DATA PRIVACY BY CONTRACT

Ifeoma Ajunwa† *and Austin Kamer*††

Protecting consumer privacy rights presents a particular challenge given the prevalence of data breaches. This Article notes that current law is woefully inadequate in protecting the privacy rights of consumers. Notably, the law fails in the following four areas: (1) classification of consumer data, (2) lack of a comprehensive approach, (3) after-the-fact focus, and (4) limited accountability for third parties. Although it may be impossible to eliminate all data breaches, more regulations can bolster protection without restricting technological advancements. This Article proposes a contractual approach to privacy protection for consumers. It argues that the creation of mandatory implied contractual terms of data privacy, regulated by the Federal Trade Commission (FTC), is necessary to better protect consumers from data breaches. Part I conceptualizes data acquisition practices, proposes a data reclassification solution, and analyzes trade-offs incurred by further regulations. Part II provides background on the discombobulated state of consumer privacy governance and how implied contractual terms solve the law's pitfalls by providing a comprehensive solution. Part III provides the following six arguments in favor of the implementation of implied contractual terms: (1) the FTC possesses the requisite authority to regulate implied contractual terms, (2) current precedent's policy implications align with the proposed contractual terms, (3) the addition of implied terms of data privacy enables a cause of action before a data breach occurs, (4) contractual obligations promote data minimization for businesses collecting consumer information, (5) the focus of the law shifts to holding more parties responsible, and (6) there is a clear path that the FTC may follow to implement the implied contractual terms of data privacy. Part IV addresses anticipated criticisms.

† Asa Griggs Candler Professor of Law, Emory Law School. Many thanks to Professors Daniel Solove, Woodrow Hartzog, and Danielle Citron for helpful comments.

†† J.D. Candidate, University of North Carolina School of Law (May 2024). Special thank you to my family and my professors for their support.

TABLE OF CONTENTS

INTRODUCTION

Although the Supreme Court has long recognized a right to privacy,[1] the question of how to preserve those rights remains a thorny one.[2] The problem of data breaches represents a particularly complex issue given that the harm from such breaches can be both present and future. Preserving a consumer's right to privacy has become especially fraught in our "data-driven" political economy where consumers are obligated to share their personal information in exchange for access to utilities (such as the internet) and for other modern conveniences.[3] January 19, 2023 marked the end of a two-month-long data breach affecting approximately thirty-seven million T-Mobile customers.[4] Before the 2023 breach, T-Mobile had pledged $150 million for security upgrades following a previous attack in 2022 that affected seventy-six million customers.[5] However, the most recent attack "raises serious questions over whether [the money] has been well spent."[6] Increased security spending does not always equate to better data protection, as evidenced by data breaches at technology giants such as Apple, Twitter, and Meta between 2022 and 2024.[7] Consumers are often unaware of what information businesses save

---

1 Griswold v. Connecticut, 381 U.S. 479, 483 (1965) ("In other words, the First Amendment has a penumbra where privacy is protected from governmental intrusion. In like context, we have protected forms of 'association' that are not political in the customary sense but pertain to the social, legal, and economic benefit of the members." (quoting NAACP v. Button, 371 U.S. 415, 430–31 (1963))).

2 *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 2 (7th ed. 2021) ("Information privacy law is an interrelated web of tort law, federal and state constitutional law, federal and state statutory law, evidentiary privileges, property law, contract law, and criminal law."); Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 798–99 (2016) ("For most courts, privacy and data security harms are too speculative and hypothetical, too based on subjective fears and anxieties, and not concrete and significant enough to warrant recognition.").

3 *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 113–14 (2019); Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 737 (2018) (arguing that courts are far too dismissive of data breach harms and advocating for a "coherent theory or approach").

4 Aaron Drapkin, *Data Breaches That Have Happened in 2022, 2023 and 2024 So Far*, TECH.CO, https://tech.co/news/data-breaches-updated-list [https://perma.cc/5JWG-KQ9C] (Jan. 2, 2024) (explaining that some of the largest technology companies have experienced cybersecurity attacks between 2022 and 2024).

5 *Id.*

6 *Id.*

7 *See id.* (outlining a timeline of data breaches from companies that have spent significant amounts of money to heighten data security).

and how they use it,[8] which leads to data acquisition that individuals did not know occurred, much less consented to. Smartwatch activities such as recording heart rate, location, blood oxygen levels, calories burned, and steps taken,[9] are stored on a computer server, waiting for third parties to access the information. Technological advancements have maximized convenience at the cost of elevated data gathering and distribution. The public's growing concern around information privacy highlights current laws' inability to provide adequate security.[10] We must secure greater legal protection against consumer data collection and dissemination without consent.

The methods by which companies store and distribute personal information have a significant impact on nearly everyone. For instance, Apple has 1.65 billion products in use (as of 2021), which generates a data repository and dispersion footprint that encompasses all technologically advanced civilizations.[11] Apple's "Apple Watch" continuously measures the heart rates of individuals using the watch.[12] The "Pixel" phone by Google allows users to disable location services, but they "can still get local results and ads based on [their] IP address[es]."[13] Apple publicly declares that it does not sell or give away any data to third parties.[14] But Apple retains user information "for so long as necessary" and further states that users' "personal data may be transferred to or accessed by entities around the world."[15] Now, consider that Apple keeps bank details, facial recognition data, personal addresses, health information, government identification data, and various other forms of information

---

8 *Your Data Is Shared and Sold . . . What's Being Done About It?*, KNOWLEDGE AT WHARTON (Oct. 28, 2019), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done [https://perma.cc/MS96-GYTE] (stating that most people are unaware of how much of their activities are tracked).

9 *See* Alex, *What Can a Smartwatch Measure? A Look at 10 Important Sensors*, SMARTTECHR (Dec. 27, 2022), https://www.smartechr.com/what-can-a-smartwatch-measure.

10 *See 2019 Consumer Data Privacy Legislation*, NAT'L CONF. OF STATE LEGISLATURES, https://www.ncsl.org/technology-and-communication/2019-consumer-data-privacy-legislation [https://perma.cc/W9WA-5ZVV] (Jan. 3, 2020) (describing how smart home devices and intelligent personal assistants' ability to collect and share personal information has heightened concerns about data privacy).

11 Jacob Kastrenakes, *Apple Says There Are Now over 1 Billion Active iPhones*, THE VERGE (Jan. 27, 2021, 5:59 PM), https://www.theverge.com/2021/1/27/22253162/iphone-users-total-number-billion-apple-tim-cook-q1-2021 [https://perma.cc/L2R9-XKDR].

12 *Apple Watch User Guide: Check Your Heart Rate on Apple Watch*, APPLE, https://support.apple.com/guide/watch/heart-rate-apda88aefe4c/watchos [https://perma.cc/2LLG-76WP].

13 *Pixel Phone Help: Manage Your Pixel Phone's Location Settings*, GOOGLE, https://support.google.com/pixelphone/answer/9083770?hl=en [https://perma.cc/5XPJ-SVWH].

14 *See* APPLE, APPLE PRIVACY POLICY 5 (2024), https://www.apple.com/legal/privacy/pdfs/apple-privacy-policy-en-ww.pdf [https://perma.cc/3RDN-CWN4].

15 *Id.* at 5, 8.

on each consumer,[16] and multiply the data by 1.65 billion devices. Even if Apple did not collect individuals' information, it still promotes third parties' collection of consumer data by including those companies' default services on each device.[17] The scant legal provisions covering such practices provide little protection.

Current law falls short in regulating data privacy in four ways. First, the law fails to properly categorize consumer information. California law permits companies to disburse consumer data if the statute considers the information deidentifiable.[18] However, individuals can easily reidentify information,[19] indicating that current law offers no concrete protection. Second, the absence of federal law results in a "patchwork" approach by state laws.[20] The lack of comprehensive federal legislation creates difficulties navigating the various statutes and inconsistent legal interpretations. Third, U.S. legal doctrines focus on penalizing companies after a data breach occurs instead of implementing preventive measures, resulting in a failure to provide protection before consumer harm materializes.[21]

Fourth, the law is inadequate in holding third parties accountable. For instance, data gathering when clicking "accept all cookies" on a website involves more than just the host company. Companies purchase data gathering software from third-party sources and sell or provide internet cookie information to advertisers and researchers, and the law permits such practices.[22] Thus, multiple parties are responsible for tracking cookies beyond the point when the consumer believes data collection ended.[23] The current regulations offer limited consumer protection against third-party entities, regardless of how invasive their

---

16 *Id.* at 3–4.

17 *See* Manik Berry, *Does Apple Sell Your Data? Everything You Need to Know*, FOSSBYTES (Mar. 31, 2021), https://fossbytes.com/apple-data-collection-explained [https://perma.cc/ZX8A-A69X] (commenting on how Apple accepts up to $12 billion from Google so that Google can remain the default search engine on Apple products).

18 *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.140(e), (m), 1798.145(a) (West 2024) (providing companies the option to disseminate deidentified data under certain circumstances).

19 *See* Daniel C. Barth-Jones, The "Re-Identification" of Governor William Weld's Medical Information: A Critical Re-Examination of Health Data Identification Risks and Privacy Protections, Then and Now 1 (Sept. 3, 2015) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2076397 [https://perma.cc/Q6CB-MQE5].

20 Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 796 (2022).

21 *See* DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT 77–78 (2022).

22 *See id.* (detailing the areas of privacy fault in third-party software that current privacy law does not address).

23 Max Stul Oppenheimer, *Internet Cookies: When Is Permission Consent?*, 85 NEB. L. REV. 383, 386–87 (2006).

technology or information acquisition practices are. The law's narrow focus on data collection companies renders the current regime ineffective.[24]

Therefore, the law fails in the following four areas: (1) classification of consumer data, (2) the lack of a comprehensive approach, (3) an after-the-fact focus, and (4) limited accountability for third parties. Although it is not possible to eliminate all data breaches, more regulations can bolster protection without restricting technological advancements.

A major scholarly development, *Breached!*,[25] authored by legal scholars Daniel Solove and Woodrow Hartzog, attempted to address failures of current consumer privacy law. The book illuminates serious privacy concerns but does not fully encapsulate a necessary solution. We compare each of the four current privacy law failures to the solutions proffered in *Breached!*

First, *Breached!* does not address the classification of consumer information. Solove and Hartzog do not address the relationship between the consumer and their information. Since the way a business obtains consumer information is equally as important as what information the company collects, failing to address information classification leaves a gap that we intend to fill. This Article sets forth guidelines for reclassifying consumer information in a way that helps broaden the scope of protected information set forth in *Breached!* The authors refer to data security as involving "personal data,"[26] without referencing the nuanced intricacies accompanying such an expansive term.

Not all classes of consumer information merit heightened protection. Although *Breached!* leaves room for further development on data classification, Solove and Hartzog provide important guiding principles on the level of protection needed. The authors illustrate that data privacy exists on a spectrum.[27] This spectrum ranges from no privacy protection, which is inequitable to consumers, to overprotecting and limiting the functional services that both consumers and businesses need.[28] Protecting all classes of consumer information leads to decreased functionality of services.[29] Protecting too few classes of consumer information leads to exposure of personal data to parties that consumers do not want their data exposed to.[30] These principles, set forth in

---

24 *See generally* SOLOVE & HARTZOG, *supra* note 21.

25 *Id.*

26 *Id.* at 131.

27 *See id.* at 70 (explaining that overprotecting information leads to decreased practicality of using certain services).

28 *See id.*

29 *See id.*

30 *See id.*

Breached!, guide this Article, including the reasoning set forth for the reclassification of consumer information and the explanation of why certain classes should remain less protected. The authors often mention differences between privacy and security.[31] This Article does not seek to change industrial security. Instead, we put the onus on businesses to determine what protections are necessary. We set forth a standard for what information should fall within the realm of protection. We agree with Solove and Hartzog's contention that "[p]rivacy is about trust, power, dignity, and the collective autonomy to set the preconditions of human flourishing,"[32] and we aim to actualize that statement in our proposal.

Second, *Breached!* illuminates the shortcomings of the sectoral approach but leaves open the question of how to fix it: "At the federal level, there was considerable talk about passing a breach notification law, but Congress has been gridlocked in partisan bickering for much of the time since 2000."[33] The authors demonstrate the sectoral approach for American consumer privacy by delving into differing breach notification laws between states: "Breach notification laws differ significantly on how they define a 'data breach'—the type of incident that triggers notification. Generally speaking, most states define a breach either as any unauthorized access to personal information or as acquisition of personal information."[34] The different definitions of breach reveal there is room for synchronicity between the states, which is where this Article fills gaps revealed in *Breached!*

This Article proposes a level of reasonableness in the comprehensive implied terms of data privacy that Solove and Hartzog disagree with. The authors disregard a reasonableness approach because "many companies find it too vague and lacking in sufficient guidance about what they ought to do."[35] We propose a differing view on the reasonableness standard for data privacy that *Breached!* does not cover.

Third, *Breached!* does not fully address a solution for the after-the-fact focus of current data privacy laws: "The law most often jumps in after the breach. But this is the least effective time for the law to become involved."[36] Solove and Hartzog are correct that the law is ill-equipped to handle data privacy breaches before it is too late. The authors posit that legal ramifications after a breach often add to the "pain" that already

---

31 *See, e.g.*, *id.* at 132.

32 *Id.* at 135.

33 *Id.* at 40.

34 *Id.* at 41–42.

35 *Id.* at 51–52.

36 *Id.* at 78.

exists,[37] but do not offer an effective proposal to solve the additional pain of punishment after the breach. Solove and Hartzog also correctly identify that "[a] better strategy would be to focus on the optimal time to intervene in the life cycle of a cybersecurity incident."[38]

This Article aims to correct the after-the-fact focus that *Breached!* identifies. Through Federal Trade Commission (FTC) regulation and compliance programs, a solution to the problem Solove and Hartzog identified is achievable. We incorporated the requirements *Breached!* spelled out into a comprehensive data privacy law framework that the authors did not fully develop in the book.

Fourth, *Breached!* does not propose a solution for expanding accountability for third parties. Solove and Hartzog set forth an employee training guide to help limit third-party exposure,[39] but employee training will not provide the same force as law. The authors note that many devices are poorly designed,[40] but do not propose a methodology to bring accountability to these designers in the way that implied contractual terms of data privacy would. Solove and Hartzog recognize the need, stating that "the law, unfortunately, isn't stepping in to correct for this market failure by forcing these manufacturers to internalize their costs."[41] Mandating contractual terms of privacy forces designers to internalize the cost of faulty products. The authors similarly demonstrate advertisers' lack of liability for faulty ads but fail to propose a solution to the problem.[42] Implied data privacy provisions in contracts provide the necessary protection that Solove and Hartzog discuss.

Regarding third-party accountability, *Breached!* states that "[l]egally mandated requirements are never administered with the same zeal as profit-motivated endeavors."[43] FTC enforcement of implied contractual data privacy terms build on the "profit-motivated" principle set forth in *Breached!* because the FTC can impose substantial penalties on third parties for privacy violations.[44]

---

37 *See id.* at 53 (arguing that penalizing companies after breaches occur and consumers are notified only makes the situation worse because the damage to consumers extends beyond what would have occurred if protections were in place to prevent breaches altogether).

38 *Id.* at 79.

39 *Id.* at 104.

40 *Id.* at 86.

41 *Id.* at 87.

42 *See id.* at 90 (stating that advertisers are not responsible for faulty advertisements because too much protection would render businesses inoperative due to falling incomes).

43 *Id.* at 96.

44 *See* FED. TRADE COMM'N, 2020 PRIVACY AND DATA SECURITY UPDATE 3, 5, 11 (2020), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf

Thus, while *Breached!* provides many important concepts to incorporate into a new data privacy law, the book does not encompass the necessary solution. This Article builds on the guidelines set forth by Solove and Hartzog by proposing a comprehensive solution that legal precedent has yet to accomplish.

A recent Supreme Court opinion, *Carpenter v. United States*,[45] gave the Court an opportunity to close the gap between law and reality. The question tasked to the Court was the permissibility of evidence of a potential suspect's location based on cell site information.[46] Cell site information is the data received from a cell phone provider about the location of a device, often taken passively without user permission.[47] The Court disappointingly came to the narrow holding that *only* in the case of police accessing cell site information to obtain consumer location may a consumer's right to privacy be invaded,[48] making no mention of data categorization, comprehensive protection, after-the-fact focus, or third-party privacy liability. Scholars have argued that the limited holding should be expanded to other technological areas and beyond the criminal context.[49] The long-felt need for governance in civil consumer privacy scenarios exists deeper than the holding in *Carpenter* provided for.

This Article argues that consumer data collection laws are inadequate to protect individual privacy and that further action—specifically, the creation of mandatory implied contractual terms of data privacy, regulated by the FTC—is necessary to achieve the law's objectives. Part I conceptualizes data acquisition practices, proposes a data reclassification solution, and analyzes trade-offs incurred by further regulations. Part II provides background on the discombobulated state of consumer privacy governance and how implied contractual terms solve the law's pitfalls by providing a comprehensive solution. Part III provides the following six arguments in favor of the implementation of implied contractual terms: (1) the FTC possesses the requisite authority to

---

[https://perma.cc/R57D-57XF] (describing the billions of dollars in penalties enforced by the FTC for privacy violations).

45 585 U.S. 296 (2018).

46 *Id.* at 300.

47 *See Historical Cell Site Data: What Is It, and Is It Protected by the Fourth Amendment?*, BREEDING CARTER (Oct. 6, 2022), https://www.breedinglaw.com/10/deferred-prosecution-for-individuals [https://perma.cc/NZ2T-JA9F] (providing a simplified version of how historical cell site data is collected).

48 *See Carpenter*, 585 U.S. at 316 (holding that in the case of a criminal defendant, law enforcement must receive a warrant before invading the privacy of an individual based on their cell phone's GPS data).

49 *See, e.g.*, Daniel de Zayas, Comment, Carpenter v. United States *and the Emerging Expectation of Privacy in Data Comprehensiveness Applied to Browsing History*, 68 AM. U. L. REV. 2209, 2243 (2019).

regulate implied contractual terms, (2) current precedent's policy implications align with the proposed contractual terms, (3) the addition of implied terms of data privacy enables a cause of action before a data breach occurs, (4) contractual obligations promote data minimization for businesses collecting consumer information, (5) the focus of the law shifts to holding more parties responsible, and (6) there is a clear path that the FTC may follow to implement implied contractual terms of data privacy. Part IV addresses anticipated criticisms.

I. ORIGINS OF DATA COLLECTION AND DISSEMINATION

Information collection and dissemination practices have become increasingly invasive to consumer privacy. As data stockpiling practices evolve, so does the intimacy of information businesses obtain from consumers. However, the law has failed to keep up with technological advances that enable these practices. This Part analyzes the relationship between the origins of data collection and law. First, data collection's historical context is analyzed, and a proposed reclassification of consumer data is put forth. Second, data dissemination practices are evaluated. Third, the difficulties of determining legally recognized privacy harms are assessed. Fourth, the trade-offs of further privacy regulations are determined to weigh the pros and cons of heightened consumer data governance.

A. *Data Collection*

Data collection is not a new concept. In 1960, scientists discovered an Ishango Bone (from 18,000 BCE) with notches marked onto its surface.[50] The notches kept track of trading activity and supplies, which helped paleolithic tribespeople predict how long their food supply would last.[51] Gradually, data collection evolved beyond inventory tracking. In 1965, the U.S. government planned "the world's first data center to store 742 million tax returns and 175 million sets of fingerprints on magnetic tape,"[52] marking the beginning of big data and invasive information acquisition practices. By 2009, "[t]he average U.S. company with over

50 Bernard Marr, *A Brief History of Big Data Everyone Should Read*, WORLD ECON. F. (Feb. 25, 2015), https://www.weforum.org/agenda/2015/02/a-brief-history-of-big-data-everyone-should-read [https://perma.cc/6ZBZ-T7JF].

51 *Id.*

52 *Id.*

1,000 employees [was] storing more than 200 terabytes of data."[53] Businesses collect information on consumers to improve services, adjust prices, predict market activity, and improve efficiency.[54] The creation of the internet connected every device and allowed companies to track categories of information on an unprecedented scale.

Companies collect a plethora of consumer information, including both quantitative and qualitative data.[55] Quantitative data includes the "what" or "how many,"[56] while qualitative data seeks a deeper understanding of "why" a consumer bought something or acted in a certain way.[57] Businesses often implement data gathering practices under the guise of necessity to improve user experience, but entities that collect consumer information often sell the data to third parties after deidentifying the information, without analyzing it, highlighting that companies' use of the data is for profit and not out of "necessity." [58]

Businesses frequently collect quantitative and qualitative data without consumer consent. Involuntarily collected data leaves consumers unaware that corporations are collecting, storing, and disseminating information such as websites visited, products bought, genetic information, location information, or environmental data from within a consumer's home,[59] among other things.

Current laws within the United States and abroad emphasize the legality of collecting and disseminating deidentified data without making a distinction between *how* entities obtain information.[60] But it is possible for tech-savvy individuals to reidentify data back to the consumer,[61] rendering the deidentified versus identifiable information mechanism for regulating privacy flawed. Further, consumer consent is impossible for each service because "[t]here are too many entities collecting and using

---

53 *Id.*

54 *See* Annabel Maw, *How Manufacturing Companies Can Benefit from Data Collection*, MFG. BUS. TECH. (Jan. 4, 2019), https://www.mbtmag.com/best-practices/article/13248680/how-manufacturing-companies-can-benefit-from-data-collection [https://perma.cc/756U-K5PS].

55 *Top 10 Personal Data Collection Methods*, INVISIBLY (Feb. 22, 2022, 1:23 PM), https://www.invisibly.com/learn-blog/personal-data-collection-methods [https://perma.cc/Z2K6-CZFU].

56 *Id.*

57 *Id.*

58 *Id.*

59 *See* Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321, 335 (2013) (explaining that consumers are often unaware of technological settings affecting their privacy).

60 *See* CAL. CIV. CODE § 1798.140(v)(1) (West 2024) (describing personal information only as information "reasonably capable of being associated with" the consumer); *see also* Regulation 2016/679, art. 4(1), 2016 O.J. (L 119) 1, 33 (EU) [hereinafter GDPR] (defining personal data as identifiable to the consumer).

61 *See* Barth-Jones, *supra* note 19.

personal data to make it feasible for people to manage their privacy separately with each entity."[62] Relying on privacy notices to inform consumers about what information companies collect is insufficient: "People need a deeper understanding and background to make informed choices. Many privacy notices, however, are vague about future uses of data,"[63] rendering current regulations ineffective. Since organizations seek to shape consumer decisions based on social science insights obtained through collecting and selling consumer information,[64] mandatory protection is essential to prevent further deviation from necessary information privacy. Instead, the law should focus on the relationship between the consumer and their data. We propose reclassifying consumer information into the following three categories: (1) voluntarily given, (2) involuntarily taken, and (3) quasi-voluntary.

1. Voluntary

Voluntarily given information refers to data the consumer actively seeks to have collected and stored. Voluntary information comes in many forms: for instance, a consumer who downloads a fitness application to track their steps or uses a food tracking application to monitor their eating habits. By doing so, the consumer has taken the initiative to have their information collected and saved. They want the data retained in a database so they can look at their historical performance, compare it to others, or publish it on the application. Other examples include survey responses and public social media posts. Ironically, giving people more control over their information leads to more data disclosure.[65] Under the current standard, the consumer's willingness to disclose information puts companies in the strange position of having to keep private or destroy information the consumer requests to remain accessible.

Companies collecting voluntarily given information, whether it is identifiable or not, are not bound by implied contractual terms of data privacy under this Article's proposal. The FTC would classify the collected data and determine which information is voluntary and which data is outside the scope of the contractual terms. Reclassifying such data according to how the consumer associates with the information, rather than whether the data is identifiable, deviates from the current privacy

62 Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1881 (2013).

63 *Id.* at 1885.

64 *Id.* at 1887–88.

65 *See* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1014 (2014).

standard.[66] Voluntarily given information is the only category that businesses can collect and disseminate that falls outside the scope of the implied contractual terms of data privacy.

2. Involuntary

Involuntarily taken data is information businesses collect without consumer knowledge. This data falls within the scope of protection for mandatory implied contractual terms. The involuntary collection of information has increased exponentially with advancing technology.[67] The scope of involuntary data acquisition is vast, including internet history, genetic information, driving speeds, pattern recognition and problem-solving abilities, computer keystrokes, and more.[68] However, the following three categories are particularly alarming and highlight the need for implied contractual terms to enhance privacy protections: (1) web browser tracking, (2) workplace surveillance, and (3) video game tracking.

a. Web Browser Tracking

Cookies for web browsers are a quintessential example of involuntary data. It is difficult to tell where technology will lead, and web browser tracking will likely change in the future. However, cookie tracking is currently a useful tool to analyze how internet tracing technology implicates involuntary data collection. Cookies are embedded text files in an HTTP file that "store data so that a server can be provided with information about the client's settings, past browsing history, authentication, or preferences without the user's needing to reenter the data."[69] Websites often fail to function properly without the user accepting cookies,[70] making it challenging for consumers to manage

---

66 *See* CAL. CIV. CODE § 1798.3(a) (West 2024) (determining that personal information is only identifiable information).

67 *See* Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 CALIF. L. REV. 735, 738–39 (2017) (describing the multitude of ways employers' tracking of employees has increased based on recent technology).

68 *See id.* at 742–43 (analyzing employer-given technology and the employer's ability to track computer data); *see also* Oppenheimer, *supra* note 23, at 387 (discussing how enabling cookies allows companies to see past websites visited); Jacob Leon Kröger, Philip Raschke, Jessica Percy Campbell & Stefan Ullrich, *Surveilling the Gamers: Privacy Impacts of the Video Game Industry*, 44 ENT. COMPUTING, Jan. 2023, no. 100537, at 1, 1–2, 4, 7 (explaining how gaming systems track players' pattern recognition and problem-solving abilities).

69 Oppenheimer, *supra* note 23, at 386–87.

70 *Cookie Consent Exemptions: Strictly Necessary Cookies*, COOKIEYES (Aug. 7, 2023), https://www.cookieyes.com/blog/cookie-consent-exemption-for-strictly-necessary-cookies [https://perma.cc/KPE9-UGY6].

them. By accepting cookies, consumers enable businesses to track how many times the consumer visits the website, the websites the consumer visited before, and how long the consumer spends on the page.[71] Companies argue that consumers voluntarily give cookie consent because the "accept" button is near the privacy policy at the bottom of the webpage.[72] But former FTC Chairman Jon Leibowitz stated, "We all agree that consumers don't read privacy policies,"[73] demonstrating the absence of consumer knowledge of what information businesses record using cookie information. This lack of transparency concerning what consumers are accepting creates dangerous privacy implications.

Implied contractual terms create consumer protection. Hitting "accept" on cookies is the user signing on the dotted line of a contract. Further, companies may use privacy policies as evidence that the consumer waived the right to a private cause of action,[74] proving the contractual nature of the interaction. Accepting cookies on a website should trigger contractual protections like implied terms of good faith. Neither party can alter or delete the terms, regardless of whether the privacy policy expressly includes the provisions. Jon Leibowitz's assertion about consumers not reading privacy policies supports mandating protection for involuntarily taken information like cookies.

b. Workplace Surveillance

Workplace surveillance programs involve expansive data collection processes.[75] Punch cards used to exemplify workplace surveillance, but technology expanded well beyond that.[76] Not only do employers track computer keystrokes, employee cell phones, and some genetic information,[77] companies also store and analyze similar data on

---

71 *See* Calo, *supra* note 65, at 1003.

72 *See* Oppenheimer, *supra* note 23, at 385, 388–89 (detailing how default browser settings accept cookies).

73 Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009, 1012 (2013) (quoting Jon Leibowitz, Chairman, Fed. Trade Comm'n, Introductory Remarks at the FTC Privacy Roundtable (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/introductory-remarks-ftc-privacy-roundtable/091207privacyremarks.pdf [https://perma.cc/AYQ5-7YAT]).

74 *See* Oppenheimer, *supra* note 23, at 391 ("Consent can insulate against civil liability for trespass, invasion of privacy, or battery . . . ."); *see also* Thorin Klosowski, *Here's What You're Actually Agreeing To When You Accept a Privacy Policy*, N.Y. TIMES: WIRECUTTER (Apr. 14, 2023), https://www.nytimes.com/wirecutter/blog/what-are-privacy-policies [https://perma.cc/CGY7-74WK] (explaining that accepting privacy policies implicates agreement to the terms).

75 *See* Ajunwa, Crawford & Schultz, *supra* note 67.

76 *See id.*

77 *See id.* at 742 (explaining that punch clocks have been replaced by thumb scans).

candidates during virtual interviews.[78] Candidates often think giving up personal information is part of the interview process when it is just a gross invasion of privacy. Employees often tolerate surveillance because their jobs depend on it.[79] Although some employees are unaware that their company is tracking them, the law does not require employee consent.[80] When employees do consent, they often have no choice because they may lose their jobs if they fail to comply,[81] demonstrating the involuntary nature of the data disclosure.

Currently, the law entitles employers to track information if the company owns the device,[82] for any purpose the business sees fit. Implied contractual terms help solidify worker privacy. Under this Article's proposal, courts should read implied contractual terms of data privacy into employment agreements, removing employee fear that privacy may cost them their jobs. Further, candidates accepting interviews should have protection when signing up for an interview through the platform that conducts the interview.

c. Video Game Tracking

The video game industry contains over two billion consumers.[83] Arcades used to encompass a vast majority of the industry.[84] However, PC games, consoles, and mobile games have become the dominant form of play.[85] Although gaming covers an array of ages, many gamers are minors.[86] Gaming consoles track minors' voice, heart rate, video, GPS, audio, controller, and play time, among many other data.[87] Such tracking methods are growing as "[m]odern game devices increasingly capture

---

78 *See* Jeffrey Dastin, *Insight—Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, REUTERS (Oct. 10, 2018, 8:50 PM), https://www.reuters.com/article/idUSKCN1MK0AG [https://web.archive.org/web/20231211190425/https://www.reuters.com/article/idUSKCN1MK0AG] (detailing how some companies are analyzing facial expressions and speech in video interviews); *see also* Seth M. Weinberg & John R. Shaffer, *Here's How Genes Determine Your Facial Features*, LIVE SCI. (Dec. 8, 2020), https://www.livescience.com/genes-found-for-facial-features.html [https://perma.cc/P54M-LYNP].

79 Ajunwa, Crawford & Schultz, *supra* note 67, at 741–42.

80 *See id.* at 743.

81 *See* Ifeoma Ajunwa, *Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law*, 63 ST. LOUIS U. L.J. 21, 26 (2018).

82 *See* Ajunwa, Crawford & Schultz, *supra* note 67, at 750.

83 Omri Wallach, *The History of the Gaming Industry in One Chart*, WORLD ECON. F. (Nov. 27, 2020), https://www.weforum.org/agenda/2020/11/gaming-games-consels-xbox-play-station-fun [https://perma.cc/3Z6K-YM6F].

84 *See id.*

85 *Id.*

86 *See* Kröger, Raschke, Campbell & Ullrich, *supra* note 68, at 13.

87 *Id.* at 4.

data from outside the game environment through a variety of embedded sensors."[88] Children use these games without knowledge that gaming companies are collecting their information.[89] And consoles may require such information to function.[90] Therefore, giving up personal information is involuntary when trying to play certain video games, which severely implicates child privacy concerns.

Implied contractual terms cover the purchase of a new game or device. Upon buying a new device, the purchase triggers contractual obligations to mandate that businesses cannot collect and disseminate involuntary consumer data. The overlap between child privacy and gaming illuminates an indispensable need for further protection. Implied contractual terms provide gamers with necessary protections, without hindering the gaming experience.

3. Quasi-Voluntary

Quasi-voluntary data falls between voluntary and involuntary data. Quasi-voluntary information includes data that consumers choose to give because their failure to provide the information significantly disadvantages the individual, and also includes instances where consumers are only partially informed. Quasi-voluntary data falls within the purview of protection under implied contractual terms of data privacy. One example of a partially informed decision includes several permissions in a single request, where the user is unaware that there is more than one permission at stake.[91] An example of a disadvantage instilled on consumers who fail to provide data is Global Positioning System (GPS) information. While consumers can navigate using maps or by memory, traveling anywhere new is burdensome without the location information provided by GPS.

Location information provides more than one piece of data. Nicole Ozer, in reference to *United States v. Maynard*,[92] stated that "aggregated data can disclose far more than the sum of its parts."[93] Expanding on this

---

88 *Id.* at 10.

89 *Id.*

90 *See id.* at 12 (describing the difficulty in getting publishers to reveal which data is necessary for console function).

91 *See* Anjanette Raymond, Jonathan Schubauer & Dhruv Madappa, *After Over-Privileged Permissions: Using Technology and Design to Create Legal Compliance*, 15 J. BUS. & TECH. L. 67, 71 (2019) (explaining the lack of knowledge consumers have when accepting several permissions in a single request).

92 615 F.3d 544, 562 (D.C. Cir. 2010).

93 Nicole A. Ozer, *Putting Online Privacy Above the Fold: Building a Social Movement and Creating Corporate Change*, 36 N.Y.U. REV. L. & SOC. CHANGE 215, 229 (2012).

concept, a trip to a doctor's office tells little information about the individual, but that trip followed by a trip to a cancer clinic tells a different story,[94] one for which insurance companies would be interested in paying. The information gleaned from quasi-voluntary data can be deeply personal. However, courts have held that GPS data is "highly public" information,[95] leading to inconsistent protection.

Enforcing regulations on quasi-voluntary data is necessary. Often, cell phones or vehicles track users' locations.[96] When purchasing a cell phone with default GPS applications downloaded, the purchase agreement should contain implied terms of data privacy the same way a newly downloaded application would. The purchase of a vehicle should include the same agreement, limiting the amount of information companies can obtain through location services that are inherently necessary in society.

B. *Data Dissemination*

Data dissemination has evolved over time, and companies disperse personal information for multiple reasons.[97] Data distribution, then, parallels data science.[98] In an effort to increase efficiency, businesses began selling data to third parties equipped to analyze the information and provide feedback for areas of improvement.[99] Also, data disbursement can revolve around research.[100] But the dawn of the internet caused businesses to expand the scope of personal information disclosures beyond traditional research and efficiency objectives.[101]

---

94 *See Maynard*, 615 F.3d at 560–62 (explaining how the aggregate of the data teaches more than each individual part).

95 *See* Ajunwa, Crawford & Schultz, *supra* note 67, at 30 (citing Elgin v. St. Louis Coca-Cola Bottling Co., No. 05CV970, 2005 WL 3050633, at *4 (E.D. Mo. Nov. 14, 2005)).

96 *See* Anthony Spadafora, *How Your Phone's Location Is Being Tracked—and How to Turn It Off*, TOM'S GUIDE (July 29, 2022), https://www.tomsguide.com/features/how-your-phones-location-is-being-tracked-and-how-to-turn-it-off [https://perma.cc/P34B-5R4B].

97 *See* Thorin Klosowski, *Big Companies Harvest Our Data. This Is Who They Think I Am*, N.Y. TIMES: WIRECUTTER (May 28, 2020), https://www.nytimes.com/wirecutter/blog/data-harvesting-by-companies [https://perma.cc/QV5V-86JY].

98 *See generally* Sarah El Shatby, *The History of Data: From Ancient Times to Modern Day*, 365 DATA SCI. (June 1, 2022), https://365datascience.com/trending/history-of-data/#8 [https://perma.cc/R4NR-7U9N].

99 *See Data Is the New Gold—How and Why It Is Collected and Sold*, USERCENTRICS (Oct. 21, 2021), https://usercentrics.com/knowledge-hub/data-is-the-new-gold-how-and-why-it-is-collected-and-sold [https://perma.cc/M3HL-MN5D].

100 *See* Barth-Jones, *supra* note 19, at 1, 3, 12 (explaining the importance of deidentified medical data for research and statistical analysis).

101 *See Data Is the New Gold—How and Why It Is Collected and Sold*, *supra* note 99.

Targeted advertisements based on internet activity as well as purchase preferences to aid manufacturers in predicting future trends became common practice.[102] However, personal data disclosure to third parties contains serious potential for harm.

Aggregated data discloses more information than the individual parts with.[103] A court determined that visiting a baby store after visiting the doctor gives away pregnancy information that companies could not otherwise obtain without aggregating GPS data by combining a first visit to the baby store with a different visit to the doctor's office.[104] An interested advertiser can buy GPS data from a service provider and display advertisements pertaining to pregnant women before the woman has decided to share that information with friends and family. In one case, this targeted advertising alerted parents that their daughter was pregnant *before* the parents knew, taking the opportunity away from the daughter and demonstrating a significant issue with data disbursement.[105] But companies are not stopping there. Many corporations are trying to advance information dissemination technology. For example, businesses file patents on data dispersion tactics yearly to analyze gamer data to determine real world characteristics of the players.[106]

Third parties have no obligation to inform consumers about how they will use their information.[107] Although some scholars encourage notice and consent requirements,[108] there is an inherent impossibility in consenting to something a consumer cannot fully understand. Third parties can use data for an infinite number of purposes and simply checking a box falls short of consumer consent. Even allowing researchers to obtain data can induce as much harm as allowing a third-party purchaser to do so because of "social engineering experiments" included in psychological assessments made possible through consumer

---

102 *See id.*

103 *See* United States v. Maynard, 615 F.3d 544, 560–62 (D.C. Cir. 2010).

104 *Id.* at 562.

105 Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012, 11:02 AM), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=38aa1c726668 [https://perma.cc/ZB3Q-EXBQ].

106 *See* Kröger, Raschke, Campbell & Ullrich, *supra* note 86, at 8 (describing how U.S. Patent No. 10,357,713 evaluates problem solving, fiscal responsibility, and aggression based on data accumulated during gameplay, among other characteristics).

107 Raymond, Schubauer & Madappa, *supra* note 91, at 84.

108 *See* Scott Jordan, *A Proposal for Notice and Choice Requirements of a New Consumer Privacy Law*, 74 FED. COMMC'NS. L.J. 251, 254–56 (2022) (describing the importance of notice and choice requirements in data privacy).

information.[109] Implied contractual terms would provide a basis for consumer protection that does not require the user to fully (impossibly) inform themselves of how third parties use their data.

C. *Harms*

Privacy harms are difficult to substantiate. Picture a world in which the futuristic, dystopian film *Minority Report*[110] is reality. Law enforcement implements invasive policies to predict crimes that will happen in the future.[111] Although murder ceases to exist, predictive analytics allow police to arrest suspects of crimes that never occurred.[112] What is the harm to the individual whose privacy invasion led to their arrest? There is a plethora of options: loss of freedom, loss of personal autonomy, unauthorized viewing of personal information, invasion of intimate privacy, and the list goes on. In the film, no court tried a single case, as the predictions were final.[113] The film demonstrates clear examples of harm when the party acquiring the data acts. But a more puzzling question arises in the analogous example of companies or third parties, instead of futuristic police, obtaining personal information but taking *no* action. What is the harm to a consumer when a website knows their purchasing history? While the film highlights an interesting concept, the privacy harm implications in the movie do not depart from current reality.

Returning from the (not-so dystopian) future, modern courts struggle to conceptualize privacy harm. Often, courts labor over Article III standing because "standing requires a concrete injury."[114] Thus, courts frequently dismiss privacy cases for lack of standing.[115] But Ryan Calo describes privacy harm as "whatever negative consequences flow from a privacy violation."[116] If courts can construe "negative consequences" as harm, consumers may meet Article III standing requirements. However, consumers perpetuate the difficulty of defining harm because of how

---

109 *See* Kröger, Raschke, Campbell & Ullrich, *supra* note 86, at 12 (quoting Nicolas Ducheneaut & Nick Yee, *Data Collection in Massively Multiplayer Online Games: Methods, Analytic Obstacles, and Case Studies*, *in* GAME ANALYTICS: MAXIMIZING THE VALUE OF PLAYER DATA 641, 641 (Magy Seif El-Nasr, Anders Drachen & Alessandro Canossa eds., 2013)).

110 MINORITY REPORT (20th Century Fox 2002).

111 *Id.*

112 *Id.*

113 *See id.*

114 Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016).

115 *See id.* at 333.

116 Calo, *supra* note 65, at 1028.

often they underestimate the risk of disseminating their data.[117] By undervaluing the risks, consumers allow businesses to collect their information without regard for the consequences. When in court, businesses can then demonstrate that thousands of other consumers were not harmed by their actions, allegedly highlighting the companies' "harmless" data acquisition practices. Standing is a barrier to consumers bringing privacy claims, but as discussed, solutions are available.

Another complication in measuring privacy harm is the often small but numerous injuries.[118] Companies' data practices often cause minute harms to single individuals, but aggregated on a large scale, they affect thousands or even millions of people.[119] Individually, the harm appears minor, but societally, the harm is substantial: "The result makes privacy violations large-scale problems that cause a significant societal impact but do not readily fit into the traditional way the law assesses harm."[120] Private litigation is difficult for individuals in the current regime because aggregating many individual privacy harms is expensive, often requiring class action lawsuits.[121] However, the FTC noted that consumer injuries are sufficient and substantial "if [they do] a small harm to a large number of people, or if [they] raise[] a significant risk of concrete harm."[122] Although privacy harms are difficult to quantify, the FTC has demonstrated a willingness to enforce privacy injuries.

Privacy harms deserve separate classifications. A proposed law attempts to classify harm as "financial, physical, or reputational injury to an individual," "[p]hysical or other offensive intrusion . . . of an . . . individual's private affairs or concerns, where such intrusion would be offensive to a reasonable person," and "[o]ther substantial injury to an individual."[123] However, Daniel Solove proposes four broad categories and sixteen subcategories of harm that better align with consumer interests.[124] The most pertinent category is breach of confidentiality.[125] Breach of confidentiality coincides with implied contractual terms and provides proof that violating implied contractual terms constitutes harm sufficiently worthy of Article III standing.

---

117 *See id.* at 1025.

118 Citron & Solove, *supra* note 20, at 816.

119 *Id.*

120 *Id.*

121 *Id.*

122 *Id.* (quoting FED. TRADE COMM'N, COMMISSION STATEMENT OF POLICY ON THE SCOPE OF THE CONSUMER UNFAIRNESS JURISDICTION, *appended to In re* Int'l Harvester Co., 104 F.T.C. 949, 1073 n.12 (1984)).

123 Consumer Online Privacy Rights Act, S. 3195, 117th Cong. § 101(b)(2) (2021).

124 Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

125 *See id.* at 526–30.

Reclassifying regulated data reduces the risk of harm. While some authors prefer categories of data based on whether the data can reasonably identify the consumer,[126] a voluntary, involuntary, and quasi-voluntary categorization provides a superior grasp of harm. Many laws allow companies to disperse deidentified data.[127] Since deidentified data is reidentifiable,[128] the potential for unknown consumer harm is substantial. As an example of reidentification harm, a third party can reidentify a consumer's credit report and sell it to a potential employer, or an individual can reidentify medical information leading to the disbursement of a patient's home address.[129] Classifying the harm under breach of a contractual duty relating to the voluntariness of the data collection provides improved options for consumers to claim privacy violations because contractual infractions on data collection would predate any unknown harm from deidentified information disbursement. Further, breach of contract claims survive Article III's standing requirements, vastly improving the current system.

D. *Trade-Offs*

With great technology comes great convenience. Phones enable connectivity to distant relatives, video conferencing promotes business, and the internet provides access to answers once buried in libraries.[130] Aspects of life became easier as technology progressed, but technological advancements often require more data to function.[131] The direct correlation between technological improvements and increased data collection inherently creates tension. Expanding data protection may prevent customers from accessing convenient technology.

Too much data protection is as dangerous as no data protection. Daniel Solove and Woodrow Hartzog analogize overprotecting data to limiting cars to fifteen miles per hour and requiring massive foam

---

126 *See* Jordan, *supra* note 108, at 265.

127 *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–.199 (West 2024) (regulating only reasonably identifiable information).

128 *See* Barth-Jones, *supra* note 19, at 5 n.3.

129 *See id.*

130 *See* Max Walker, *Technology's Role in Improving Almost Every Aspect of Our Lives*, INTERCOMMEDIA (Feb. 2, 2022), https://www.intercommedia.org/technologys-role-in-improving-life [https://perma.cc/4H9X-W7HE].

131 *See* Statista Rsch. Dep't, *Data Usage in Marketing and Advertising—Statistics & Facts*, Statista (Jan. 6, 2023), https://www.statista.com/topics/4654/data-usage-in-marketing-and-advertising/#topicOverview [https://perma.cc/Z2RA-CSB7] (describing how target advertisements require knowing what consumers buy, their location, and their name).

bumpers to prevent accidents.[132] But the reduction in accidents is not worth the inconvenience of never driving on a highway.[133] The same reasoning applies when consumers flock to companies like Facebook (now Meta) and Google. Large companies are not attractive for their privacy policies, but for their "fine-tuning and personalization of search and social network services."[134] Unreasonably restricting data collection hinders companies' ability to draw or please customers. Since businesses often operate internationally, restricting free-flowing information across borders may hinder trade.[135]

However, some limitations on data collection and dissemination are necessary. While a great deal of information from a consumer device may enhance their shopping experience, "[t]hese technologies also raise threats to privacy."[136] To prevent cessation of business but maintain convenience, implied contractual terms would mandate that voluntarily given data remain unprotectable. A consumer is free to seek out the convenience of Facebook or Google at their own expense. But employers collecting data on workers and potential candidates involuntarily must abide by implied contractual terms of data privacy. Not only will implied contractual terms protect the employee, but, contrary to widespread belief, limiting involuntarily collected data in the workplace may actually boost efficiency.[137] Therefore, contractual data privacy terms strike a balance between convenience and technological improvements.

II. CURRENT STATE OF REGULATIONS

The United States' data privacy regime is broken. The crippled nature of the current law is a product of varying approaches to privacy regulation. This Part proceeds by examining four crucial aspects of the current regulations. First, a necessary dissection of the multilevel sectoral approach occurs. The second Section evaluates the after-the-fact focus of the law. Third, the target of current laws receives scrutiny for misapplication. The fourth Section highlights the failure of the notice and choice regime.

---

132 SOLOVE & HARTZOG, *supra* note 21, at 70.

133 *See id.*

134 Pasquale, *supra* note 73, at 1014.

135 *See* Anupam Chander & Paul M. Schwartz, *Privacy and/or Trade*, 90 U. CHI. L. REV. 49, 85 (2023).

136 Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2072 (2004).

137 *See* Ajunwa, Crawford & Schultz, *supra* note 67, at 744–45 (explaining that tracking information for compliance may prevent employees from finding better ways to get results).

A. *Sectoral Approach*

The United States lacks a comprehensive federal data privacy law. Instead, the United States incorporates a sectoral approach both geographically and in data category.[138] Like other aspects of data privacy, rapid technological advancements have surpassed the law's ability to keep pace. The federal government relies on states to enact comprehensive laws, of which California and Illinois are among the leaders.[139] But Congress has enacted laws to regulate technology sectors such as health care information and credit reporting.[140] Although advocacy groups "proposed statutory text for a comprehensive consumer privacy law,"[141] the current state of the law remains fragmented.

1. Geographic

Geographically distinct privacy laws pose innate difficulties. According to the California Consumer Protection Act of 2018 (CCPA),[142] only personal data warrants protection under the law.[143] The CCPA describes personal data as information that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with particular consumer or household."[144] Thus, a limitation of the CCPA is the lack of coverage for deidentified data obtained involuntarily from the consumer, even though Daniel Barth-Jones has highlighted technological savvy citizens' ability to reidentify data.[145] Although California's data privacy law is consistently considered the best among the states,[146] lobbying from some of the many

138 *See* Asay, *supra* note 59, at 325 (stating that the United States has implemented several sectoral laws that target specific industries).

139 Casey Leins, *States with the Strongest Online Privacy Protections*, U.S. NEWS (Oct. 23, 2019, 2:24 PM), https://www.usnews.com/news//best-states//articles//2019-10-23//states-with-the-strongest-online-privacy-laws [https://perma.cc/J3JL-DRN8].

140 *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of the U.S. Code); Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x.

141 Jordan, *supra* note 108, at 257.

142 CAL. CIV. CODE §§ 1798.100–.199 (West 2024).

143 *Id.* § 1798.140(v)(1) (defining what data warrants protection).

144 *Id.*

145 Barth-Jones, *supra* note 19.

146 Leins, *supra* note 139.

tech companies in California led to "weakening the definition of 'de-identified data,'"[147] causing further difficulties within the state.

State laws are not created equal. Illinois defines personal information in the Personal Information Protection Act (PIPA) differently than the CCPA.[148] "Personal Information," according to PIPA, requires association between an individual's first name or initial to a list of six other pieces of information.[149] Many companies in California also operate in Chicago. The lack of unanimity between state definitions of personal information imposes major restrictions on businesses. Companies must change their practices in each state depending on the geographical privacy law. But the connectivity of consumers to corporations makes business difficult where a California consumer seeks to voluntarily give personal information to an Illinois-operated company. Difficult legal questions, such as which state law applies, which geographic law businesses should follow, and how businesses track which state the information comes from, arise when conducting multistate business. Each legal inquiry hinders a company's efficiency because the business must spend time and resources to find a solution. A comprehensive federal law like mandatory implied contractual terms would unify the law and prevent geographic distinctions.

2. Data Category

Beyond the geographic approach lies the equally problematic data category option. Federal law narrowly applies to certain fields and "if the company doesn't fall within an often-narrow scope of sectoral coverage, the law is inapplicable to their activities."[150] Common examples include the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[151] and the Fair Credit Reporting Act (FCRA).[152]

Congress did not intend HIPAA and the FCRA to protect consumer privacy. HIPAA was created to "to improve portability and continuity of health insurance coverage."[153] Although HIPAA provides secondary data privacy protections to "'covered entities' such as health plans, health care

147 Salomé Viljoen, *The Promise and Pitfalls of the California Consumer Privacy Act*, DIGIT. LIFE INITIATIVE @ CORNELL TECH (Feb. 19, 2021), https://www.dli.tech.cornell.edu/post/the-promise-and-pitfalls-of-the-california-consumer-privacy-act [https://perma.cc/CPJ3-QHBK].

148 *See* 815 ILL. COMP. STAT. § 530/5 (2024).

149 *See id.*

150 Raymond, Schubauer & Madappa, *supra* note 91, at 90.

151 Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of the U.S. Code).

152 15 U.S.C. §§ 1681-1681x.

153 Pub. L. No. 104-191, 110 Stat. 1936 (preambulatory language).

providers, and health care clearinghouses," Apple Watch health data and location services are not covered.[154] The tangential privacy concerns within HIPAA do little to protect the involuntarily obtained health and location information stored on user-wearable technology. The FCRA also lacks sufficient data privacy protections: "[T]he FCRA only protects . . . private . . . information contained within the files of consumer reporting agencies."[155] Federal sectoral laws are inadequate because they are "incredibly limited in scope—thereby leaving a large swath of individuals who fall outside these situations and environments unprotected."[156] Implied data privacy affords broader protection to consumers because it would apply to all data categories.

Senators have proposed legislation for a comprehensive data privacy law. Senator Maria Cantwell introduced the Consumer Online Privacy Rights Act (COPRA) in 2021,[157] but the Senate has refused to take any further action as of early 2024. However, the Act covers only "information that identifies, or is linked or reasonably linkable to an individual,"[158] leading to the same problems demonstrated in state law. Another weakness of the Act is mandating consent.[159] While consent appears productive, users rarely read privacy statements,[160] making the Act toothless.

But the Act is not entirely unusable. COPRA properly puts regulation within the authority of the FTC.[161] Congress has not reviewed the Act in three years and will likely drag its feet (highlighting the slow pace of the law). However, aspects of the Act fit neatly within of the framework of implied contractual terms of data privacy. An important facet of implied contractual terms is FTC enforcement. Although the Act is unlikely to pass soon, COPRA proposes important enforcement mechanisms.

B. *After-the-Fact Focus*

Current "[d]ata security law jumps in at the wrong time."[162] Often, geographic and data category laws inflict punishment after a data breach

154 Raymond, Schubauer & Madappa, *supra* note 91, at 91.

155 *Id.*

156 *Id.*

157 S. 3195, 117th Cong. (2021).

158 *Id.* § 2(8)(a).

159 *See id.* § 2(1) (requiring consent from the consumer).

160 Pasquale, *supra* note 73, at 1012.

161 S. 3195 § 301(a).

162 SOLOVE & HARTZOG, *supra* note 21, at 77.

occurs.[163] Since companies are underregulated in how they collect data, businesses store millions of pieces of information on consumers that are ripe for data breaches.[164] But because regulators and courts struggle to determine privacy harm, victims are rarely made whole when a data breach occurs.[165] And too many data security failures occur each year for regulators to pursue every company responsible for improperly protecting consumer information.[166] Consumers need an enforcement mechanism to secure their privacy before a breach manifests.

Proposed legislation fails to solve the after-the-fact focus. Senator Roger Wicker has sponsored the SAFE DATA Act,[167] which has remained untouched by Congress in the past three years. The Act attempts to provide real-time control of privacy policies by mandating a privacy officer for each covered entity.[168] The Act's data privacy officer requirement seems promising but is insufficient. The complex nature of privacy imposes an impossible task on a single privacy officer to preemptively avoid harmful data collection practices. Also, the privacy officer is unlikely to tell consumers they can sue the company for the business's privacy violation. But promisingly, the Act states that the FTC will be responsible for enforcing any violations.[169] The failure of the SAFE DATA Act is that FTC regulation would only occur *after* a violation likely to lead to a data breach. Including implied contractual terms would mandate data privacy before a breach occurs because the initial agreement between the consumer and the business provides baked-in privacy protection.

Breach of implied contractual terms would occur before a data breach. If a company collects involuntary consumer data, the company would have to delete the data within a reasonable time. If the company's practice violates the terms, the company would be subject to liability before someone hacks their servers. This proposal would allow for consumers to bring a cause of action *before* a violation of another law occurs, such as a data breach or unlawful dissemination to a third party. Because even deidentified data stored on a server can pose dangers to consumers,[170] it is important to prevent businesses from dispensing all

---

163 *See* CAL. CIV. CODE § 1798.150 (West 2024) (describing a private cause of action available to consumers who have been subject to unauthorized disclosure).

164 Dylan Curran, *Are You Ready? Here Is All the Data Facebook and Google Have on You*, THE GUARDIAN (Mar. 30, 2018, 3:17 PM), https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy [https://perma.cc/4CYY-X52U].

165 *See* SOLOVE & HARTZOG, *supra* note 21, at 8.

166 *Id.*

167 S. 2499, 117th Cong. (2021).

168 *Id.* § 301.

169 *Id.* § 401.

170 *See* Barth-Jones, *supra* note 19.

involuntary and quasi-voluntary information. Although the proposed legislation is insufficient, both the SAFE DATA Act and COPRA correctly identified the FTC as the regulating body. The FTC holds jurisdictional power to regulate contractual terms.[171] Within the proposal for implied contractual terms exists the ability for the FTC to audit data privacy practices for compliance.

C. *Wrong Target*

The current regime wrongfully exacts punishment on only one party. As Solove and Hartzog note, "The law loves to pummel the breached organization," but "many actors . . . contribute to data breaches."[172] Software developers create unreliable products, manufacturers produce unsecured devices, ad platforms host malicious ads, and the list goes on.[173] As noted by Natalie Kim, "One criticism of a liability regime where the data controller solely bears the blame is that it excessively burdens data controllers and fails to incentivize third parties to adopt and follow adequate privacy practices."[174] Privacy laws targeting just the company collecting the data provide insufficient protection for consumers.[175]

Geographic and data category laws focus solely on the entity collecting the information. For example, the CCPA focuses on one entity.[176] Although considered the most protective data privacy law,[177] the CCPA enables a consumer to bring a private cause of action against a *business* that has violated the duty to implement reasonable security procedures.[178] The law defines business in a manner that excludes software developers and data collection technology creators.[179] HIPAA also provides a narrow scope of enforcement. HIPAA enforces action on

---

171 *See* Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (detailing the FTC's jurisdiction to regulate unfair and deceptive trade practices).

172 SOLOVE & HARTZOG, *supra* note 21, at 77.

173 *Id.* at 77–78.

174 Natalie Kim, Note, *Three's a Crowd: Towards Contextual Integrity in Third-Party Data Sharing*, 28 HARV. J.L. & TECH. 325, 343–44 (2014).

175 SOLOVE & HARTZOG, *supra* note 21, at 78.

176 *See* CAL. CIV. CODE § 1798.150 (West 2024).

177 Leins, *supra* note 139.

178 § 1798.150.

179 *See id.* § 1798.140(d)(1) (describing a business as needing to meet $25 million in annual gross revenues in the preceding calendar year; buy, sell, or share 100,000 or more consumers' personal information; or "[d]erive[] 50 percent or more of its annual revenues from selling or sharing consumers' information").

health care providers but does nothing to provide protection against the technology developers that create a risk of exposing health information.[180]

Proposed legislation also misses the mark. COPRA provides for an annual privacy risk assessment "and other quality control practices."[181] The internal nature of a privacy risk assessment focuses only on the company collecting data, keeping other responsible parties outside the scope of liability. COPRA does, however, propose an option for internal or external auditing for algorithm-based decisions.[182] But the bill creates no mechanism for enforcing safe data practices by software developers or other third-party developers of algorithm-based technology,[183] just for the company implementing the technology. Mandatory implied contractual terms would dictate interactions between consumers and businesses, but also between developers and businesses. Therefore, implied contractual obligations would force developers to create systems that provide data privacy, lest the businesses have a cause of action against the developers.

The mechanism for potential data privacy enforcement against third parties exists. The FTC possesses authority to enforce data privacy laws against third parties.[184] The FTC's ability to regulate "unfair or deceptive acts or practices in or affecting commerce"[185] puts it in a position to protect consumer privacy used in commerce, which Congress defines broadly.[186] The FTC has pursued enforcement actions against data brokers,[187] demonstrating that the agency, in limited circumstances, actively protects consumer privacy. But since there are so few data privacy regulations, companies that collect and disseminate data are often not acting unfairly or deceptively in the eyes of the law. There exists a need for implied terms of data privacy to bring current businesses' harmful practices, such as the development and implementation of data collection technology, within the reach of the FTC.

---

180 Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320a–7e).

181 Consumer Online Privacy Rights Act, S. 3195, 117th Cong. § 202(b)(2) (2021).

182 *Id.* § 108(b)(2).

183 *See id.*

184 *See* Kim, *supra* note 174, at 329.

185 15 U.S.C. § 45(a)(1).

186 *See* Gibbons v. Ogden, 22 U.S. (9 Wheat.) 1 (1824) (describing Congress's ability to regulate commerce).

187 *See* Kim, *supra* note 174, at 329–33.

D. *Notice and Choice*

Notice and choice proposals provide a flawed consumer privacy framework. Solove argues that, "[i]n some cases, privacy law should move beyond relying so heavily on consent."[188] Most information privacy laws that exist in the United States, although they are few and far between, require businesses to provide consumers with notice of privacy policies and for users to have a choice to opt in or opt out.[189] Scott Jordan's analysis of the CCPA and the European General Data Protection Regulation (GDPR)[190] determined that "[t]he notice requirements in these two options have proven to be insufficient to provide consumers the information necessary to make informed choices about their use of services and applications."[191]

Solove has detailed the shortcomings of the American notice-and-choice system. Simply stated, if the consumer fails to opt out of having their data collected, then the individual has consented.[192] Thus, the notice-and-choice regime places the responsibility on the consumer to dig into *every* privacy notice they encounter and decide whether they want to proceed.[193] For involuntarily collected information, the current system places the responsibility of affirmatively opting out of each data gathering service onto the user, otherwise they have consented in the eyes of the law. To make matters worse, reading privacy notices is arduous, resulting in "a remarkably low percentage of people opt[ing] out,"[194] which allows companies to use consumers' information because the notice-and-choice regime fails to provide inherent protection that implied contractual information privacy would provide. Although the notice-and-choice policy is broken, "about a dozen states have enacted consumer privacy laws. All primarily involve posting a notice about the sale of personal data to third parties or the sharing of personal data for targeted advertising and then providing people with a right to opt out."[195]

State laws exemplify a broken notice and consent system. The CCPA requires businesses to inform consumers as to the categories of personal information the business will collect and the purpose for collecting such

188 Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593, 637 (2024).

189 Jordan, *supra* note 108, at 254.

190 GDPR, *supra* note 60.

191 Jordan, *supra* note 108, at 254.

192 Solove, *supra* note 188, at 600.

193 *Id.*

194 *Id.* at 602.

195 *Id.*

information.[196] Consent for the CCPA exists insofar as consumers have a right to delete data that they do not want stored.[197] But there exists no protection against companies couching privacy terms in a twelve-page document that no user will ever read.[198] However, when accepting terms "[i]n the tort context, '[c]onsent means that the person concerned is in fact willing for the conduct of another to occur.'"[199] Consumers' lack of awareness of what provisions are in privacy policies, meant to give them notice, only enables consumers to unknowingly waive private causes of action against businesses. Implied contractual terms of data privacy would avoid the issue of unknowing consent because of the unchangeable nature of the obligation.

Proposed legislation minimally changes this dynamic. The SAFE DATA Act limits a business's right to transfer "covered data" or process "sensitive covered data" of the consumer without prior consent.[200] But the SAFE DATA Act takes small steps to prevent privacy policies burying important information.[201] The Act requires, among other elements, "a prominent heading that would enable a reasonable individual to easily identify the processing purpose for which consent is sought."[202] While a prominent heading improves the chances a consumer sees the information, it remains unlikely that a consumer will read the statement, let alone fully understand what consenting to data dissemination entails.

Global data regulations also provide flawed consent requirements. The GDPR requires affirmative consent, which "requires a clear voluntary indication of consent"[203] that is more restrictive than the United States' notice-and-choice system because failure to opt out does not automatically opt the consumer in like it does in the United States.[204] In order for companies to collect customer information, the company must comply with a permissible purpose under the GDPR.[205] However, express consent is only one of multiple permissible purposes for organizations to collect private information, rendering consent

196 CAL. CIV. CODE § 1798.100(a)(1) (West 2024).

197 *Id.* § 1798.105.

198 *See* Pasquale, *supra* note 73, at 1012 (quoting the former FTC chairman about the lack of consumers reading privacy statements).

199 Oppenheimer, *supra* note 23, at 390 (second alteration in original) (quoting RESTATEMENT (SECOND) OF TORTS § 892 cmt. b (AM. L. INST. 1979)).

200 SAFE DATA Act, S. 2499, 117th Cong. § 104(a) (2021).

201 *See id.* § 104(b) (explaining the requirements for consent that are heightened as compared with various state laws).

202 *Id.* § 104(b)(3).

203 Solove, *supra* note 188, at 602.

204 *See id.* at 600.

205 *Id.* at 602–03.

effectively optional.[206] Therefore, even though the regulation is widely regarded as the most rigorous among data privacy laws,[207] it still possesses similar problems to the notice-and-choice system because of the large number of permissible purposes for which businesses can collect information while remaining GDPR-compliant.

Mandatory contractual terms avoid notice and consent issues. Solove posits the solution of "murky consent."[208] This Article goes beyond "murky consent" to enact a solidified policy to protect consumers from involuntary and quasi-voluntary information collection and dissemination. Inherent contractual terms in every agreement between: (1) technology developers and businesses, (2) businesses and third parties, and (3) businesses and consumers, would provide protection without requiring that the business, or the consumer, read lengthy legal contracts to know their rights. Good faith is mandatory in both common law and under the Uniform Commercial Code.[209] Parties cannot contract around the duty of good faith and the law does not require good faith in writing.[210] Comparing implied contractual terms of data privacy against the implied duty of good faith reveals that consumers would not need to read the privacy agreements for the law to afford protection, deviating from the notice-and-choice regime. While the implied duty of good faith remains distinct from implied duty of data privacy, the principles remain the same and grant the consumer protection without the need for notice and consent.

III. SUPPORT FOR IMPLIED CONTRACTUAL TERMS

Various sources support implied contractual terms of data privacy. Statutes, case law, government agency authority, and scholars offer legal reinforcement for the implementation of contractual terms. This Part

---

206 *See id.* ("The GDPR recognizes six lawful bases: (1) consent of the data subject; (2) processing is necessary to the performance of a contract to which the data subject is a party; (3) processing is necessary to comply with a legal obligation; (4) processing is necessary to protect the vital interests of the data subject or another person; (5) processing is necessary to perform a task carried out in the public interest; and (6) processing is necessary for the controller's legitimate interests or those of a third party.").

207 *See id.* at 603 (noting that "[e]xpress consent is one of the strictest forms of consent in privacy laws").

208 *See id.* at 598 (describing "murky consent" as a set of fictions because while it appears to provide consent, it lacks legitimate enforcement).

209 U.C.C. § 1-304 (AM. L. INST. & UNIF. L. COMM'N 2022); *see* ev3, Inc. v. Lesh, 114 A.3d 527, 539 (Del. 2014) (stating that companies are obligated to act in good faith).

210 *See* Katie Shonk, *How to Negotiate in Good Faith*, HARV. L. SCH.: PROGRAM ON NEGOT. (Sept. 4, 2023), https://www.pon.harvard.edu/daily/business-negotiations/negotiate-good-faith [https://perma.cc/ZM8C-FE5S].

analyzes six aspects of support for an implied duty of data privacy. First is the regulation of implied contractual terms by the FTC. Second, current precedent, based on case law and statutes, supplies an initial foundation for contractual terms. Third, this Part proffers support for a cause of action before a data breach occurs. Fourth, implied contractual terms reinforce data minimization principles. Fifth, statutory precedent provides for expanding the liable parties for privacy violations. Lastly, this Part puts forth a clear strategy for implementing mandatory implied contractual terms for data privacy.

A. *Federal Trade Commission Regulation*

The FTC is the regulatory authority for consumer privacy. While the FTC has governed consumer privacy for quite some time,[211] the public has paid little attention. The historical development of the FTC's authority illuminates how the FTC is suited to regulate implied contractual terms of data privacy and show why the FTC is still the best option for data privacy enforcement.

Congress has granted the FTC the authority to regulate unfair and deceptive trade practices.[212] While this explicit congressional authority does not include the authority to regulate privacy policies, the FTC has "long had authority (since 1970) to enforce [the] FCRA, which was passed to ensure that consumer reporting agencies respected consumers' privacy. But until the late 1990s, few other privacy laws granted the FTC new enforcement powers."[213] Thus, the FTC's regulatory ability over privacy matters was born.[214] The FTC's ability to enforce the FCRA expanded its authority to ensure security and confidentiality of customer records and to protect consumers from unauthorized access to their information.[215] Legal scholars Daniel Solove and Woodrow Hartzog describe the boom in privacy regulation by the FTC, stating the following:

> Thus, between 1995 and 2000, the FTC jumped into the privacy regulatory space in a dramatic way, acquiring new power with each passing year. As the FTC began to enforce [the Children's Online Privacy Protection Act] and [the Gramm-Leach-Bliley Act] it largely

211 *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585 (2014) (describing how the FTC has enforced consumer privacy for more than fifteen years).

212 15 U.S.C. § 45(a)(2).

213 Solove & Hartzog, *supra* note 211, at 602 (footnote omitted).

214 15 U.S.C. § 45(a)(2).

215 *Id.* at 602–03.

> followed the same model as the notice-and-choice regime it relied upon to enforce its general Section 5 powers.[216]

The FTC in the early 2000s became the dominant body of governance in the consumer privacy space. But many legal scholars are skeptical of the FTC's authority in this realm, because, despite years of FTC enforcement, there are hardly any judicial decisions to show for it.[217]

Even absent judicial opinions recognizing the FTC as the primary data privacy regulation agency, the FTC continues to grow its authority: "Over the past fifteen years, the FTC has gradually accumulated territory and power. It developed a body of doctrines one by one in a form that most legal academics do not pay much attention to."[218] The FTC began privacy policy oversight through its congressionally granted powers and started filing complaints against businesses for privacy concerns under the umbrella of "unfairness."[219] However, because the FTC can only enforce Federal Trade Commission Act violations or infringements, the FTC lacks the ability to create substantive privacy protections.[220] Because the FTC cannot create substantive doctrines, there exists an unmet need for implied contractual terms of data privacy in every agreement. The FTC does not need to develop the law, but the FTC clearly possesses authority to enforce it. While the FTC can enforce new privacy laws, resources at the agency are not abundant.

The lack of FTC resources leads to questions about whether they can handle every data privacy matter. Recently, the FTC announced that they employ roughly forty employees to oversee privacy and data security.[221] Although a limited number of employees comprise the information security division of the FTC, the existence of a data privacy division for more than fifteen years demonstrates a willingness, and the requisite authority, to enforce privacy laws.[222] The purpose of the division is "to 'address [] cutting-edge consumer privacy matters through aggressive

---

216 *Id.* at 604. The section 5 powers referenced in the article refers to the general authority of the FTC to regulate deceptive and unfair trade practices. *See id.* at 602; *see also* 15 U.S.C. § 45.

217 Solove & Hartzog, *supra* note 211, at 585.

218 *Id.* at 606.

219 *Id.* at 599.

220 *Id.*

221 *See* Harper Neidig, *FTC Says It Only Has 40 Employees Overseeing Privacy and Data Security*, THE HILL (April 3, 2019, 11:01 AM), https://thehill.com/policy/technology/437133-ftc-says-it-only-has-40-employees-overseeing-privacy-and-data-security [https://web.archive.org/web/20221206230416/https://thehill.com/policy/technology/437133-ftc-says-it-only-has-40-employees-overseeing-privacy-and-data-security]; *see also* Solove & Hartzog, *supra* note 211, at 600–01 (detailing the Department of Labor statistics showing only 46 employees were working in the privacy divisions of the FTC in 2011).

222 *See* Solove & Hartzog, *supra* note 211, at 601 (explaining that the FTC created the Division of Privacy and Identity Protection in 2006).

enforcement, as well as rulemaking, policy development, and outreach to consumers and business.'"[223]

Despite limited resources for data privacy, the FTC can assess serious penalties. The FTC has previously enforced privacy violations on large companies like Google.[224] However, a $22.5 million fine is a small price for a company earning almost $40 billion in revenue in the same year.[225] But, as of 2020, these penalties have grown up to the $5 billion levied on Facebook for its sharing of personal information,[226] showing the FTC has teeth to enforce data privacy. Beyond monetary penalties, the FTC audit process is one companies want to avoid. The process is long and expensive for businesses,[227] which alone may deter companies from maintaining unreasonable consumer privacy policies. The FTC can demand the following:

> [T]he specific detailing of the agreed-upon safeguards to protect consumer information; an explanation of "how such safeguards are appropriate to the respondent's size and complexity, the nature and scope of the respondent's activities, and the sensitivity of the covered device functionality or covered information"; an explanation of "how the safeguards that have been implemented meet or exceed the protections" agreed upon in the consent order; and a certification of the effectiveness of the company's protections by "a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession."[228]

Relating back to implied contractual terms of data privacy, the FTC's auditing policy aligns with the requirement of a reasonable standard and whether the company obtained the information involuntarily. The auditing process often ends with a consent order requiring the company to perform specific tasks in order to become compliant, demonstrating the ability of the FTC to enforce proposed data privacy solutions.

The FTC remains the best option: "FTC settlements are viewed by the community of privacy practitioners as having precedential weight. Privacy lawyers routinely use FTC settlements to advise companies about

---

223 *Id.* (alteration in original) (quoting *Social Security Numbers in Commerce: Reconciling Beneficial Uses with Threats to Privacy: Hearing Before the Subcomm. on Com., Trade & Consumer Prot. of the H. Comm. on Energy and Com.*, 109th Cong. (2006) (statement of Jon Leibowitz, Chairman, Fed. Trade Comm'n), https://www.govinfo.gov/content/pkg/CHRG-109hhrg29388/html/CHRG-109hhrg29388.htm [https://perma.cc/84EE-VVCZ]).

224 *Id.* at 605.

225 *Id.* at 605–06.

226 FED. TRADE COMM'N, *supra* note 44, at 3.

227 *See* Solove & Hartzog, *supra* note 211, at 606 (describing the audit process as lengthy, demanding, and exhaustive).

228 *Id.* (quoting *In re* HTC Am. Inc., No. 122-3049, 2013 WL 3477025, at *11 (F.T.C. 2013)).

how to avoid triggering FTC enforcement."[229] Not only do their settlements carry legal weight, but the FTC can also mandate companies to implement programs designed to address privacy concerns, develop and manage new and existing products and services, and protect consumers' personal information.[230] In addition to forcing companies to comply, the FTC also mandates the deletion of involuntarily obtained data,[231] which is the crux of implied contractual terms of data privacy. Further, once the FTC steps in, they continue to regulate compliance: "Virtually every company that settled with the FTC agreed to engage in some kind of regular recordkeeping to facilitate the FTC's enforcement of the order."[232] Therefore, the FTC remains the best option for enforcement because they can deliver damaging punishments that carry precedential weight, force policy changes within a business, and continue to monitor that company for compliance.

B. *Current Precedent*

In order to fully understand how current case law and statutes align with the adoption of implied contractual terms of data privacy, we must first explore how contractual legal principles move from ideas to implied terms in all contracts. This Section proceeds by first exploring how the commonly accepted doctrines of good faith and unconscionability worked their way into the Uniform Commercial Code (U.C.C.) as mandatory terms in every contract for the sale of goods. The second portion of this Section analyzes how current precedent supports data privacy terms as the next good faith or unconscionability doctrine to get codified.

1. Historical Support

The historical development of good faith illuminates a path for implied terms of data privacy. Implied contractual terms of good faith demonstrate a quintessential example of justice arriving in American jurisprudence through values and adaptation of commonsense principles. While good faith was not always codified as an implied

229 *Id.* at 621.

230 *Id.* at 618.

231 *Id.* at 616–17.

232 *Id.* at 618.

contractual protection, the U.C.C. eventually included good faith as a mandatory implied term for contracts involving the sale of goods.[233]

Historically, good faith principles were based on what was reasonable and fair.[234] After centuries of use in legal opinions around the world,[235] the American legal system still had not codified the principle. However, Samuel Martin summarizes the American adoption of good faith by stating the following:

> While good faith was not a completely foreign concept in early American contract law, and one would be hard-pressed to find a court decision stating that no level of good faith is necessary between contracting parties, it was not included in the first Restatement of Contracts, which was published in 1932. At least through the early 20th century, the United States' jurisprudence echoed England's on the matter. In 1933 however, good faith made its first dramatic appearance in the 1933 case *Kirke Le Shelle Co. v. Paul Armstrong Co* [sic], and 19 years later it was codified in the Uniform Commercial Code.[236]

Common law contracts for services reflected the codification of good faith for the sale of goods in the U.C.C. Originally, good faith claims were ancillary to other breach of contract claims and could not provide footing to state a claim.[237] However, courts grew more accepting of good faith violations and began to allow a breach of good faith to give rise to a cause of action.[238]

A claim for data privacy violations mirrors that of the early legal understanding of good faith. A sense of what is unreasonable and unfair is palpable when analyzing situations where large businesses take advantage of consumers by storing their location when they are

---

233 U.C.C. § 1-304 (AM. L. INST. & UNIF. L COMM'N 2022).

234 *See* Samuel Martin, The Evolution of Good Faith in Western Contract Law 1–2 (June 13, 2018) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3177520 [https://perma.cc/F937-G7DM]. Samuel Martin describes Roman jurisprudence allowing parties to assert good faith, which enabled the judges to use equitable discretion to decide cases before them "in accordance with what appeared to be fair and reasonable." *Id.* at 2 (quoting Simon Whittaker & Reinhard Zimmermann, *Good Faith in European Contract Law: Surveying the Legal Landscape*, *in* GOOD FAITH IN EUROPEAN CONTRACT LAW 7, 16 (Reinhard Zimmermann & Simon Whittaker eds., 2000)). Martin further explains that "fair and reasonable" are the grounds on which the good faith doctrine developed. *See id.* at 2 (quoting Whittaker & Zimmermann, *supra*, at 16).

235 *See* Bürgerliches Gesetzbuch [BGB] [Civil Code], § 242, https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html#p0742 [https://perma.cc/RQ89-R9LH] (Ger.); *see also* Martin, *supra* note 234, at 1–2 (citing Roman law as using good faith in their legal analysis).

236 Martin, *supra* note 234, at 12 (footnotes omitted) (citing Kirke La Shelle Co. v. Paul Armstrong Co., 188 N.E. 163 (N.Y. 1933)).

237 *See id.*

238 *See id.* at 12–13.

commuting to work,[239] keeping sensitive information on minors,[240] and using virtual hiring as a way to save biological information.[241] Courts in criminal contexts turn to the constitutional right of privacy when police use consumer cell site information against a suspect.[242] However, courts are increasingly mentioning data privacy, similar to historical opinions that included principles of good faith without explicitly labeling the reasoning under a doctrine of good faith.[243] Following the development of good faith doctrines, a codification of underlying principles of data privacy based on a sense of what is reasonable and fair to the consumer is inevitable. As happened with the U.C.C., if Congress passes context-dependent legislation for data privacy, common law will likely follow suit as it did with the adoption of good faith from goods in the U.C.C. context to services under the common law. And the codification of good faith is an example of how courts and legislatures can comfortably adopt mandatory implied contractual terms. Further, codification can enable consumers to bring a private cause of action for data privacy that can stand alone.

Codifying a legal principle requires meticulous and precise language. This Article does not propose the specific language required, but only proposes the guidelines for such language by drawing from the definition of good faith. Good faith, like data privacy, is not definitionally all-encompassing. Good faith is not an inclusive term, but an excluder term.[244] It rules out various things according to context, similar to how privacy is not an inclusive term, but one that rules out various bad behaviors by companies.[245] It would be impossible to include all definitions of good faith. In coming to this conclusion, the U.C.C. drafters looked to leading contractual case law at the time in New York and California that made decisions highlighting bad faith.[246] Similarly, legislators can look to California's consumer privacy legislation as leaders in data privacy for examples of information privacy violations.[247]

---

239 *See* Ajunwa, *supra* note 81, at 30.

240 Kröger, Raschke, Campbell & Ullrich, *supra* note 68, at 13.

241 *See* Dastin, *supra* note 78 (including facial expression analysis during interviews); *see also* 740 ILL. COMP. STAT. 14/10 (West 2024) (excluding photographs from biometric data but leaving the possibility of videos being considered biometric data).

242 *See, e.g.*, United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).

243 *See* Martin, *supra* note 234, at 12.

244 Robert S. Summers, *The General Duty of Good Faith—Its Recognition and Conceptualization*, 67 CORNELL L. REV. 810, 818 (1982).

245 *See id.*

246 *Id.* at 812.

247 *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–.199 (West 2024).

Defining data privacy as an excluder sufficiently passes legislative muster. The definition of good faith under the U.C.C. includes a reasonableness requirement.[248] A reasonableness standard for good faith looks at the circumstances and context in order to determine what qualifies. A definition of data privacy that also includes reasonableness excludes unreasonable behavior but does not propose an all-inclusive list of what constitutes proper data security. Therefore, including a level of reasonableness in the definition of data privacy as an excluder is sufficient to withstand legislative scrutiny like the good faith definition did many years ago.[249]

Prominent legal scholars believe that codifying good faith embodied vast case law and symbolized "a commitment to the most fundamental objectives a legal system can have—justice."[250] Data privacy, then, expands on the constitutional right to privacy, which provides fundamental protections to all U.S. citizens. Further, before the codification of such an important principle like good faith, judges fictionalized the law to provide equitable remedies.[251] While the concern for data privacy is relatively new, there exists a risk that courts will start to interject their own equitable remedies in this area and begin to fictionalize the law to provide protections for information privacy that expand on the right of privacy that the Constitution already provides.

Another prominent legal premise originating in reason and fairness is the doctrine of unconscionability.[252] Unconscionable terms include provisions that are so unfair to one party that the court can step in and render the agreement invalid.[253] Similar to the development of good faith, courts employed unconscionability reasoning to strike down contracts before the U.C.C. codified the principle.[254] The development of the unconscionability doctrine mirrors the development of consumer data privacy in many respects. However, unconscionability took centuries to develop,[255] and the rapid pace of technological development forces the

---

248 U.C.C. § 1-201(b)(20) (AM. L. INST. & UNIF. L. COMM'N 2022).

249 Summers, *supra* note 244, at 821.

250 *Id.* at 811.

251 *Id.* at 813.

252 *See* U.C.C. § 2-302 (AM. L. INST. & UNIF. L. COMM'N 2022) (describing the ability of courts to render contracts void if they are unconscionable).

253 *See id.*

254 *See* Charles L. Knapp, *Unconscionability in American Contract Law: A Twenty-First Century Survey*, *in* COMMERCIAL CONTRACT LAW: TRANSATLANTIC PERSPECTIVES 309, 309–12 (Larry A. DiMatteo, Qi Zhou, Severine Saintier & Keith Rowley eds., 2013).

255 Per Gustafsson, The Unconscionability Doctrine in U.S. Contract Law 6–7 (Fall 2010) (L.L.M. thesis, Lund University), https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=1761847&fileOId=1764250 [https://perma.cc/6W2D-VNEW].

law to act quicker in the context of data privacy in order to protect U.S. citizens.

The District of Columbia Court of Appeals decision in *Williams v. Walker-Thomas Furniture Co.*[256] exemplifies unconscionability and how legislation for data privacy can follow suit. In *Williams*, a furniture store allowed customers to purchase items on installment plans.[257] Title to the goods would remain with the furniture company until the customer paid the entire purchase price.[258] But each new item purchased would encumber all previous items.[259] In the event of default, the furniture store could repossess all the purchased items.[260] When deciding the agreement was unconscionable, the court of appeals determined that the court possessed the authority to deem the agreement so unfair to the customer as to render the agreement void (even though the court had not addressed the unconscionability question).[261] The court reasoned that "when a party of little bargaining power, and hence little real choice, signs a commercially unreasonable contract with little or no knowledge of its terms, it is hardly likely that his consent, or even an objective manifestation of his consent, was ever given to all the terms."[262] Companies collecting, storing, and selling consumer information offer similarly unfair agreements, albeit for data privacy instead of repossession, as did the furniture company in *Williams*. The customer has no choice but to accept the terms in both scenarios. Courts can adopt data privacy rulings like the *Williams* court adopted unconscionability. Courts possess authority to render a contractual judgment based on equity in contract disputes, allowing data privacy concerns to guide judicial decisions. Lastly, the *Williams* court concluded that the U.C.C.'s adoption of the unconscionability doctrine was just a codification of the existing case law.[263] The court's reasoning demonstrates a pathway for data privacy to become the next mandatory implied contractual term. Modern cases are starting to recognize the need for consumer privacy protection, similar to the protection *Williams* provided against unconscionability. Legislators can look to the development of the unconscionability doctrine to guide them in codifying data privacy.

Codification of implied data privacy provisions can parallel unconscionability. Unconscionability developed through courts finding

256 350 F.2d 445 (D.C. Cir. 1965).

257 *Id.* at 447.

258 *Id.*

259 *Id.*

260 *Id.*

261 *Id.* at 448.

262 *Id.* at 449.

263 *Id.* at 448–49.

an "absence of meaningful consent [sic]" and "terms unduly [sic] favorable to one [sic] party."[264] Many information privacy cases involve parties consenting to data collection or storage through involuntary means. Absence of meaningful consent and unduly favorable terms ultimately led to the unconscionability doctrine's integration into the U.C.C. Whether contractual terms appeared in plain language or were located in conspicuous places also played a role in the development of the doctrine.[265] An illustrative similarity between unconscionability and data privacy is that unconscionability developed through "[s]ome required disclosure of various terms that were typically obscured or hidden entirely."[266] The deceptive practices of some parties allowed judges to overrule the sale of goods in these special contexts. In the case of adhesion contracts, where there were little to no options for bargaining and negotiating, courts found that such contracts were procedurally unconscionable.[267]

The development of data privacy is similar to that of unconscionability. Hiding terms in long privacy policies, using confusing and complex language, and making consumers search for particular provisions has parallels in the rationale for the development of the unconscionability doctrine. Adhesion contracts bear remarkable similarities to requiring accepting cookies or using a GPS in order to use a website or app. The consumer has no bargaining power and must accept the terms to use the product. Thus, the logical progression from the current state of allowing companies to collect information from unknowing consumers is statutory protection for consumers.

Similar to the definition of good faith, the U.C.C. defines unconscionability broadly.[268] Case law also discussed the idea of unconscionability without specifically mentioning unconscionability.[269] Many constitutional violations of privacy are not specific to consumer privacy, but still play major roles in solidifying the need for etching data privacy into implied contractual terms.[270] Like good faith, there is not an all-encompassing definition of what unconscionability is, but rather it is left to the courts to define its metes and bounds.[271] Legislation need not define data privacy, which would allow the law to sweep in future

264 Knapp, *supra* note 254, at 311–12 (quoting *Williams*, 350 F.2d at 449).

265 Gustafsson, *supra* note 255, at 17.

266 Knapp, *supra* note 254, at 313.

267 *Id.* at 320–21.

268 *See* U.C.C. § 2-302(1) (AM. L. INST. & UNIF. L. COMM'N 2022).

269 *See, e.g.*, Henningsen v. Bloomfield Motors, Inc., 161 A.2d 69, 86 (N.J. 1960).

270 *See* United States v. Maynard, 615 F.3d 544, 555 (D.C. Cir. 2010).

271 *See* Gustafsson, *supra* note 255, at 13 (explaining that the unconscionability determination is for the court, not the jury).

developments in information gathering techniques and technologies, like it did for good faith and unconscionability.[272]

The obvious question remains: If unconscionability is broad, it covers skewed data privacy practices, right? Unfortunately, that is not the case. Legal researchers have conducted various federal- and state-level studies to determine the effectiveness of an unconscionability claim.[273] A study of federal cases determined that approximately one out of every three cases claiming unconscionability succeeded.[274] State-level success was drastically lower, and in some states even dipped as low as four percent.[275] The failure of courts to enforce unconscionability demonstrates a need for a separate doctrine for data privacy. And unconscionability claims often act as shields, when consumers facing information privacy violations need a sword.[276] While the development of unconscionability illustrates a path for codifying data privacy, there are obvious pitfalls that leave consumers severely disadvantaged.

2. Present Support

Requiring implied contractual terms aligns with the spirit of domestic and foreign data privacy law. A long-standing interpretation of the Fourth Amendment "is to protect people's right to privacy."[277] Although the Fourth Amendment typically stands for the right to privacy from governmental entities,[278] the concepts of data privacy overlap with the Constitution's original contemplation of privacy. Courts have reviewed the right to privacy in the context of data collection practices and have held for the consumer.[279] Congress has also enacted statutes that offer some data privacy protection, demonstrating Congress's ability to enforce a law like mandatory terms of data privacy.

Current United States case law aligns with contractual privacy terms. Earlier, we argued that GPS data is classified as quasi-voluntary. The

---

272 *See id.* at 11.

273 *See* Brian M. McCall, *Demystifying Unconscionability: A Historical and Empirical Analysis*, VILL. L. REV. 773, 789–92 (2020).

274 *Id.* at 789–90 (finding a roughly thirty-seven percent success rate at the federal level for unconscionability claims by merchants).

275 *Id.* at 790–91.

276 *See* Gustafsson, *supra* note 255, at 15.

277 *Fourth Amendment*, CORNELL L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/fourth_amendment [https://perma.cc/UBB6-ZMYA] (discussing the Fourth Amendment right to privacy as being historically viewed as protection from governmental search and seizures).

278 *See id.*

279 *See* Carpenter v. United States, 585 U.S. 296, 321 (2018) (holding for a consumer whose cell site location was obtained illegally).

Supreme Court in *Carpenter v. United States*[280] determined that a government entity seeking GPS data from a service provider, used to establish his location during the commission of a crime, violated the defendant's Fourth Amendment right to privacy.[281] While the holding in *Carpenter* narrowly focuses on GPS data obtained by the government, the principle of consumer data privacy is prevalent in the opinion.[282] The defendant did not voluntarily give the GPS data, a fact that the Court found was sufficient to warrant protection.[283] Implied contractual terms align with mandating protection for quasi-voluntarily given information, similar to the holding in *Carpenter*.

A D.C. Circuit case provides an example of case law reinforcing implied terms of data privacy. *United States v. Maynard* also involves GPS data.[284] The facts are similar to *Carpenter v. United States*, but the reasoning the court used in *Maynard* highlights the data privacy implications with broader scope.[285] The court reasoned that "[the] whole reveals more . . . than does the sum of its parts."[286] In other words, aggregating data informs companies about consumers on too detailed a level. Thus, providing mandatory contractual terms aligns with the holding in *Maynard* by limiting the amount of data businesses collect, reducing the harm of aggregating data.

Statutes also support implied contractual terms of consumer privacy. The CCPA hints at contractual terms when referring to deidentified information. Scott Jordan summarizes how the CCPA takes contractual terms a step further than the FTC mandates, stating:

> The third legal control in the FTC Report is that if a business makes de-identified information available to other companies, it must "contractually prohibit such entities from attempting to re-identify the data." This legal control ensures that the direct recipient of de-identified information doesn't re-identify the information. The CCPA takes this a step further, requiring that a business possessing de-

280 585 U.S. 296.

281 *Id.* at 310 (holding that historical cell site location information, obtained without a warrant, from a consumer device admitted into evidence in a criminal trial was a breach of the defendant's right under the Fourth Amendment).

282 *See* de Zayas, *supra* note 49 (arguing that the narrow holding in *Carpenter* needs to be expanded because the privacy implications are narrow in scope but have the ability to apply to other situations).

283 *Carpenter*, 585 U.S. at 310.

284 615 F.3d 544, 555 (D.C. Cir. 2010).

285 *See id.* at 568.

286 *Id.* at 558.

> identified information "[c]ontractually obligates any recipients of the information to comply with all provisions of this subdivision."[287]

The CCPA demonstrates how contractual terms fit within the folds of consumer privacy. Instead of mandating companies to create new contracts that require third parties to comply, a contractual provision built into every exchange easily covers the CCPA's goals.

Proposed legislation supports the mandatory nature of contractual privacy terms. COPRA states that "[a] covered entity shall not condition the provision . . . to an individual on the individual's agreement to waive privacy rights."[288] The Act supports unwaivable terms of data privacy by refusing to allow companies to contract around privacy provisions, like terms of good faith.

Foreign privacy policy reinforces implied consumer privacy laws. The GDPR specifically refers to contracts within the law.[289] Often considered the pioneer of consumer privacy, the GDPR provides staunch support for contractual terms governing data privacy. The GDPR states that "[t]he carrying-out of processing by a processor should be governed by a contract . . . setting out . . . the type of personal data and categories of such data subjects."[290] Contractual terms are an important piece of the GDPR and support requiring implied obligations of data privacy. Forcing data security into every contract prevents ambiguous language and avoids courts needing to construe each company's privacy policy. Therefore, the solution to many data privacy problems neatly aligns with U.S. case law, statutes, and foreign privacy standards.

C. *Cause of Action Before Breach*

FTC enforcement of implied contractual terms fixes the after-the-fact focus: "A better strategy would be to focus on the optimal time to intervene in the life cycle of a cybersecurity incident. Sometimes that will be before the incident . . . and sometimes this will be . . . before a risk of harm manifests itself."[291] The enabling statute for the FTC, and

---

287 Jordan, *supra* note 108, at 320 (footnote omitted) (first quoting FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 21 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/8HA4-44AG]; and then quoting CAL. CIV. CODE § 1798.140(m)(3) (West 2024)).

288 Consumer Online Privacy Rights Act, S.3195, 117th Cong. § 109 (2021).

289 GDPR, *supra* note 60, recital 81, at 16.

290 *Id.*

291 SOLOVE & HARTZOG, *supra* note 21, at 79.

interpretations by privacy scholars, indicates support for FTC enforcement before a data breach occurs.

The statute creating the FTC, the Federal Trade Commission Act (FTCA),[292] highlights the FTC's ability to enforce contractual terms before a data breach. Congress granted the FTC authority to regulate unfair trade practices affecting commerce.[293] Data collection and dissemination often produce income for companies, falling within the realm of trade. And the FTCA explicitly states that "[s]uch relief may include, but shall not be limited to, rescission or reformation of contracts."[294] Under the FTCA, regulation of deceptive behavior to avoid contractual obligations is within the FTC's purview.[295] Although the major questions doctrine mandates that the FTC only regulates what Congress has authorized it to,[296] Congress has specifically stated that contracts are within FTC power.[297] As part of the solution, the FTC can audit companies' data collection and dissemination practices for compliance. If businesses are not complying, the FTC possesses the authority to reprimand a company before a data breach occurs for deceptive trade practices.[298] So, adding an auditing function fits within Congress's contemplation of FTC authority.

Privacy scholars also call for a cause of action before a data breach: "The FTC should work with data controllers to set minimum contracting standards with subcontractors and other third parties and ensure that such requirements are represented to the public as part of a controller's privacy policy."[299] Requiring contractual terms allows consumers to bring a claim when a company is in breach of the privacy policy, which may come before a data breach occurs. Another scholar posits that the law should equip consumers with the ability to bring a private right of action against "companies anywhere along the chain of information distribution" and that "the FTC and state attorneys general would have

---

292 Federal Trade Commission Act, 15 U.S.C. §§ 41–58.

293 *Id.* § 45(a)(1).

294 *Id.* § 57b(b).

295 *Id.*

296 *See* West Virginia v. EPA, 597 U.S. 697, 724 (2022). In *West Virginia v. EPA*, the Court analyzed the scope of a governmental agency's authority under the major questions doctrine to determine the EPA's authority in regulating a system of emission reduction. *Id.* at 716. The major questions doctrine requires "Congress to speak clearly if it wishes to assign to an agency decisions of vast economic and political significance." *Id.* (quoting Util. Air Regul. Grp. v. EPA, 573 U.S. 302, 324 (2014)).

297 John Newman & Amy Ritchie, *Contract Terms That Impede Competition Investigations*, FED. TRADE COMM'N (June 16, 2023), https://www.ftc.gov/enforcement/competition-matters/2023/06/contract-terms-impede-competition-investigations [https://perma.cc/8QZ5-827H].

298 15 U.S.C. § 45f(a)(3)–(4).

299 Kim, *supra* note 174, at 344.

the ability to enforce the law."[300] Implied terms force responsibility on each party, from technological conception to implementation, and can enable a consumer to bring a claim against any party in violation of the terms. Strict liability for violation of contractual terms "obviates proving fault, and the vast repositories of personal data that are being maintained about people can be analogized to . . . ultrahazardous activities."[301] Violating implied contractual terms may not impose strict liability, but the principle of forcing cessation of "ultrahazardous activities" aligns with the idea behind mandating such terms.

D. *Data Minimization*

Enacting a reasonable time standard for companies to dispose of consumer data strikes a necessary balance between businesses and individuals. Businesses need some consumer information to produce an effective product.[302] Implied terms of data privacy will not hinder a company from gathering required information. It would afford businesses a reasonable time to analyze the data and then delete involuntary and quasi-voluntary information. Proposed legislation and policy scholars agree that data minimization within a reasonable time is necessary.[303]

COPRA proposes a reasonable time standard and a right to data minimization.[304] The Act limits businesses' authority to "process or transfer covered data beyond what is reasonably necessary."[305] COPRA further requires deletion of data that served its intended purpose, unless consumer consent was given to retain such data.[306] While the Act requires data minimization within a reasonable time, the data minimization provision requires consumer consent,[307] which companies can easily bury in the privacy policies. Thus, COPRA shows support for the idea of data

---

300 Asay, *supra* note 59, at 351.

301 Citron & Solove, *supra* note 20, at 862.

302 *See* Bernard Marr, *How to Understand Your Customers and Their Needs with the Right Data*, FORBES (Feb. 3, 2022, 1:37 AM), https://www.forbes.com/sites/bernardmarr/2022/02/03/how-to-understand-your-customers-and-their-needs-with-the-right-data/?sh=359bae1f2f68 [https://perma.cc/F6CE-S7DU] (stating that understanding consumer behavior is one of the most powerful features of data and helps keep companies on the cutting edge).

303 *See* Consumer Online Privacy Rights Act, S. 3195, 117th Cong. § 106 (2021); *see also* Arushi Gupta, Victor Y. Wu, Helen Webley-Brown, Jennifer King & Daniel E. Ho, *The Privacy-Bias Tradeoff: Data Minimization and Racial Disparity Assessments in U.S. Government*, 2023 FACCT: PROC. ACM CONF. ON FAIRNESS, ACCOUNTABILITY & TRANSPARENCY 492.

304 S. 3195 § 106.

305 *Id.*

306 *Id.* § 107(b)(3).

307 *Id.* § 106(2).

minimization but fails to provide any real bite. Nonetheless, the Act displays the importance of mandating such data minimization practices, which implied contractual terms of data privacy accomplish by requiring the deletion of involuntary and quasi-involuntary information.

Privacy scholars call for data minimization. Legal scholars often represent a public policy outcry.[308] Implicating privacy for minors, an article states, "video games have been described by psychology and data science researchers as 'rich natural laborator[ies],' 'ideal test bed[s] to collect and study data related to human behavior,' and 'social engineering experiments that can generate a goldmine of behavioral data.'"[309] Industry experts consider the amount of information collected extraordinarily high.[310] Involuntarily given data from gaming demonstrates the overwhelming need to cut down on how much information companies store. Paul Schwartz offers a solution that requires heightened software design that minimizes data acquisition.[311] But a change to technological design may cost companies millions of dollars to revamp their products. Implied contractual terms would allow a company to collect and analyze involuntary and quasi-involuntary data for a reasonable time before permanently deleting the data. Thus, implied terms provide a happy medium to companies and consumers but still promote data minimization.

Mandatory data privacy blends COPRA and privacy scholars' concerns. While COPRA fails to remove the consumer consent requirement, the proposed solution stands for the proposition that companies collect too much data. Further, privacy scholars highlight the implications of overcollecting and storing information, with some calling for drastic technological changes to promote data minimization.[312] Implied terms governing consumer data exchanges would better protect individuals than COPRA because the terms are mandatory. Implied data

---

308 *See Law and Public Policy*, STAN. L. SCH., https://law.stanford.edu/education/degrees/joint-degrees-within-stanford-university/law-public-policy [https://perma.cc/54QJ-A9EW] (stating that "law is a major instrument of public policy").

309 Kröger, Raschke, Campbell & Ullrich, *supra* note 86, at 12 (citations omitted) (first quoting Rita M. Bush, *Preface* to PREDICTING REAL WORLD BEHAVIORS FROM VIRTUAL WORLD DATA, at vii, vii (Muhammad Aurangzeb Ahmad, Cuihua Shen, Jaideep Srivastava & Noshir Contractor eds., 2014); then quoting Zahid Halim, Muhammad Atif, Ahmar Rashid & Cedric A. Edwin, *Profiling Players Using Real-World Datasets: Clustering the Data and Correlating the Results with the Big-Five Personality Traits*, 10 IEEE TRANSACTIONS ON AFFECTIVE COMPUTING 568, 568 (2019); and then quoting Nicolas Ducheneaut & Nick Yee, *Data Collection in Massively Multiplayer Online Games: Methods, Analytic Obstacles, and Case Studies*, *in* GAME ANALYTICS, *supra* note 109, at 641, 641).

310 *Id.*

311 *See* Schwartz, *supra* note 136, at 2105–06.

312 *See, e.g.*, *id.*

privacy also addresses privacy scholars' concerns without costing companies extreme amounts of money to retool their products.

E. *Expanding Liable Parties*

Current law allows for the expansion of liable parties without undue legislative overhaul. Although Solove and Hartzog contend that "[t]he law needs to expand its scope to hold more actors accountable for data breaches,"[313] current FTC authority enables the enforcement of implied contractual terms against third parties. And public policy demands third party liability.

The FTCA supports third party responsibility. The FTC has the power to "gather and compile information concerning, and to investigate from time to time the organization, business, conduct, practices, and management of *any* person, partnership, or corporation engaged in . . . business [that] affects commerce."[314] The FTCA grants the FTC authority over third parties, supporting the ideology behind implied contractual terms. The FTC can hold third-party technology developers—including the businesses who implement the technology—liable for violations of the mandatory terms of data privacy.

Public policy requires expanding responsible parties: "The current notice-and-choice model gives consumers too little control and accessibility when it comes to third-party data sharing."[315] But implementation of "[a] comprehensive consumer privacy law may apply to a broader class of entities than businesses."[316] Implied privacy terms would provide a comprehensive data security law that expands the scope of liable parties. Further, scholars such as Anjanette Raymond have contemplated FTC enforcement of responsible party expansion.[317] Although Raymond seeks a notice-and-choice regime,[318] the important aspects of the public policy outcry for expanding responsible parties through FTC enforcement remain eminent. Implied contractual terms of data privacy fit within the metes and bounds of both public policy and FTC enforcement.

---

313 SOLOVE & HARTZOG, *supra* note 1, at 78.

314 15 U.S.C. § 46(a) (emphasis added).

315 Kim, *supra* note 174, at 341.

316 Jordan, *supra* note 108, at 315.

317 *See* Raymond, Schubauer & Madappa, *supra* note 91, at 105 ("The FTC could stipulate provisions that require companies to provide consumers with a third-party recipient list before a company shares [personally identifiable information] with its third-party vendors.").

318 *See id.* at 88–89.

F. *How to Implement?*

Multiple paths are available for implementation. Although proposed legislation amending the U.C.C. is desirable (if not crucial), enacting legislation is difficult. Case law could slowly implement an implied contractual obligation of data privacy, and the FTC can enforce such rulings. This Article has discussed at length the FTC's authority over contractual terms affecting commerce. This Article further described how the FTC would enforce mandatory implied contractual terms of data privacy. However, an explicit roadmap will provide a clearer picture of implementation, whether it be statutory or through common law.

We propose the following implementation procedures: The FTC would review privacy policies before company implementation. At the discretion of the FTC, companies tracking consumer information must submit privacy policies to the FTC before enacting a data collection practice. The FTC's review of privacy policies will look to whether the policy implements the requirements of mandatory implied contractual terms of data privacy—that is, whether the company deletes involuntarily and quasi-involuntarily collected data. The FTC can then make their review of the privacy policy publicly available. Although the reviewing process will not include technology developers, courts could still hold those third parties liable to consumers for product creation that violates the implied contractual terms of data privacy.

Further, the FTC would perform periodic audits. To ensure continued compliance, the FTC may perform periodic audits of companies that collect user information and the technology the companies implement. These audits assure that companies comply with contractual terms and allow the FTC to observe the technology implemented by such companies. Enabling the FTC to analyze the technology used for data collection allows the agency to hold third-party technology developers liable for breaches of the implied contractual terms of data privacy.

IV. RESPONDING TO CRITICS

There are three anticipated criticisms to the implementation of mandatory implied contractual terms of data privacy. The first is whether there is a real mechanism of enforceability through the FTC. The second is that implied terms of data privacy are the same as the already mandatory obligation of good faith. The third criticism is that businesses' interactions with consumers are not contracts, thus making the proposal moot. In this Part, we show that (1) the FTC possesses authority to

regulate data privacy policies, (2) companies can comply with good faith and fair dealing and still violate consumer data privacy interests, and (3) there exists a contractual relationship whenever buying a product or clicking "accept."

A. *Enforceability*

Some scholars may question the ability of the FTC to enforce data privacy obligations. Because the FTC may only regulate "[u]nfair methods of competition in or affecting commerce,"[319] there is a question whether data privacy "affects commerce." Also, the scope of the FTC is not unlimited.[320] Therefore, not only must implied contractual terms "affect commerce" but they must also fall within Congress's intended purpose for the FTC.

The FTC has viewed data privacy issues before: "[T]he FTC has charged a company with unfair trade practices when its security and privacy policies markedly diverged from industry standards."[321] Also, the FTC issued a rule containing recommendations for businesses regarding data privacy.[322] The rule implicates, the FTC's desire to enforce consumer privacy.[323] A summary of the rule and FTC trends states:

> [T]he FTC took two meaningful actions that signaled the FTC's desire to expand its role in setting and enforcing cybersecurity and data privacy standards: the FTC clarified the scope of the often ignored HBN Rule and the FTC amended the Safeguards Rule to strengthen the data security requirements for financial institutions.[324]

Although the two actions involve health information and financial institutions, the proposition remains sound that the FTC can enforce consumer privacy. Moreover, data dissemination affects commerce because companies profit from the distribution.[325] Further, Congress

---

319 15 U.S.C. § 45(a)(1).

320 *See, e.g.*, AMG Cap. Mgmt., LLC v. F.T.C., 593 U.S. 67 (2021). .

321 Pasquale, *supra* note 73, at 1016.

322 *See* Standards for Safeguarding Customer Information, 86 Fed. Reg. 70272 (Dec. 9, 2021) (codified at 16 C.F.R. 314).

323 Alexander Boyd & Jessica L. Peel, *Tech Transactions & Data Privacy 2022 Report: The FTC's Expanding Role in Cybersecurity and Data Privacy Enforcement in 2022*, NAT'L L. REV. (Feb. 9, 2022), https://www.natlawreview.com/article/tech-transactions-data-privacy-2022-report-ftc-s-expanding-role-cybersecurity-and [https://perma.cc/R2S6-FG66]. .

324 *Id.*

325 *See* Klosowski, *supra* note 97 (describing data brokers selling consumer information).

specifically demonstrated the desire for FTC power to enforce consumer privacy in proposed legislation in COPRA and the SAFE DATA Act.[326]

FTC enforcement is inevitable and allowable. Mandatory implied contractual terms of data privacy fall within the scope of the FTC, and some legal scholars recognize the need for FTC enforcement: "The [FTC] has filled the statutory vacuum to lead the development of regulations in the online privacy space."[327] Therefore, although there are certainly questions about the FTC's ability to enforce data privacy rights, those concerns are diminutive in the face of statutory and legislative history.

B. *Good Faith and Fair Dealing?*

There is an argument that good faith subsumes any implied duty of consumer privacy. But companies can operate in good faith while still disseminating consumer information. For example, a business can give consumer medical data, often deidentified, away for research purposes. Hospitals may use the research to try to predict and cure future diseases. But businesses can also give consumer information away for a less noble purpose. A company can give data to researchers to determine targeted advertising, which has proven harmful to consumers.[328] What determines if one dissemination practice abides by good faith? The inquiry becomes difficult, but consumers should decide whether they want their data disseminated based on whether they voluntarily give their data up. Data privacy thus exists separately from the duty of good faith.

Businesses may also analyze data in good faith. Companies may need to analyze consumer information to provide a better product. The collection practice falls outside the scope of good faith because companies rarely collect data in bad faith, even though the practice may harm the consumer.[329] Therefore, there exists a need for a separate body of law to protect consumers' data interests.

---

326 *See* Consumer Online Privacy Rights Act, S. 3195, 117th Cong. § 301 (2021); SAFE DATA Act, S. 2499, 117th Cong. § 401 (2021).

327 Kim, *supra* note 174, at 328; *see also* Solove & Hartzog, *supra* note 211, at 585.

328 *See* Hill, *supra* note 105.

329 *See* Ellyn Shook, Eva Sage-Gavin & Susan Catrall, *How Companies Can Use Employee Data Responsibly*, HARV. BUS. REV. (Feb. 15, 2019), https://hbr.org/2019/02/how-companies-can-use-employee-data-responsibly [https://perma.cc/N5V6-RD6W] (highlighting the positive uses of employee data that would not qualify as bad faith).

C. *Are These Contracts?*

A final criticism of implied contractual terms is that clicking "accept" on cookies in a web browser, using a GPS app, or buying some technology does not warrant contractual protection: "Although privacy notices look similar to a contract, courts have still not yet held consistently that they are contracts, and to this day, it is notable how few cases have directly addressed the issue."[330] However, courts throughout modern American history support the enforcement of nontraditional contracts found in hyperlinks and terms buried deep within the bowels of a privacy policy.[331]

Nancy Kim supplies the strongest support for the interactions between consumers and businesses as contractually binding. Kim details the development of contract law to the digital age by stating the following:

> "Courts eventually recognized the shrinkwrap license as a legitimate contract, which paved the way for courts to recognize the legitimacy of other innovative contracting forms, such as the clickwrap (which the user assents to by clicking on an icon indicting agreement) and the browsewrap (which is a hyperlink to a webpage containing legal terms which a user assents to by continuing to use the site after notice of the terms)."[332]

The terms "clickwrap" and "browsewrap" encapsulate the online agreements consumers enter into when visiting a website or accepting the terms of a virtual interview. Kim notes that "[c]ourts have approved clickwrap agreements, finding that a 'click' accepts the terms contained on the website, even if the terms are viewable only through a hyperlink."[333] Thus, there is legal support for a contractual relationship between the consumer and the business regarding data privacy. And not only do consumers not read the privacy policies, but businesses also create the agreements expecting the consumers not to read them,[334] leading to companies hiding terms in the interior page that consumers can only access by clicking on a hyperlink at the bottom of the web page.[335]

---

330 Solove, *supra* note 188, at 601.

331 *See* Nancy S. Kim, *Contract's Adaptation and the Online Bargain*, 79 U. CIN. L. REV. 1327 (2011) (detailing how shrinkwrap and clickwrap contracts developed into enforceable contracts throughout the twentieth century).

332 *Id.* at 1328–29 (footnote omitted).

333 *Id.* at 1336.

334 *Id.* at 1328; *see also* Pasquale, *supra* note 73, at 1012 (quoting the former FTC chairman stating that consumers do not read privacy statements).

335 Kim, *supra* note 331, at 1337.

Kim also explains the general acceptance of online contracts and the benefits provided to the companies implementing them. Mass-market contracts, similar to privacy policies, "differ[] from traditional contracts because their terms [are] non-negotiable and offered to the consumer on a 'take it or leave it' basis."[336] But "despite their shortcomings," Kim notes, "courts and commentators generally recognize[] that standard form agreements [are] efficient and, to varying degrees, socially beneficial."[337] Although Kim is referencing mass agreements for the sale of goods, location services, privacy policies, and company data, retention policies are often included in the same agreements. In order to use a product, a consumer has to agree to those terms and allow companies to collect their information in an agreement that courts consider binding, and that often protects only the company.

Kim demonstrates how enforcing these agreements as contracts is detrimental to consumers. First, companies use form agreements as a shield.[338] But, "[g]iven the blanket nature of contractual assent, . . . acceptance of the shielding [of companies] meant acceptance of the provisions that served functions other than shielding."[339] Once courts began enforcing arbitration provisions from assent through "clicking accept," companies shifted from "shielding" themselves to using the agreements offensively. Companies set the boundaries of the contracts, and courts were abiding by the terms. Kim discusses how the acceptance of hidden terms regarding consumer privacy moved the function from shielding companies from liability to offensively selling and profiting from the terms in the form agreements that consumers accept with just a click.[340] As the dynamic shifted from defensive to offensive, consumers became unprotected in their data privacy rights and often felt deflated once they became aware of what they agreed to: "Most consumers are likely unaware of the rights granted via these [hidden] provisions since most consumers fail to read online agreements. More troubling, at least some consumers would have declined the primary transaction if they had known about the additional benefits being extracted via the [hidden] provisions."[341] Consumers would almost certainly rethink accepting cookies or using a particular headset when playing video games had they known what information they were agreeing to disclose beforehand. An agreement that companies use as a

336 *Id.* at 1333.

337 *Id.*

338 *Id.* at 1337–38.

339 *Id.* at 1339.

340 *Id.* at 1343.

341 *Id.* at 1342–43 (footnote omitted).

sword to profit off the consumer and that courts already find contractual in nature reveals the binding quality of the interaction.

A predominant assumption throughout this Article is that consumers are not reading the terms when clicking accept and that they should have implied data privacy protections when doing so. However, support for a contractual arrangement between businesses and consumers still exists when the consumer does read the policy. Imagine this hypothetical contract: A cookie policy is hyperlinked next to the accept button. The hyperlink takes the consumer to a seventy-page document outlining the terms of acceptance. As previously discussed, courts enforce "browsewrap" agreements as contracts.[342] On page forty-three, a provision states that there is no contractual agreement between the consumer and the business. The consumer reads the policy. What are the chances they picked up on this so-called noncontractual acceptance?

As Shmuel Becher and Uri Benoliel note, "In the context of consumer contracts, scholars have warned that the language firms employ in their standard form contracts is incomprehensible and abstruse."[343] Consumers reading such polices miss valuable information found in "an onslaught of words[] or present[] . . . in awkward and non-user-friendly forms. Such practices prevent consumers from reading and understanding their contracts and, thus, undermine contractual transparency."[344] Legal scholars conducted a study that found 498 out of 500 contracts received a readability score lower than the recommended score for consumers to understand the conditions.[345] The difficulty for consumers is that if the privacy policy stated that it was not a contract, customers reading the policy would likely miss that and not understand that they are not protected, even when the agreement seems like a contract.

Further, companies constantly change privacy and data policies: "Firms frequently change terms in their consumer contracts, even after consumers accept them."[346] When companies update terms and conditions, "firms often make the original contract inaccessible after unilaterally modifying it, so consumers cannot view the original version they accepted."[347] And another study concluded that 98.54% of term

342 *See id.* at 1336.

343 Shmuel I. Becher & Uri Benoliel, *Dark Contracts*, 64 B.C. L. REV. 55, 61 (2023).

344 *Id.* at 61–62 (footnotes omitted).

345 *Id.* at 62.

346 *Id.* at 67.

347 *Id.* at 63.

changes did not require consumers' active assent to such changes,[348] in addition to the consumer not being able to see what had changed. Not only would consumers struggle to understand that the hyperlinked terms would not create a contract, but, if the terms changed, the consumer would likely be unaware.

The difficulty of reading, and the ever-changing nature of these agreements, support a contractual relationship. If consumers read an entire document and still have a high probability of misunderstanding provisions, then courts should still enforce these "browsewrap" agreements like they have been doing for years,[349] but with the added protection of implied terms of data privacy. Further, changing provisions without consumer consent warrants protection for the consumer from sophisticated businesses through implied terms of data privacy.

The rise of mass-produced goods and widespread internet use greatly complicated traditional notions of contract formalities. In fact, legal scholars see "[c]ontract law's stance on private party control over enforcement . . . as incoherent."[350] Form agreements with obscure provisions online render legal analysis of consideration difficult to determine. But "being in a digital 'contract' does not hearken back to a bilateral, legal relationship commitment based on a signature, but rather an imposition and a click."[351] Therefore, legal scholars like David Hoffman and Zev Eigen appear to support the proposition that a consumer hitting the "accept" button creates a legally binding contract.[352] Not only is there support for the notion that online agreements are contracts, but Hoffman and Eigen go on to explain why consumers need those agreements to bind the consumer and the business.

Online agreements change consumer behavior: "Online legalese presents an especially complex behavioral story. Likely because everyone has long acknowledged—and now we all know—that no one reads form contracts."[353] Not only are consumers clicking accept and binding themselves to things like arbitration, sale of their personal information, and choice of law, but consumers are changing their behavior after doing so: "Differences in norms of contracting online and offline thus matter in predicting and understanding consumer behavior—both before and after

348 *See id.* at 67 (finding that a study of 479 consumer contracts revealed that 472 of the contracts included provisions that allowed the company to change the terms of the agreement without consumer consent).

349 *See* Kim, *supra* note 331, at 1336.

350 David A. Hoffman & Zev J. Eigen, *Contract Consideration and Behavior*, 85 GEO. WASH. L. REV. 351, 395 (2017).

351 *Id.* at 393.

352 *See id.* (stating that an online agreement may create a legal relationship with just a click).

353 *Id.* at 355–56 (footnotes omitted).

an online exchange transpires."[354] The change in consumer behavior demonstrates that people believe they are accepting something when they click "accept all cookies" and they know there is an agreement when they "accept the terms and conditions" for a GPS application, but oftentimes the "online legalese" prevents consumers from knowing exactly what it is they agreed to. The consumer's belief that they have entered into a contract supports the notion that involuntarily and quasi-voluntarily given information creates a contractual relationship.

From a public policy perspective, if every "accept" waives the right to bring suit for web browser tracing,[355] then there is support that there is a contractual relationship between the consumer and the business. Downloading an application requires accepting the terms and conditions in the same way that accepting cookies does. And because consumers are not reading privacy statements,[356] there exists an unmet need to enforce the privacy policy as a contractual agreement.

Further, privacy enforcement is available through breach of fiduciary duty claims.[357] However, establishing a breach of fiduciary duty is historically difficult.[358] Fiduciary duty claims highlight the fact that there is a contractual agreement, but also display the difficulty the consumer faces when attempting to bring a claim that the company violated a "special obligation[]" to the consumer.[359] Mandating data privacy terms, like terms of good faith, alleviates the need for a "special obligation." Therefore, a contractual relationship exists between consumer and business, but implied contractual terms of data privacy would provide a more accessible solution to consumers.

CONCLUSION

The law consists of numerous gaps that allow businesses to misuse consumer information. Companies may collect and disseminate data with little regulation. The current regime fails to provide adequate protection for individuals. With massive data breaches happening at an alarming frequency,[360] every passing day there is the danger that millions

354 *Id.* at 356 (explaining the behavioral changes that consumers go through after entering into agreements).

355 *See* Oppenheimer, *supra* note 23, at 390.

356 *See* Pasquale, *supra* note 73, at 1012.

357 Ifeoma Ajunwa, *Genetic Testing Meets Big Data: Tort and Contract Law Issues*, 75 OHIO ST. L.J. 1225, 1244 (2014).

358 *Id.* at 1250.

359 *Id.*

360 Drapkin, *supra* note 4.

of people could have their privacy violated. The devices we use in our daily lives are obtaining sensitive information that can easily find its way into the wrong hands. The fragmented regulations available provide little protection. A restructuring from deidentified data to a voluntary, involuntary, and quasi-voluntary approach provides consumers with more control over their information. Further, mandatory implied contractual terms, enforced by the FTC, provide a comprehensive approach that protects all data categories and unifies the different approaches taken by the states. And implied contractual terms get ahead of the technological curve by not limiting their applicability to certain technologies. Consumers are often unaware of the location in which businesses store their credit card, location, browser history, or other personal information. Technology advances rapidly, and brain tracking technology currently exists.[361] Without mandatory data privacy regulation, soon someone can own your thoughts like they do your purchase history.

361 *See* NEURALINK, https://neuralink.com [https://perma.cc/NZ9G-QZPF].