to some extent ultimately defeats the purpose of blockchain technology.²⁹¹ While users have utilized their crypto as legal tender, they do not fall neatly within the pockets clearly defined by Congress's prior regulations and law.²⁹² The inherent nature of cryptocurrency makes it hard for a specific government entity or agency to preside over its regulations and governance.²⁹³ Whether this increased regulation will help or harm low-socio economic classes' access to these new resources, particularly in the area of financial surveillance impact on privacy, is at contention. The lack of direct applicable regulations in place makes it difficult for these platforms to streamline privacy requirements.²⁹⁴

Applying existing data privacy laws onto the blockchain space is like fitting a square into a circle mold. It cannot be effective for three main reasons:

1. Existing data privacy regulations and laws are geared towards centralized systems where third-parties are able to control

290. See Kevin George, *Cryptocurrency Regulations Around the World*, INVESTOPEDIA (last updated Nov. 30, 2022) (laying out the history of regulations in the blockchain space as new regulation frameworks emerged consistently in 2022 under the Biden Administration to officially govern this area) [perma.cc/5GJD-FBQV].

291. See Ashley Longman, *The Future of Blockchain: As Technology Spreads, it May Warrant More Privacy Protection for Information Stored with Blockchain*, 23 N.C. BANKING INST. 111, 120, 125–26 (2019) (registering with FinCEN and implementing AML programs are necessary to prevent money laundering and terrorist activities and maintain up-to-date recordkeeping of related transactions).

292. See Jeremy Papp, *A Medium of Exchange for an Internet Age: How to Regulate Bitcoin for the Growth of E-Commerce*, 15 U. PITT. J. TECH. L. & POL'Y 33, 48 (2014) (setting forth similarities and differences between cryptocurrency and fiat money with the conclusion that both can fall under Congress's jurisdiction, but the autonomous nature, value, and goals of efficiency within the crypto platforms all fall outside the current statutory framework).

293. See *id.* at 49 (existing regulatory and law frameworks cannot encompass cryptocurrency usage and nature, making it harder to regulate the space).

294. See *id.* (challenging existing databases and their data methods will be difficult as it directly impacts the very nature of decentralized information).

the inflow and outflow of data.²⁹⁵ Since blockchains are decentralized with information forever captured into the chains, the inflow and outflow of information cannot be readily controlled, especially if the datapoint is already within the chain.²⁹⁶ Key elements such as the right to opt-in or opt-out in traditional data privacy spaces cannot be readily implemented into blockchains as all data persisted. Technologies can limit implementation of what data actually gets entrenched into the chains, such as zero-knowledge proofs, but the basic model of blockchains utilized contains data that can be tracked and exploited.²⁹⁷ Blockchain analytical companies have emerged in the past few years to help blockchain corporations and governments track and assess who are utilizing major platforms.²⁹⁸ Since this data is open-source, any individual with internet connectivity is able to analyze blockchain transactions on their own.²⁹⁹ Thus, data surveillance can be seen as enlarged to anyone who has sufficient resources and knowledge on how to extract and exploit the data.

2. Blockchains falling within preset regulated industries, such as money transmitters, financial institutions, or securities, will follow its associated regulations for consumer protections.³⁰⁰ However, most blockchains are able to curtail these regulations

295. See *Opt-In and Privacy Laws in North America and Europe*, L-SOFT (listing all jurisdictions requiring an opt-in and opt-out data collection requirements) [perma.cc/B6UQ-8DLJ].

296. See Carlo Gutierrez, *Making Blockchain Comply with GDPR: The Challenges and Fixes*, ALTOROS (Oct. 30, 2018) (explaining the challenges that blockchains present for compliance with GDPR laws) [perma.cc/C29M-UJCP].

297. See *The Privacy Paradox in Blockchain: Best Practices for Data Management in Crypto*, DENTONS (June 9, 2022) (“All participants in public blockchain networks trust in the sanctity of the information because they can see and analyze that information equally and in real time. But if all the information is transparent, it becomes accessible to anyone and may, theoretically, be used by unknown actors for unknown purposes.”) [perma.cc/83HF-E7Z2].

298. See Marko Mihajlović, *Top 8 Best Blockchain Analytics Tools*, SHRIMPY ACAD. (Oct. 5, 2022) (“Blockchain analytics tools are used to fight cyber-criminal activity, monitor compliance, analyze markets, and investigate blockchain activity. In this article, I’ll introduce you to the 8 best blockchain analytics tools the market has to offer.”) [perma.cc/LUF6-YSRU].

299. See Kirsty Moreland, *How to Read a Blockchain Transaction History*, LEDGER ACAD. (last updated Oct. 27, 2022) (providing a step-by-step guidance into how to verify and read transactions on a blockchain) [perma.cc/JUE6-JLL5].

300. See *generally Blockchain & Cryptocurrency Laws and Regulations 2023 | USA*, GLOB. LEGAL INSIGHTS [perma.cc/XE4H-YD5S].

due to identifications that do not fall within neatly defined spaces. This presents issues on how data privacy laws are applied to industries regulators do not oversee. Some blockchains argue their data collection does not fall under existing data privacy laws because the transactions are anonymous or because they do not meet clearly defined definitions of regulated spaces.³⁰¹ However, as discussed, anonymity within blockchain is a common myth under right investigative tools.

3. Blockchains have evolved significantly since its emergence and will continue to evolve rapidly. Regulations and laws currently in place are too two-dimensional and cannot keep up with the speed of technological advances, especially with the limited defined terms. Regulatory agencies and governments constantly must release guidance *after* issues arise. Regulations and laws for this space should be proactive of data privacy issues rather than corrective action to prevent reoccurrences. Federal agencies and industry leaders have no guarantee or the ability to predict how this area will develop. Time is of the essence because as the area evolves with greater technological advances, it will be harder to impose data privacy laws.

The innate qualities of blockchain and DeFi that enable the space to help low socio-economic classes can also be the same qualities that hinder the growth of an equal playing field.³⁰² While blockchains are capable of allowing for ease of access, transparency, and low costs to allow more people to stay intertwined economically with the rest of the world, corporations and governments who utilize this new technology can use these same features to their advantage for data collection.³⁰³ To encompass all that blockchains has to offer to low socio-economic

301. See *How Private is the Blockchain?*, BITSTAMP (Aug. 10, 2022) (explaining application of anonymity in various different blockchain platforms) [perma.cc/F4LC-GKW6].

302. See Kshetri, *supra* note 261, at 203 (“Blockchain-based solutions can be used to develop offerings that are appropriate to meet the needs of disadvantaged groups. Blockchain-based business models can enable the economics of small transactions. That is, using blockchain, banks and financial institutions can possibly exploit zero or very low marginal cost economics.”).

303. See *id.* (“Using blockchain, it is possible to keep an audit trail of transactions. In this way, accountability and transparency can be achieved in the data-exchange process.”).

groups, a solution to alleviate these pains is to create more standardized and flexible data privacy regulations.

VII. The Necessity for Standardized Data Privacy Regulations for Blockchains and Emerging Data Collecting Technologies

The regulation of our private data cannot be one-dimensional because data and technology are never stagnant.³⁰⁴ Majority of the existing data privacy laws amongst states and the limited federal ones defer consumer data protection responsibility to third parties; thus, corporations are responsible for data they indirectly accumulated.³⁰⁵ There has been growing pressures to increase protection of private information as an increasingly large part of consumers' lives have become digitalized.³⁰⁶ However, the lack of comprehensive data privacy laws created uncertainty over what constitutes as unjust data usage and provided corporation the gateway to continue gaining insight into individuals' financial information, which can disparately impact socio-economic classes. The challenge is that the blockchain space does not readily fall within the defined scope of existing federal regulations and laws that were structured to protect against data invasion. Other than basic KYC and AML requirements, most regulations cannot readily be applied to govern how data is collected, retained, and utilized in the blockchain space due to the nature of how data is stored and how the regulations are structured.³⁰⁷

304. See Andrew Burt, *Why Privacy Regulations Don't Always Do What They're Meant To*, HARV. BUS. REV. (Oct. 23, 2018) (balancing how broad data privacy regulations end up is crucial to how impactful they can be on arising technologies because if regulators go too broad, it can encourage data monopolies, but if they are too focused, some entities will be able to escape due the constraints) [perma.cc/JET7-ZDLN].

305. See generally Hossein Rahnema & Alex "Sandy" Pentland, *The New Rules of Data Privacy*, HARV. BUS. REV. (Feb. 25, 2022) [perma.cc/Q8AU-BN4S].

306. See BERNASEK & MONGAN, *supra* note 19 at 218–19 (elucidating it is governments' responsibility to incorporate sufficient regulatory controls to ensure protection can be evolving at the same pace as technological advances).

307. See Alfredo De La Cruz, *Blockchain Comes Under Data Privacy Scrutiny*, JD SUPRA (Mar. 31, 2021) (breaking apart blockchain structures means different regulatory agencies have to unite to ensure there is sufficient protection within this space) [perma.cc/RF7L-FMWK].

Blockchains require a more standardized regulatory space to provide users the confidence to utilize the new technology while knowing they are protected.³⁰⁸ Industry leaders have encouraged the usage of blockchains to stay competitive in markets.³⁰⁹ Therefore, to remain a competitive market, the United States cannot ignore this sector while balancing adequate data privacy regulations and new data collecting technologies.³¹⁰ There is a two-fold requirement that applies to actors within this space and to governments:

1. Requiring actors within this space to integrate mandatory cryptographic concepts like zero-knowledge proofs as the minimum to ensure privacy; and,
2. Governments have to formulate explicit regulations and laws to fill in the loopholes so protection of privacy is integrated at the onset of a new technology rather than an afterthought.

A. Required Implementation of Zero-Knowledge Proofs

Blockchains are fundamentally structured to be a safer option than traditional record-keeping methods due to built-in security measures such as encryption, hashing, and zero-knowledge proof systems (ZKP).³¹¹ A zero-knowledge proof is a “cryptographic protocol where a party can prove possession of certain information

308. See Sandro Psaila, *Cryptocurrency Security Standard (CCSS)*, DELOITTE (advocating for a harmonization of standards to promote confidence in cryptocurrencies) [perma.cc/FDW4-E6G9].

309. See *id.* (arguing that over-regulating and shutting out new forms of finances will simply push the technology to available markets so regulations should recognize the importance of personal financial products, which directly calls for a need for adapting regulations).

310. See Electric Coin Company, *Jack Gavigan on Regulation and Privacy-Protecting Technology*, YOUTUBE (Sept. 20, 2018) (stating that the structure of blockchains, which allows them to bypass current regulations, is deeply concerning and as a result regulators and policymakers have to connect with blockchain leaders and creators to better understand the industry in order to apply current basic privacy protection concepts toward this new area) [perma.cc/U5D8-XK5D].

311. See *Zero-Knowledge Proofs*, ETHEREUM (last updated Feb. 10, 2023) (providing a brief history of the zero-knowledge proof, a way that parties can prove various aspects of transactions without knowing the underlying facts themselves, which has been evolving and used in several applications today) [perma.cc/P97Q-UQTU].

without revealing the information itself” to strengthen information security.³¹² On a basic level, ZKP systems apply algorithms to inputted data and return an output of either true or false if the information matched without revealing the underlying information; a user only learns of the information’s truthfulness.³¹³ For example, a system contains a complex mathematical problem with the complete solution and a user wishes to verify if the answer they obtained is correct; through ZKP, the system will automatically confirm or deny if the solution matches, but does not reveal the solution or actual answer.³¹⁴ It is especially beneficial in protecting personal and sensitive data if deployed correctly since data is encrypted *before* a user interacts with any service providers.³¹⁵ ZKPs are easily integrated into blockchains to group people together within the cryptography space who operate on a basic level of distrust.³¹⁶ They are also applicable across various industries.³¹⁷

312. *See id.* (“Zero-knowledge proofs represented a breakthrough in applied cryptography, as they promised to improve security of information for individuals.”).

313. *See Zero Knowledge Proof: Type, Advantages, Use Cases*, HYPERSIGN (June 09, 2023) (“Zero-knowledge proofs operate through a complex cryptographic process where a prover aims to convince a verifier of the validity of a statement without revealing the actual data.”) [perma.cc/X7QQ-9WMW].

314. *See* Yuqing Cui, *Application of Zero-Knowledge Proof in Resolving Disputes of Privileged Documents in E-Discovery*, 32 HARV. J. L. & TECH. 633, 640 (2019) (illustrating usages of zero-knowledge-proofs in a Sudoku puzzle where users can determine if their solution was correct without seeing the actual inputs).

315. *Id.*; *see also* *What is Zero-Knowledge Encryption?*, CHAINLINK (Nov. 30, 2023) (explaining that there are multi-step encryptions with zero-knowledge proofs sending information to ensure greater privacy and security protection making it effectively impossible for services to gain access to permissionless knowledge) [perma.cc/Q6Q4-VEK3].

316. *See* Electric Coin Company, *Perspectives: Tromer on Zcash Cryptography*, YOUTUBE (Oct. 25, 2018) (stating that trusting a blockchain is not the ultimate goal to strive for, rather these new technologies should put users to trust in logic, mathematics, and what academia has determined to be true schemes of information to provide a more trusted process underlying these technologies) [perma.cc/SP25-KZXZ].

317. *See* Alexander Ray, *Zero-Knowledge Proof: A Revolutionary Leap in Data Protection*, FORBES (July 25, 2023) (“In the banking industry, ZKP can transform customer authentication. Financial institutions can verify details of customers, such as age, creditworthiness or account balances, without accessing their

ZKPs have already proven themselves efficacious in protecting data in various countries.³¹⁸ Estonia integrated ZKP into a digital identity framework for consumers to share limited personal data with service and goods providers and created a pilot program that has allowed easier access and facilitated lower costs to citizens voting.³¹⁹ Singapore’s government, with “Project Ubin,” is attempting to implement ZKPs into personal data platforms through decentralized banking.³²⁰ Through “Project Ubin,” Singapore is striving to create a form of decentralized banking with the help of ZKP for privacy and security measures. Most notably, the European Union Committee has approved the usage of ZKPs in the European digital identity framework with anticipation of complete implementation in the coming years.³²¹ EU consumers will directly manage the sharing of various data with service providers in their daily lives, including but not limited to opening bank accounts, checking into hotels, renting cars, verifying ages, filing tax returns, applying to universities, and requesting public documents.³²²

sensitive personal data. This ensures secure transactions and mitigates the risks of identity theft and fraud.” [perma.cc/BZ6V-PLM5].

318. See *id.* (“Several governments have recognized the potential of ZKP for safeguarding personal data and have begun embracing this technology in their operations.”).

319. See Ravi Chamria, *Practical Use Cases of Zero Knowledge Proofs*, ZEEVE (Nov. 10, 2023) (“ZKP applications resolve the problem of rigging in voting through a privacy preserving, smart-contract triggered check and balance mechanism. The voters can anonymously cast their votes without revealing their true identity and the cryptography computations ensure that results could be verified on-chain to restore the true essence of democracy.”) [perma.cc/5S4K-R3Z4].

320. See Michael del Castillo, *Details Emerge on Singapore Central Bank’s Blockchain R&D*, COINDESK (July 23, 2017) (“By tokenizing global currencies and protecting the privacy of each transaction using zero-knowledge proofs, Intel’s software guard extensions, or other means currently being explored, the new system of self-executing smart contracts could increase both the speed and privacy of international transactions.”) [perma.cc/R3QC-QH2H].

321. See David Attlee, *European Union Discusses Using Zero-Knowledge Proofs for Digital IDs*, COINTELEGRAPH (Feb. 16, 2023) (“While the latest draft is still not available publicly, the press release specifies that EU citizens would be granted full control of their data, with the option to decide what information to share and with whom”) [perma.cc/G7KD-RD8C].

322. See *European Digital Identity*, EUR. COMM’N (using the new EU Digital Identity Wallet will allow consumers to have a grasp on their personal data when

However, even with a strong technological security, there are cons to this system that result in uneven protection for the average consumer.³²³ Advanced security systems like ZKPs are typically tied to insurmountable costs behind the hardware, proof verifications that require complex computations, and challenging implementation processes.³²⁴ There are also inherent trust assumptions in which participants are already assumed to be honest during onboarding. Such assumptions make it harder to implement any proving mechanisms once in the system.³²⁵ Lastly, as technology continues to advance and the usage of quantum-computing becomes more rampant, it is unsure if ZKP security systems can withstand or stay up to speed with immunity to these developments.³²⁶

The cons of ZKPs does not outweigh its benefits. The United States should follow Estonia, Singapore, and the EU's footsteps to implement a standardized form of ZKPs to protect consumers' data privacy. This will allow consumers to have a baseline of security while accessing goods and services without the cost of all of their personal data. Limiting access to data collection will constrain corporate surveillance and give consumers their economic choice back to maximize consumer surplus.

interacting with businesses and will be a relatively easy implementation for all parties involved) [perma.cc/FDY9-JA5U].

323. See Electric Coin Company, *Eran Tromer on the Importance of Privacy*, YOUTUBE (Sept. 6, 2018) (explaining the reality that criminals are able to put in the necessary resources to obtain privacy on blockchains, while citizens who cannot cover mental, physical and convenience overheads have to give up on privacy in exchange for utilizing these services) [perma.cc/NFV2-CZU8].

324. See *Zero-Knowledge Proofs*, *supra* note 311 (recognizing the many drawbacks of zero-knowledge proof systems and how it may not be the one-size-fits-all solution to data-privacy issues).

325. See *id.* (creating the necessary connection between the information protected and the data matching up via the zero-proof technology requires provision of the initial information that is assumed to be true and once entered is in the system indefinitely).

326. See *id.* (explaining that the development of quantum computers could affect the security model in the future).

B. Call for Standardized Blockchain Regulations

The federal government needs to create standardized data privacy regulations that are readily adaptable to emerging technological advances handling data to protect consumers' privacy. As more industries and countries have implemented blockchain technology, cryptocurrency payments, and utilize cryptocurrency generally, having direct insight into one's financial standpoint can hinder price alterations to specific groups.³²⁷ By having regulations that hinder this insight can protect those in every socio-economic class to make more reasonable economic choices and maintain consumer surplus resulting in a more efficient market.³²⁸

New regulations or laws must adapt to the new model of data-collecting technologies. At minimum, these regulations and laws must instill the requirement of additional safeguards and zero-knowledge proof technologies within spaces like blockchain. Regulations and laws cannot have clear distinctions between centralized and decentralized systems.³²⁹ It has to be flexible to adapt to any form of arising data-collecting system. This means understanding not only how these systems operate and utilize data but also the concept that data lives indefinitely within a chain. Built-in mechanisms are required to ensure there is no data leakage or greater ease for corporations to resort back to their surveillance ways. Only then will they be able to continuously protect consumer privacy and combat corporate surveillance.

327. See WORLD ECONOMIC FORUM, THE APPROPRIATE USE OF CUSTOMER DATA IN FINANCIAL SERVICES 7 (2018) (illustrating how access to consumer financial data could encourage companies to target, or exclude, consumers based on real or perceived risks); see also U.S. DEP'T OF TREASURY, CRYPTO-ASSETS: IMPLICATIONS FOR CONSUMERS, INVESTORS, AND BUSINESSES 46–49 (2022) (explaining how “[d]ifferent populations and individuals vulnerable to disparate impacts may be subject to greater harms” such as targeting marketing, fraud, and scams).

328. See Lizzie O’Shea, *Digital Privacy is a Class Issue*, NEW REPUBLIC (May 30, 2019) (“These practices particularly affect poor people, who are more dependent on cheap or free online services. The services appear to cost nothing, but payment is in data rather than dollars. Such a transaction renders the user into a source to be mined for information . . .”) [perma.cc/Z7WF-AMM4].

329. See Shah, *supra* note 16 (distinguishing between these two systems is crucial because most regulations are only centered around centralized systems and proving insufficient for decentralized).

Previous efforts include the Cryptocurrency Security Standard (CCSS) introduced in 2014, which provides baseline guidance on security standards and has been commonly implemented amongst most cryptocurrency platforms.³³⁰ However, the CCSS focuses mainly on the management and storage of the crypto asset itself within transactions and not as much on the private information of users.³³¹ In addition, with the rapid emergence of various crypto startups, many new firms do not operate under the CCSS standard when it comes to security due to lack of resources or tests in place.³³² This is a major security issue as these companies do not even comply with the most basic level I compliance.³³³ CCSS is not managed by a government authority and therefore has not had immense success in implementation.³³⁴ A more comprehensive protection over users' personal information is required.

The American Data Privacy Protection Act (ADPPA)³³⁵ is one of the first federal-level data privacy protection legislation introduced in recent years, but failed to be enacted in December of 2023.³³⁶ It was the first federal data privacy bill progressed far enough in the bill voting process to potentially have an impact on

330. See Psaila, *supra* note 308 (specifying this standard emerged only for the cryptocurrency space amongst concerns of security).

331. See *id.* (providing standards for secure management of crypto environments in which wallets operate within is the main focus of CCSS, which makes it more limited in application).

332. See *id.* (lacking sufficient baseline regulations already hinders the protection of data privacy).

333. See *id.* (“While reviewing current breaches, it appears that every system that suffered a high profile cryptocurrency breach was found to be non-compliant with CCSS Level 1.”).

334. See Govindraj Basatwar, *Cryptocurrency Security Standard (CCSS) – A Quick Guide*, APPSEALING (last updated July 06, 2022) (“The crypto currency security standard (CCSS) Steering Committee is armed with a mission to improve the standards of crypto currency dealings and apply industry best practices to manage CCSS. . . . There are predominantly two areas that are the focus – asset management and operations.”) [perma.cc/AF2S-72LQ].

335. H.R. 8152, 117th Cong. (2022).

336. See Matt Davis, *What is the American Data Privacy and Protection Act (ADPPA)?*, OSANO (Aug. 5, 2022) (explaining since it is a federal law, it will preempt all state law to provide a baseline of privacy and data protection for consumers so states can still implement their own data privacy laws but it will have to be stricter) [perma.cc/6UJE-RKU7].

how data is utilized, but industry leaders deem there is still a long way to go for approval from Congress for protection of this caliber.³³⁷ This Act provides broad definitions of covered entities to those that are currently under the FTC or a common carrier under the Communications Act.³³⁸ It attempted to cover all data linked or can be reasonably linked to an individual or device such as IP addresses, prior protected data such as data surrounding children’s privacy, sensitive data such as race, ethnicities, genetics, social security numbers, etc.³³⁹ Large data holders will have a different level of oversight and data privacy requirements due to the sheer volume of data they will have to engage.³⁴⁰ It also covered smaller businesses that were not previously covered by federal or most state privacy laws due to their size.³⁴¹ The last major change would be the ability for consumers to opt out of data collection regardless if there are any monetary transactions.³⁴² This legislation proposal is a suitable starting point for blockchain regulations and government agencies to begin formulating legislation for blockchain that is more comprehensive.

FTC’s impositions on Facebook back in 2019 can provide a great framework on corporation’s internal controls. Requirements include establishing an independent privacy committee to remove

337. *See id.* (updating the status as it is now requiring both Republicans and Democrats to support the law and there will most likely be revisions and changes along the way to appease both parties).

338. *See id.* (providing the definition of covered entities—“any entity or person that collects, processes, or transfers data and is subject to the Federal Trade Commission Act, is a common carrier under the Communications Act, or is a non-profit”—and noting that it “covers the vast majority of businesses”).

339. *See id.* (describing the notable features of the Act as including preemption, protection of for certain types of data, and rights of action for noncompliance).

340. *See id.* (listing the affected companies who would have to comply, which is broken down by revenue, amount of data impacted, number of consumers’ data utilized).

341. *See id.* (explaining how “nearly every kind of business is subject to the ADPPA,” whereas “other state privacy laws generally don’t restrict businesses that process fewer than 100,000 individuals’ data”).

342. *See id.* (opting-out option were traditionally required for only banks and similar financial institutions while other businesses that did not fall within this line of category are free to input their data collection and privacy methods into the usage contract with no repercussions).

unconstrained control by directors to make privacy decisions,³⁴³ and a mandatory designation of compliance officers at every level overseen by the independent privacy committee to implement privacy protections and submit quarterly reports to associated overseeing government agencies.³⁴⁴ This separation is imperative for privacy to be protected independent of business decisions.

The confluence of past government agencies' actions and proposed legislations can generate a framework of privacy protections to be implemented. Whether it is imposing new regulating responsibilities upon existing agencies or creating a new agency to fully oversee emerging spaces, the move for more federal standardization and oversight is a necessity. Corporations should never be given the option to abrogate their responsibility to protect privacy. Current data privacy legislations are still too focused on the centralization of data in traditional fashions where data is controlled by identifiable entities and are malleable. Without removing the division between real-world applications to advanced technologies, regulations and laws will never be able to catch up to ways data privacy can be infringed upon. Flexibility is required to be applicable to rising technologies that collect and utilize data.

VIII. Conclusion

As a recognized fundamental human right, data privacy should be protected zealously throughout new emerging technological advances, such as blockchain, to combat corporate surveillance.³⁴⁵ Existing regulations and laws, whether it is in the United States or internationally, are currently insufficient to protect against this exploitation with traditional forms of

343. See *United States v. Facebook, Inc.*, 456 F. Supp. 3d 115, 120 (D.D.C. 2020) (listing the terms of the stipulated order, one of which requires Facebook to “[commission] regular, independent assessments of its privacy practices and provid[e] them to the FTC”).

344. See *id.* (noting that the requirements grant Facebook substantial abilities to avoid liability).

345. See Electric Coin Company, *Sean Bowe on Privacy and Regulation*, YOUTUBE (Sept. 20, 2018) (agreeing to the importance of privacy within the blockchain and decentralized finance space to further balance innovation and creating necessary protections).

corporations, much less new technologies that encompass a much greater volume of consumer data. Blockchain's decentralized, speed, and transparency has contributed to its increasing popularity, but those are the same elements that allow it to escape compliance with existing data privacy laws. Blockchains already possess the ability to be the future of advancements and have immense potential to ensure those in lower socio-economic classes have the chance to engage within the world economy. If their data is utilized for further corporate surveillance as payment in exchange to participate and grow financially, it completely defeats the purpose of decentralized finance and increased privacy. Instead of forcing blockchain to comply with regulations and laws created for a centralized system, regulations and laws have to be adaptable to blockchain's innovation. It is incredibly important for policymakers and regulators to heed greater attention in the coming years to ensure blockchain technology can continue to develop to integrate all groups of people without exploitation.