Washington and Lee Journal of Civil Rights and Social Justice

Volume 29 | Issue 4 Article 7

Spring 2023

# Do Not Touch My Data: Exploring a Disclosure-Based Framework to Address Data Access

Francis Morency
*Washington and Lee University School of Law*, morency.f23@law.wlu.edu

# Do Not Touch My Data: Exploring a Disclosure-Based Framework to Address Data Access

Francis Morency*

*Abstract*

*Companies have too much control over people's information. In the data marketplace, companies package and sell individuals' data, and these individuals have little to no bargaining power over the process. Companies may freely buy and sell people's data in the private sector for targeted marketing and behavior manipulation. In the justice system, an unchecked data marketplace leaves black and brown communities vulnerable to serious data access issues caused by predictive sentencing, for example. Risk assessment algorithms in predictive sentencing rely on data on individuals and run all relevant data points to provide the likelihood that a defendant will recidivate low risk, medium risk, or high risk. These algorithms are flawed and deeply biased because they use factors that correlate with race and socioeconomic status. The law should recognize people's property interests in their data. Recognizing individuals' property interests in their data sets up a robust disclosure-based solution. The disclosure-based solution gives individuals substantial control over their data. The Note proposes a centralized platform— the Private Information Reporting System— for individuals to know where their data is used and*

* J.D. Candidate, May 2023, Washington and Lee University School of Law. This Note was initially inspired by Shoshana Zuboff's *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. I would like to sincerely thank everyone who helped me throughout the Note writing process. Specifically, I would like to extend my appreciation to my faculty advisor, Professor Joshua A. Fairfield and Note Editor, Emma Burri for all their guidance and recommendations. I would also like to thank Professors Kish Parella and A. William Mackie who helped flesh out solutions to the data access problem. Finally, I would like to thank my family and friends who offered constant support as I worked on this Note.

*restrict companies from selling it. This will result in more power for individuals and equity in the justice system.*

*Table of Contents*

I. Introduction ..... 151

II. Background: The Data Problem and Solutions ..... 152

III. The Data Marketplace ..... 154
A. Surveillance Capitalism: How Much Should We Be Worried About Companies' Access to Our Data? ..... 156

IV. Choosing the Best Legal Tool to Protect Data ..... 159
A. Looking Back, Privacy Law and Data Protection ..... 159
1. The Information Privacy Regime Cannot Keep up with Modern Technology ..... 160
2. The California Consumer Privacy Act ("CCPA") ..... 161
3. The European Union's General Data Protection Regulation ("GDPR") ..... 163
B. Looking Forward: Property Law May Protect Data ..... 165

V. Data Access' Negative Impact on Communities of Color ..... 169
A. Predictive Sentencing ..... 169

VI. Solving the Data Access Problem ..... 175
A. Disclosure-Based Solutions ..... 176
1. The Private Information Reporting System ..... 177
2. The Federal Trade Commission May Oversee the Private Information Reporting System ..... 178
a. Deceptive Statements ..... 179
b. Unfairness ..... 179
c. The Unfairness Legal Theory and Online Privacy ..... 181
3. Increasing Consumer Trust for Minorities by Adopting the Do Not Track List Framework. ..... 182
a. Revisiting the Opt-in and Opt-out approaches ..... 184
b. Apple Pay's Cryptographic Token Analogy: Anonymizing Purchaser's Information ..... 185
c. Addressing the Private Information Reporting System's Limitations ..... 187

VII. Conclusion ..... 187

## *I. Introduction*

Picture this— it is July 2016, and you are one of the 500 million users downloading Pokémon Go. With just a click, the application takes you back to your childhood dreams of following in Ash Ketchum's footsteps: traveling across the land, searching far and wide— catching and training Pokémon. The download is complete, and your phone prompts you to allow Pokémon Go to use your location. You agree. Next, it prompts you to enable the application to access your phone's camera. You agree. You start your adventure. As you walk around the real world, your character moves with you, and Pokémon appear on the virtual game board, replicating your surroundings. This is one example of augmented reality.[1]

Walking around your neighborhood, you get tired of seeing the same Pokémon. Your friend texts you, "I found a Pikachu at the mall!" Excited, you hop on the bus and make your way there. You find Pikachu, and you catch it. You start walking around the mall, ecstatic at this rare catch. Looking at your phone, you notice a Poké Stop nearby—it is Starbucks. Good, because you need to restock on Poké balls and collect eggs. You get all you need in the game, but you could also use a snack. So, you order a Pokémon Go Frappuccino and a croissant. You sit down to enjoy your snack and think, "would I have gone to the mall today and bought snacks at Starbucks but for Pokémon Go?"

Pokémon Go is more than an augmented reality mobile game. The game is a powerful tool that manipulates players' behavior and increases business profit.[2] A company can partner with

1. *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 312 (1st ed. 2019) (noting that Niantic designed Pokémon Go to be "played" in the real world, not on a screen as the game is structured like a treasure hunt bringing players outside).

2. *See* Tim Bradshaw & Leo Lewis, *Advertisers Set for a Piece of 'Pokémon Go' Action,* FIN. TIMES (July 12, 2016) (noting that John Hanke, the chief executive of Niantic, Pokémon Go's developer always planned on a revenue stream for the app focusing on players "chas[ing] cartoon creatures at 'pokestops' and 'gyms'" for profit) [perma.cc/RDG9-7NZP].

Pokémon Go to become a "sponsored location—" locations within the virtual game board drive real foot traffic and business profit.[3]

Niantic— Pokémon Go's developer— is not the only company to target users using data.[4] Corporations use targeted ads based on people's data to get them to spend money on specific products.[5] Once a company gets its hand on people's data, it can manipulate their behavior— this is the new economic system known as surveillance capitalism.[6] The economic system of surveillance capitalism facilitates a market in which Niantic is a participant.[7]

## *II. Background: The Data Problem and Solutions*

Companies treat human experiences in cyberspace as free raw material to improve digital products and anticipate what users will do now, soon, and later.[8] Information that companies collect to predict users' desires is known as behavioral data.[9] Behavioral data collection has proven lucrative for companies.[10] As the behavioral data marketplace grows, so does the concern for consumers' data.[11] In exchange for Niantic's augmented reality, Facebook's social platform, and Google's search capabilities,

3. *See id*. (explaining that retailers and other companies can sponsor places on the app's virtual map, as advertisement space that encourage players to go to a particular building or store, providing a new revenue stream for Niantic and companies sponsoring these places).

4. *See How Companies Profit and Use Your Personal Data,* CBS THE SCREENING HOUSE (demonstrating that Facebook and Google take user's personal data as the cost of using the websites' services) [perma.cc/HAA4-3NRB].

5. *See id*. (pointing out that Facebook stores users' identifiable content, which can be used to sell users targeted ads).

6. *See* ZUBOFF, *supra* note 1, at 7 (stating that surveillance capitalism is the unilateral claim over human experience as a free raw material translating into behavioral data).

7. *See id.* at 318 (showing how Niantic participates in surveillance capitalism by collecting user data for profit).

8. *See id.* at 8 (using behavioral data to anticipate what users will do now, soon, and later).

9. *See id.* (defining behavioral data).

10. *See Big Data & Business Analytics Market to Reach USD 684.12 Billion by 2030, Growing at a CAGR of 13.5%*, VALUATES REPS. (Oct. 29, 2021) (valuing the big data market) [perma.cc/BB6K-R673].

11. *See* Swish Goswami, *The Rising Concern Around Consumer Data and Privacy*, FORBES (Dec. 14, 2020, 7:40 AM) (explaining the rising concerns around how and when consumer data is used) [perma.cc/VFW6-R3EB].

consumers give up their behavioral data.[12] Corporations collect this information and sell it to other businesses who use it to manipulate users, increase foot traffic for their businesses and, in turn, make a profit.[13]

On the other side of profit-making goals is the devastating implications of the data market on criminal defendants when it comes to predictive sentencing.[14] This Note looks at the detrimental effects of risk assessment algorithms[15] on communities of color when it comes to predictive sentencing.[16]

Private and public entities exercise unrelenting access to people's data through the data marketplace— a market where data brokers[17] capture, package, and sell people's data to predict and manipulate their behavior.[18] The Note starts by setting the stage and defining the data marketplace. The Note moves on to contend that to solve the data problem, the legal system must first recognize property interests in data because historically, privacy law does not offer optimal solutions to the data problem. Next, the Note discusses how a part of the data market—predictive

12. *See* ZUBOFF, *supra* note 1, at 88 (noting that user services are the method for attracting behavioral data, which users supply to generate revenue for companies).

13. *See* ZUBOFF, *supra* note 1, at 10 (contending that these products and services are not the value exchange, they are actually "hooks" that lure users into their operations to users' personal experiences).

14. *See* Jacob D. Humerick, *Reprogramming Fairness: Affirmative Action in Algorithmic Criminal Sentencing*, 4 COLUM. HUM. RTS. L. REV. 213, 220 (2020) (noting that sentencing discrimination is exacerbated by data from algorithms comprised of factors like socioeconomic status, marital status, and employment status).

15. *See id.* at 220 (defining risk assessment algorithms as a model that uses "statistical probabilities based on factors such as age, employment history, and prior criminal record" to predict recidivism).

16. *See* Candice N. Jones, *A Broken Pattern: A look at the Flawed Risk and Needs Assessment Tool of the First Step Act*, 5 HOW. HUM. & C.R. L. REV. 185, 200 (2020) (contending that people of color are disproportionately affected by the justice system and that racial biases are likely built into the data and the risk assessment tool itself).

17. *See* Ashley Kuempel, *The Invisible Middlemen: A Critique and Call for Reform of the Data Broker Industry*, 36 NW. J. INT'L L. & BUS. 207, 209 (2016) (defining the data broker industry as one that collects and sells information on people behind the scenes without people's knowledge).

18. *See* ZUBOFF, *supra* note 1, at 314 (insisting that data brokers' sole aim is to manipulate and modify users' behavior).

sentencing—negatively affects criminal defendants. The, the Note then turns to solutions. Users need a disclosure-based solution that recognizes data as property and creates a centralized system where people may control over their information. The disclosure-based solution turns users into stakeholders in the data market and calling companies to shape data protection policies with users in mind. The Note then concludes.

### *III. The Data Marketplace*

The data marketplace involves buyers and sellers who transact over people's behavioral data.[19] Behavioral data is data generated by a customer's engagement with a business.[20] For example, data on the individual is produced whenever someone types a query into Google's search engine.[21] With each search, Google gives answers to the individual and stores the user's data for various purposes.[22] Google can use the data to improve its services, but also its targeted marketing tactics.[23]

Companies have a deep interest in people's data.[24] The global big data market was valued at 198.08 billion USD in 2020 and is forecasted to grow to 684.12 billion USD by 2030.[25] Companies are interested in people's data because it tells a story about the individual.[26] That story aids with anticipating what people will do

19. *See What is a Data Marketplace?* SNOWFLAKE (defining the data marketplace as an online transactional location or store that facilitates buying and selling of data) [perma.cc/Z6RB-YARH].

20. *See* ZUBOFF, *supra* note 1, at 7 (identifying behavioral data as the information produced from raw material claims and converted from online human experience).

21. *See id.* at 67 (adding that each Google search query produces loads of collateral data such as number and pattern of search terms, how a query is phrased, spelling, punctuation, dwell times, click patterns, and location).

22. *See id.* at 6 (storing personalized data uploaded to Google's servers).

23. *See id.* at 68–69 (noting that while data is used to improve services, the data is also captured and stored for targeted marketing).

24. *See* ZUBOFF, *supra* note 1, at 59 (recognizing Google's economic interests in capturing raw data and transforming them into behavioral data for profit).

25. *See Big Data & Business Analytics Market to Reach USD 684.12 Billion by 2030, Growing at a CAGR of 13.5%*, *supra* note 10 (valuing the big data market).

26. *See* ZUBOFF, *supra* note 1, at 7–8 (fabricating behavioral data into prediction products that anticipate what users will do now, soon, and later).

now, soon, and later. The information collected on people help with targeted marketing to increase sales.[27]

Google exploits information that is a by-product of user interactions.[28] Google can store key words that people search—"cheap" and "best"; the company also has the power to store behavioral data such as number and pattern of search terms, how questions are phrased, spelling, punctuation, dwell times, click patterns and location.[29] Google can use the continuous flow of data to turn the search engine into a recursive learning system—producing quicker results and predicting which products an individual would want to see— but also, the company can package and sell the data so that other companies can market their products with precision.[30]

As advice to large and small brands, Google highlights a four-step approach to appealing to customers: (1) Ensure brand presence to keep the product strategically front of mind while customers explore; (2) Employ behavioral science principles; (3) Close the gap between trigger and purchase; and (4) Build flexible, empowered teams who can work cross-functionally.[31] The approach fits perfectly in Google's targeted marketing system, where companies can pay for ad space that is tailored for specific users and show up on users' screens based on data Google collects.[32] Companies throughout cyberspace benefit from this

27. *See id.* (noting that prediction products allow participants in the data marketplace to grow wealthy by trading people's data).

28. *See id.* at 68 ("Google exploits information that is a by-product of user interactions, or data exhaust, which is automatically recycled to improve the service an entirely new product.").

29. *See id.* at 67 (storing behavioral data); *see also* Alister Rennie & Jonny Protheroe, *How People Decide What to Buy Lies in the 'Messy Middle' of the Purchase Journey*, GOOGLE (July 2020) [perma.cc/E4D8-EHEA] (demonstrating how collateral data may be used).

30. *See* ZUBOFF, *supra* note 1, at 68 (turning Google's search engine into a recursive learning system that constantly improves search results and spur product innovations such as spell check, translation, and voice recognition, leading to greater profit).

31. *See* Rennie & Protheroe, *supra* note 29 (highlighting the four-step approach to that marketers can use to appeal to customers).

32. *See Grow Your Business with Google Ads*, GOOGLE ADS (allowing companies to buy ad space to "get in front of customers when they're searching for business like yours on Google Search and Maps") [perma.cc/Q48P-FSV8].

economic system, and the next section explains the system's mechanics.

### *A. Surveillance Capitalism: How Much Should We Be Worried About Companies' Access to Our Data?*

Surveillance capitalism is the "unilateral claim over human experiences as a free raw material translating into behavioral data" and interpreting that data to "anticipate what you will do now, soon, and later."[33] While companies use behavioral data to improve the online user experience, society should be concerned about how much access companies have to their information, and how companies use it.

Companies like Google exercise a unilateral claim over people's data by allowing users to use the platform for free; with each search, data is generated, packaged, and sold to the actual customers— data brokers.[34] Each phrase typed into Google's search engine produces collateral behavioral data on the number and pattern of search terms, how the query is phrased, spelling, punctuation, dwell times, click patterns, location, and even the users' emotions.[35]

Once packaged, collateral behavioral data provides detailed stories of an individual's thoughts, feelings, and interests.[36] The more information Google collects, the more the company can improve user experience on the platform.[37] Collecting collateral behavior data could turn the search engine into a recursive

33. *See* ZUBOFF, *supra* note 1, at 8 (defining surveillance capitalism).

34. *See* Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L. J. 1460, 1478 (2019) (showing how companies like Palantir collect and sell data to police, government agencies, and private companies so they can use its predictive profiling tools).

35. *See* ZUBOFF, *supra* note 1, at 67 (detailing the types of data that is considered collateral).

36. *See id.* (illustrating how much Google can tell about a person simply by trailing their online activity and how this information provides a broad sensor of human behavior).

37. *See id.* at 68 ("Google's engineers soon grasped that the continuous flows of collateral behavioral data could turn the search engine into a recursive learning system that constantly improved search results and spurred product innovations such as spell check, translation, and voice recognition.").

learning system[38] that constantly enhances search results and spurs innovations such as spell check, translation, and voice recognition.[39] Predictive texting is another example of a recursive learning system.[40] Through predictive texting, the more a consumer texts, the more an iPhone can predict the next word a user will type.[41] However, there are dangers to creating this system of optimizing user experience.[42]

While data collection creates a more user-friendly platform, it can also lead to new forms of societal stratification.[43] By buying individuals' data, companies are empowered to divide people into "high-value" and "high-risk" categories so that marketers can reach lucrative groups and exclude undesired groups from their offers.[44] Behavioral data at such a granular level will undoubtedly benefit those with wealth and power, and disadvantage others.[45]

Palantir Technologies, Inc. ("Palantir") is a prime example of how data collection by companies will inevitably lead to new forms

38. *See* Kapczyski, *supra* note 34, at 1468 (turning the search engine into a system that improves search results by collecting and learning from data that is inputted by users with each query); *see also* ZUBOFF, *supra* note 1, at 411 (storing behavioral data for future analysis to improve the system's prediction on what users want to see based on popular searches).

39. *See id.* at 68 (referencing Kenneth Cukier who observed that Google exploits collateral data to improve service or create an entirely new product).

40. *See iPhone User Guide*, APPLE (identifying predictive texting as a system that learns users" behavior the more they type on their phones) [perma.cc/5GBA-R49Y].

41. *See id.* (demonstrating that as users type on the iPhone keyboard, they can see predictions for the next word, emoji that could take the place of the word, and other suggestions based on their recent activity and information from their apps).

42. *See* ZUBOFF, *supra* note 1, at 109 (asserting that surveillance capitalism is becoming increasingly dangerous as companies develop a "cyberlibertarian" ideology where they aggressively assert First Amendment principles to fend off any form of oversight that could limit the "algorithmic orderings of information").

43. *See* Kapczyski, *supra* note 34, at 1478 (highlighting concerns about regressive distributions of wealth and stratification regarding race).

44. *See id.* (contending that Zuboff obscures a crucial social reality that an uncontrolled data marketplace will create a new stratification in society despite the individualistic benefits).

45. *See id.* (referring to the stratification created where powerful groups can benefit from the data marketplace while those who cannot afford it cannot).

of societal stratification.[46] Palantir, founded in 2003, is a software platform that analyzes data for many government organizations.[47] The company helps organizations gather and make sense of loads of data.[48] The company helps to collect data from various sources—internet traffic and cellphone records—and interprets the information.[49] Palantir packages the data and tells stories with it in ways that will be useful to data-buyers.[50]

Among Palantir's customers are police, government agencies, and private companies that can pay for its costly predictive profiling tools.[51] Law enforcement increasingly relies on big data to fuel predictive policing.[52] Police departments that use Palantir's services rely on data to predict where future crimes may occur.[53]

Using data to predict behavior and crime locations is harmful to marginalized communities, mainly when law enforcement relies on incomplete data, leading them to increase police presence in black and brown neighborhoods—over policing—because the data asserts that past crimes are a good sign for where future crimes

46. *See id.* (explaining how Palantir intensifies stratifications by selling data to those who can afford it: police, government agencies, and private companies).

47. *See* Mary E. Callahan et al., *Chartering the Future: What to Expect from Big Data*, 7 J. NAT'L SEC. L. & POL'Y 341, 344 n. 5 (2014) (describing the purpose of Palantir).

48. *See* Cade Metz et al., *What's a Palantir? The Tech Industry's Next Big I.P.O.*, N.Y. TIMES (Aug. 26, 2020) (illustrating that Palantir is primarily a software company that helps organizations make sense of data) [perma.cc/GWW5-KDEY].

49. *See id.* (explaining how Palantir helps companies gather data that companies want to collect).

50. *See id.* (showing that Palantir does not merely collect data, but the company also interprets the data it collects for other companies that use Palantir's services).

51. *See id.* (demonstrating the real-time effects of the data marketplace by showing how wealthy people can benefit the most from this market while underserved groups do not).

52. *See* Moish Kutnowski, *The Ethical Dangers and Merits of Predictive Policing*, 2 J. CMTY. SAFETY & WELL-BEING 13, 13 (2017) (acknowledging that predictive policing is becoming a trend and relies on Big Data infrastructure).

53. *See* Kapczyski, *supra* note 34, at 1478 (using algorithms trained on historical data to predict behavior but are entrenched in bias).

will occur.[54] Along with predictive policing, predictive sentencing throws another blow to Black and Latino communities.

The disclosure-based solution, which promotes user autonomy over data, requires the law to recognize users' property interest in their data. Part IV of the Note explains why the law should recognize people's property interest in their data.

## *IV. Choosing the Best Legal Tool to Protect Data*

Unfortunately, legislators have employed information privacy to address the data problem.[55] Current legislation like the California Consumer Privacy Act ("CCPA") and the European Union's General Data Protection Regulation ("GDPR") fail to give users control over their information because these regimes are structured around mere notice and consent.[56] Lawmakers may strengthen data protection efforts by recognizing people's property interests in their data. This section explores the weaknesses in current legislation and court decisions that shape how the legal system addresses the data problem.

### *A. Looking Back, Privacy Law and Data Protection*

Information privacy—the term depicting the culmination of privacy torts—is the ability to control and protect one's personal information.[57] Nearly sixty years ago, Dean William Prosser

54. *See* Kutnowski, *supra* note 52, at 13–14 (demonstrating that relying on predictive policing results in negative results for poor communities and communities of color because it perpetuates a vicious cycle of criminal behavior).

55. *See* Rob Bonta, *California Consumer Privacy Act*, STATE CAL. DEP'T JUST. OFF. ATT'Y GEN. (Feb. 15, 2023) ("This landmark law secures new privacy rights for California consumers.") [perma.cc/ETN6-W29K]; *see also* Ben Wolford, *What is GDPR, the EU's New Data Protection Law?*, GDPR.EU ("The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world.") [perma.cc/YY6D-8YD6].

56. *See* Viktor Mayer-Schönberger, *Beyond Privacy, Beyond Rights-Towards a "Systems" Theory of Information Governance*, 98 CAL. L. REV. 1853, 1859 (2010) (addressing information privacy's permission-and-consent structure as giving individuals only limited control over how others use their personal information).

57. *See id.* at 1854 (defining information privacy).

outlined a comprehensive framework of "the right to privacy"[58] and how it can be protected through torts.[59] Since then, there has been a boom in activity in cyberspace, and people's information has been translated to data on the internet, causing concern over what privacy means online.[60]

### *1. The Information Privacy Regime Cannot Keep up with Modern Technology*

As technology develops, people are concerned about their privacy, or at least they should be.[61] In the nineteenth century, for example, technological developments like the telegraph drove concerns over privacy protection because users were worried that the information they transmitted would not be secure.[62] More recently, technological developments shifted the global economy to dematerialize data and shift information into cyberspace, thus promoting more efficient transactions.[63] For example, most financial industries abandoned physical ledgers and replaced them

58. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 213 (1890) (describing the right to privacy as an innate guarantee rather than a right that rises from some other legal tool).

59. *See id.* at 218–19 (protecting the right to privacy through torts).

60. *See* Mayer-Schönberger, *supra* note 56, at 1854 (commenting that over 1.8 billion people are accessing the internet).

61. *See id.* (showing that the exponential increase in reliance on information calls for laws to protect information privacy and how internet users have growing concern over this development).

62. *See* Urs Gasser, *Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy*, 130 HARV. L. REV. F. 61, 61–62 (2016) (providing an example of a technological development that raised the alarm for more privacy protection); *see also* Thomas McMullan, *The World's First Hack: The Telegraph and the Invention of Privacy*, THE GUARDIAN (Jul. 15, 2015) ("By the turn of the century, business users were concerned about privacy, and cable companies were therefore keen to ensure they knew anything sent by cable was secure.") [perma.cc/27GA-AKL7].

63. *See* Kapczyski, *supra* note 34, at 1488 (arguing that "dataf[ying]" finance as technologies and law coevolved to enable instantaneous transactions and leading to new forms of securitization and demonetization); *see also id.* at 1490 (advancing technology providing companies with overreach to information was facilitated by neoliberalism).

with online accounts to keep track of information and process it more efficiently.[64]

Technological developments usually draw in privacy concerns. These concerns are usually addressed through privacy law comprised of a complementary web of federal and state contracts, consumer protection privacy torts, and sector-specific consumer rights laws.[65] Privacy law is inefficient to address data issues because the area lacks precision.[66] Nevertheless, privacy law around data is merely structured around notice and consent, which alone, does not provide sufficient protections because the regime fails to ensure that people retain control and access over their data.[67] The CCPA and the GDPR demonstrate the pitfalls of the notice and consent regime.

### *2. The California Consumer Privacy Act ("CCPA")*

In 2018, California became one of the first states to take a dramatic step toward consumer data protection.[68] California state legislatures established the CCPA to give consumers greater control over their personal information.[69] The CCPA creates new

---

64. *See id.* at 1487 (noting a rising percentage of jobs involve information processing).

65. *See* Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 592 n. 36 (2021) (referring to 15 U.S.C. § 45(a)(1) (2018), which prohibits "unfair or deceptive acts or practices in or affecting commerce").

66. *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2008).

> Privacy, however, is a concept in disarray. Nobody can articulate what it means. Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations.

67. *See* Salomé Viljoen, *supra* note 65, at 598–99 (contending that notice-and-consent regimes fail to ensure that people retain control and access over their data).

68. *See* Bonta, *supra* note 55 (recognizing the novelty of the CCPA over data protection in 2018).

69. *See* Assemb. B. 375 § 2(g), 2017–2018 Reg. Sess. (Cal. 2018) (enacted) ("People desire privacy and more control over their information. California Consumers should be able to exercise control over their personal information, and

consumer rights within three main categories: the right to know, the right to delete, and the right to opt out.[70] The right to know grants consumers the right to request that a business disclose details about what personal information they collected on the individual.[71] The right to delete requires companies to delete personal information collected from consumers upon verified consumer request.[72] Finally, the CCPA gives consumers a right to opt out, where they have the right to direct businesses not to sell their personal information.[73] The CCPA only gives consumers the right to opt-out of companies selling their data; it does not allow consumers to opt-out of data collection.[74] The CCPA also creates a private right action.[75]

One of the unique features of the CCPA is that it creates a private right of action, where consumers may seek damages if their personal information is exposed because of a business's failure to "implement and maintain reasonable security procedures and practices."[76] Consumers do not need to wait until the company holding their data experiences a breach, nor do consumers need to experience financial harm before they bring the cause of action.[77]

---

they want to be certain that there are safeguards against misuse of their personal information.").

70. *See* Rebecca Harris, Note, *Forging a Path Towards Meaningful Digital Privacy: Data Monetization and the CCPA*, 54 LOY. L.A. L. REV. 197, 217 (2020) (noting the users right to know, delete and the right to opt-out of data sharing).

71. *See id.* (specifying that consumers may find out the categories of personal information to which companies have access, what sources were used to collect that information, for what purpose, and who had access to the information).

72. *See id.* (outlining California's consumer right to delete where businesses are required to delete consumer personal information once the request is verified).

73. *See id.* (showing that consumers have a right to avoid personal data collection from the outset, and that businesses must notify consumers of that right).

74. *See* MATTHEW P. GOODMAN & DYLAN GERSTEL, SHARPENING AMERICA'S INNOVATIVE EDGE, 22–23 (William Reinsch & Scott Miller eds., 2020) (noting that a key difference between the GDPR and the CCPA is that the GDPR allows European citizens to opt out of data collection, not only opting out of companies selling user personal information).

75. *See* CAL. CIV. CODE § 1798.150(a)(1)(A) (West 2023) (allowing users to recover damages).

76. § 1798.150(a)(1).

77. *See* Harris, *supra* note 70, at 227 (allowing users to recover following a data breach, even if the data exposure did not result in financial harm).

Instead, the law provides that "[a]ny consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices" may sue to recover damages between $100 and $750.[78]

Further, the CCPA has a "cure" requirement where the consumer must first notify the accused business in writing explaining the violation and provide 30 days for the company to cure the breach.[79] Following a failure to cure, users may initiate litigation to vindicate their rights.[80] California's statute falls short and is dissimilar to Europe's GDPR because while the CCPA highlights the right to know, delete, and opt-out, it does not give consumers complete ownership over their data.[81]

### *3. The European Union's General Data Protection Regulation ("GDPR")*

The European Union enacted the GDPR in 2018 as comprehensive privacy law.[82] The GDRP includes detailed practices that companies must follow to protect consumer data, fines for non-compliance, and a jurisdictional provision that allows the regulations to apply to U.S. companies doing business in Europe and collecting data on EU citizens.[83] The GDPR offers greater protection over consumer data than other legislation in the

78. CAL. CIV. CODE § 1798.150(a)(1)(A).

79. § 1798.150(b).

80. *See* Harris, *supra* note 70, at 227 (allowing suit against a company who fails to cure the data breach).

81. *See* Jordan Yallen, *Untangling the Privacy Law Web: Why the California Consumer Privacy Act Furthers the Need for Federal Preemptive Legislation*, 53 LOY. L.A. L. REV. 787, 820 (2020) ("[F]ailing to 'give consumers complete ownership of their data.'").

82. *See* Harris, *supra* note 70, at 214 (explaining the origins of the EU GDPR).

83. *See* Andrew Crayden, *A Modern-Day Gold-Rush: Applying Property Principles to Data Using Mineral Rights Concepts and the Rule of Capture*, 81 LA. L. REV. 949, 966–68 (2021) (including more detailed practices that companies must follow to protect consumer data, increased fines for non-compliance, and provisions that also affect most U.S. companies).

United States. Under the law, companies must protect consumers' data in any operation.[84]

The GDPR treats data privacy as a "fundamental right," which explains why the GDPR offers a more robust data protection framework.[85] The GDPR grants citizens the right to be forgotten.[86] The right to be forgotten goes further than the CCPA because European citizens may prohibit companies from selling their information and keep companies from collecting information altogether.[87]

A notable difference between the CCPA and GDPR is that the CCPA uses the "opt-out" framework while the GDPR uses the "opt-in" framework.[88] The opt-in framework requires users to affirmatively consent before businesses may sell a consumer's personal information.[89] Conversely, the opt-out framework requires users to demand that companies stop selling users' personal information.[90] Users have more power over their personal information under the opt-in model.[91]

The GDPR offers more robust means to provide people with more agency over their data, but it is not enough.[92] The GDPR

84. *See* Wolford, *supra* note 55 (characterizing the GDPR as the toughest privacy and security law in the world because it gives users the right to know which companies use their information and the right to delete their information).

85. See Council Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 (recognizing that the right to data protection is a fundamental right of natural persons); *see also* Crayden, *supra* note 83, at 969 (discussing World War II as a catalyst for Europe to consider data privacy as a fundamental right).

86. *See* Harris, *supra* note 70, at 214 (describing the right to be forgotten as individuals' right to demand that companies delete their personal data).

87. *See* Alessandra Masciandaro, *Cleaning-up After Carpenter: Personal Data as Property Under the Fourth Amendment*, 51 SETON HALL L. REV. 1241, 1265 (2021) (recognizing that the GDPR, not the CCPA gives individuals the "right to be forgotten").

88. *See* CAL. CIV. CODE § 1798.120(b) (West 2023) (showing that consumers have the "right to opt-out" of businesses selling their information).

89. *See* Harris, *supra* note 70, at 231 (calling the user to give affirmative consent for the business to access and use consumers' data).

90. *See id.* at 217 (granting a right to have businesses not sell individuals' own data).

91. *See id.* at 231 (requiring consumers to affirmatively provide consent before businesses may sell that consumer's personal information).

92. *See id.* at 214 (showing that GDPR gives European consumers greater control over their data).

lacks a centralized platform that allows users to proactively protect their data by changing who may access it. The disclosure-based approach proposes a centralized platform where users can restrict business' access to individuals' data. The disclosure-based approach only works if the law recognizes people's property interests in data. The next section discusses the tools available to help the law recognize data as property. It begins with an understanding that property is all about information.

### *B. Looking Forward: Property Law May Protect Data*

Property law is the most suitable legal area to deal with people's data issues.[93] Property is all about information.[94] Traditional property rights involve organizing information about who owns what over a specific period.[95] Further, when it comes time to pass the property interest to someone, the information attached to that property in a county land registry is updated.[96] Ownership interest in land is pure information.[97] Information in a county registry is essential for identifying who owns which house and how much land around each house goes with it.[98] The house and the land are distinct from the ownership interest, which is pure information.[99] The rocks or trees around the land may serve

93. *See* Heather Payne, *Sharing Negawatts: Property Law, Electronic Data, and Facilitating the Energy Sharing Economy*, 123 PENN ST. L. REV. 355, 381 (2019) (classifying data as property leads to greater protections over data).

94. *See* Joshua A.T. Fairfield, Bitproperty, 88 S. CAL. L. REV. 805, 811 (2015) ("[P]roperty is information.").

95. *See id.* at 813–15 (pointing to sources of conveying information about property over time—registries, for example—is one good way of depicting who possesses what).

96. *See id.* at 827 (stating an ownership claim over real property through property registry).

97. *See id.* at 827–28 (describing that the need for property information is centralized for an appropriate property system).

98. *See id.* at 826–27 (using information about a house to know how much land comes with it).

99. *See id*. (distinguishing the house from ownership interest which is made clear through information attached to the property).

as a border, and their meanings and significance are pure information.[100]

By looking at the land, one can identify a particular set of trees that signifies where ownership interests end.[101] On a road trip through a country, one might notice no difference between the land on either side of the border when they cross stateliness. However, maps identify border information. For example, the French territory of Alsace changed nationality multiple times throughout history—changing the borders between Germany and France every time.[102] Despite the shifting borders on the map, the land itself never changed— the information did. Various governments have used data to record the characteristics attributed to that property, like who owns it.[103]

Therefore, since property systems rely on information, property law is the most tenable framework to protect data.[104] Information about the physical world is stored in cyberspace. Thinking about property as information fits into the history of property rights in the United States. However, corporations may continue to extract people's data because Court's do not recognize an individual's property interest in that data.

If courts recognize people's property interests over their data; it will be possible to sue for conversion in a disclosure-based system where companies unlawfully take people's data or turn it over to the government.[105] *Moore v. Regents of the University of*

100. *See id.* (contending that borders gain their meaning, not by their physical attributes, but by the information attached to that border, thus making trees or rocks around the land signify boundaries).

101. *See id.* (showing that information attached to trees and rocks around land accords significance as borders to the land).

102. *See Alsace-Lorraine Territory, France*, BRITANNICA (last updated Jan. 11, 2023) (listing the border changes between France and Germany) [perma.cc/K4ZJ-TDZS].

103. *See id.* (redrawing maps to keep track of which Country owned the territory).

104. *See* Payne, *supra* note 93, at 381 (showing the benefits of dealing with data through property law).

105. *See* Moore v. Regents of Univ. of Cal., 793 P.2d 479, 489 (1990) (ruling that Moore could not recover on a conversion claim because he did not have ownership interest over his excised cells).

*California*[106] shows the realm of possibilities for data protection if the law recognized people's property interest in their data.[107]

One might think that his blood cells belong to him, but in John Moore's case, the Supreme Court of California concluded otherwise. John Moore was a patient at UCLA Medical Center and underwent treatment for hairy-cell leukemia.[108] Moore's Doctor—Dr. Golde recommended a spleen removal for Moore.[109] Unknown to Moore, Dr. Golde harvested parts of Moore's spleen to take them to a separate research unit.[110]

Dr. Golde took Moore's cells for his independent research and established a cell line for which the doctor also applied for a patent.[111] Moore brought 13 causes of action, among them, one for conversion.[112] Conversion is a tort claim that protects a person's possessory and ownership interest in personal property.[113]

Moore contended that he continued to own his cells even after the doctor removed them from his body, at least to the extent of directing how the doctor could use them.[114] Moore claimed a proprietary interest in all the products his cells helped to create.[115]

---

106. *See id.* at 497 (holding that the Doctor was not liable under the tort of conversion for patenting Moore's cells).

107. *See* Kapczyski, *supra* note 34, at 1505 (recognizing that although *Moore v. Regents of California* is typically only discussed in property or health-law contexts, it also serves as a canonical case shaping the information economy).

108. *See Moore*, 793 P.2d at 480 (showing that Moore was receiving treatment for hair-cell leukemia at the Medical Center of the University of California at Los Angeles).

109. *See id*. at 481 (informing Moore that his life was at risk and recommending that Moore get his spleen removed to slow down the disease).

110. *See id*. (explaining that portions of Moore's spleen were taken to a separate research unit for a study that was not intended to have any relations to Moore's medical care).

111. *See id*. at 482 (detailing how Dr. Golde turned Moore's cells into a cell line and patented them as a means to produce certain proteins potentially worth billions of dollars as treatments).

112. *See id.* (noting that Moore brought 13 causes of action and Dr. Golde demurred each).

113. *See id.* at 487 (showing that Moore theorized that he continued to own his cells after they were removed from his body and never consented to Dr. Golde using them for research purposes).

114. *See id*. (arguing that Moore at least had the right to direct how his removed cells were used).

115. *See id*. (claiming an interest in all current and future products that his cells helped to create).

In *Moore*, the California Supreme Court decided the novel issue— imposing conversion liability for using human cells in medical research.[116] The court held that the tort of conversion did not give Moore a cause of action under existing law because California statutory law drastically limits patients' control over excised cells;[117] and since Moore did not expect to retain possession of his cells after they were removed, the court concluded that he did not have ownership interest over them.[118] Property law remains consistent— courts are more inclined to reward the labor that went into capturing and innovating the property.[119]

The *Moore* holding supports a corporation's ability to extract and accumulate personal data, trumping an individual's entitlement to that data.[120] Regrettably, the law does not treat data as people's property; instead, companies capture and package people's data to sell and improve targeted marketing.[121] However, based on the discussion throughout this Section, data may be viewed as property because property is all about information.[122]

---

116. *See id*. (showing that the reviewing court was the California Supreme Court).

117. *See id*. at 491 ("Notwithstanding any other provision of law, recognizable anatomical parts, human tissues, anatomical human remains, or infectious waste following conclusion of scientific use shall be disposed of by interment, incineration, or any other method determined by the state department [of health services] to protect the public health and safety.").

118. *See id*. at 488–489 (explaining that after their removal, Moore did not expect to retain possession of his cells, because to successfully challenge Dr. Golde's usage, Moore must have retained an ownership interest over them but he did not).

119. *See* Masciandaro, *supra* note 87, at 1263 (rewarding the labor that went into hunting the fox by holding that the act created a property right); *see also* Moore v. Regents of Univ. of Cal., 793 P.2d 479, 485 (1990) (reasoning that important medical research relies on economic incentives, so the court needed to protect those interests).

120. *See* Kapczyski, *supra* note 34, at 1506, n. 253 (noting that the majority barred the plaintiff from obtaining the benefit of his own cell's value but permitting the defendants to retain and exploit the total economic value from getting the cells).

121. *See id*. at 1503 (showing that companies have a legal right to the data they collect from individuals by claiming it as valuable and secret commercial information).

122. *See* Payne, *supra* note 93, at 381 (noting that when data is classified as property, there will be greater protections).

Until the legal system recognizes people's property interests in their data, people will navigate cyberspace vulnerable to the intricacies of the data market. Part V demonstrates the negative implications of the data market on communities of color and low-income communities.

### *V. Data Access' Negative Impact on Communities of Color*

Part V of the Note discusses the data's impact on Black, Latino, and low-income communities. Data sets determine a defendant's likelihood of committing a crime; thus, the justice system uses them to issue defendants' sentences. On its face, using data to issue sentences removes human judgment and uses the neutrality of data.[123] The issue is that humans input data.[124] Humans might use factors that correlate with race or socioeconomic status— perpetuating discrimination.[125]

#### *A. Predictive Sentencing*

This Section covers risk assessment tools that judges use to calculate defendants' recidivism rates. While risk assessment tools aid with judicial efficiency and replace human judgment when sentencing people, it is riddled with data that endorses sentencing discrimination.[126] First, the Section looks at the foundation for predictive sentencing, the major players, and the data on which judges rely to sentence people. Then, the discussion turns to explaining why certain factors that comprise the data are discriminatory. Finally, the Section explains why the discrimination caused by using specific types of data is unconstitutional and harmful to people.

---

123. *See* Humerick, *supra* note 14, at 216 (explaining that the recommended sentence from the algorithm is intended to remove individual human bias while maintaining fairness).

124. *See id*. at 234 (relying on data with a history of racial bias reflects the same racial bias the risk assessment tools claim to avoid).

125. *See id*. at 224 (showing that factors like socioeconomic status, economic status, and marital status are out of the defendant's control and exemplify the existence of sentencing discrimination).

126. *See id*. (listing the discriminative factors used by risk assessment tools).

Judges weigh various data points to decide the length of a criminal defendant's sentence: the applicable sentencing guidelines recommendations, the harm done to the community, the defendant's criminal history, the defendant's employment status at the time of arrest and residential stability and pieces of the defendant's personal information.[127] To alleviate the burden of going through each of these data points and measuring them against each other, judges in many states turn to a risk assessment algorithm.[128] Risk assessment algorithms rely on data, and run all relevant data points to provide the likelihood that a defendant will recidivate: low risk, medium risk or high risk.[129] From a defendant's recidivism risk rate, the judges rely on machines to assign a recommended sentence.[130] In theory, risk assessment algorithms remove individual human bias to sentence defendants fairly.[131] Unfortunately, the system designed to replace human judgment is flawed because it is using data that is racially biased.[132]

Algorithmic sentencing denotes a framework in which judges use risk assessment algorithms to determine defendants' sentences by objectively balancing data points relating to the defendant's recidivism rate.[133] Judges use these algorithms to make predictions about future crimes by gathering decades worth of publicly available information at the individual, community, and

127. *See* Humerick, *supra* note 14, at 216 (providing some of the factors that go into calculating rates of recidivism); *see also Indiana Risk Assessment System*, UNIV. OF CIN. (April 23, 2010) (showing how Indiana considers the defendant's employment status at the time of arrest and residential stability (socioeconomic factors) to determine recidivism rate) [perma.cc/4NZD-TDW2].

128. *See* Humerick, *supra* note 14, at 216 (using the risk-assessment algorithm to alleviate the burden of manually considering factors that contribute to recidivism rates).

129. *See id*. at 217 (having run all the relevant data points using risk assessment tools, the judge will tell how likely the defendant is to recidivate).

130. *See id*. (relying on the algorithm to issue the defendant's sentence).

131. *See id*. at 224 (applying historically biased data to produce algorithms that determine recidivism rates).

132. *See id*. (using socioeconomic factors that lead to racial bias to render decisions on defendants' recidivism).

133. *See id*. at 225–226 (explaining how the risk assessment algorithm relies on "big data"—"data that describes a large volume of data that can be mined for information.").

state levels.[134] The risk assessment algorithms automates criminal justice— using a large volume of data to predict a defendant's criminal conduct, and in turn recidivism rate.[135] Unfortunately, risk assessment tools are no more reliable than predictions of individual laypeople on the internet.[136]

The Correctional Offender Management Profiling for Alternative Sanctions ("COMPAS"),[137] a risk assessment tool was developed by Northpointe, inc. in the 1990s.[138] The COMPAS risk assessment tool uses factors like socioeconomic status, employment status, marital status, and zip code—which may have predictive value—but using these factors also endorses sentencing discrimination based on factors the defendant cannot control.[139] Risk assessment tools assign each factors certain scores, adding them up to determine the sentence.[140] The different weight assigned to factors like socioeconomic status, employment status marital status, and zip code can count against the defendant.[141] In

134. *See id.* at 225 (explaining the system of gathering decades worth of public information about people to make predictions about future crime by simply adding up specific data points).

135. *See id*. at 226 (defining automation in algorithms as applying an automated protocol to a large volume of data to make predictions about criminal conduct).

136. *See id*. at 224 (referencing Julia Dressel and Hany Faird contending that the COMPAS risk assessment in Wisconsin "is no more accurate or fair" than predictions from laypeople on the Internet).

137. *See* Cindy Anderson, *Risk Assessment Instruments Are Inappropriate for Sentence Reform: Real Solutions for Reform Address Racial Stratification*, 12 GEO. J. L. & MOD. CRITICAL RACE PERSP. 187, 193–194 (2020) (explaining that Northpointe is the organization that created COMPAS—a risk assessment tool that uses algorithms to calculate recidivism rates).

138. *See* Andrew L. Park, *Injustice Ex Machina: Predictive Algorithms in Criminal Sentencing*, UCLA L. REV. (Feb. 19, 2019) (explaining origins of COMPAS) [perma.cc/FS43-Z5HC].

139. *See* Humerick, *supra* note 14, at 224 (relying on these factors endorses sentencing discrimination and may account for racially biased policing practices in their neighborhood, perpetuating institutionalized discrimination); *see also* Sonja B. Starr, *The New Profiling Shy Punishing on Poverty and Identity is Unconstitutional and Wrong*, 27 FED. SENT'G REP. 229, 230 (2015) (exhibiting that while socioeconomic, family and neighborhood-related factors do not explicitly consider race, they are highly race-correlated).

140. *See* Humerick, *supra* note 14, at 221 (assigning scores to each factor to determine the defendant's recidivism rate).

141. *See id*. at 221, 224 (indicating that higher scores indicate a higher risk of recidivism).

*State v. Gauthier*[142] the Supreme Judicial Court of Maine gave heavy weight to Gauthier's high score on a popular risk assessment tool, disregarding his youth and history of mental illness, sentencing Gauthier to 60 years for murder.[143] Further, because of trade secrecy laws, courts cannot obtain information on the source of risk assessment data on which risk assessment tools like COMPAS reach conclusions to declare sentences.[144]

Risk assessment tools like COMPAS are racially biased.[145] To find a solution to racially biased sentencing, it is important to identify who needs to be held accountable: the judge who renders the sentence, the companies who gather and calculate the recidivism rates or the platforms which hold the information. To identify who should be held accountable, one needs to consider what type of information is the subject of forming algorithms that tell the story of a defendant's recidivism.

Risk Assessment tools use official records to collect and verify information like employment status at the time of arrest, residential stability, and prior convictions to calculate recidivism rates.[146] Factors like prior convictions, employment status, and residential stability are verified using official records that are public.[147] Despite being public information, these factors are used in a discriminatory way.[148] Thus, the companies who gather and calculate recidivism rates, and most importantly the jurisdictions

142. *See* State v. Gauthier, 939 A.2d 77, 85 (Me. 2007) (ruling that the trial court did not err in its sentencing determination).

143. *See id*. (refusing to consider Gauthier's youth and mental health as mitigating factors because the court contended that it would not outweigh the other aggravating factors).

144. *See* State v. Loomis, 881 N.W.2d 749, 756—757 (Wis. 2016) (showing that an expert testified that "[t]he Court does not know how the COMPAS compares that individual's history with the population that it's comparing them with").

145. *See* Humerick, *supra* note 14, at 223 (criticizing the risk assessment tool, COMPAS, because it is no more accurate or fair than a layperson's predictions).

146. *See Indiana Risk Assessment System*, UNIV. CIN. (April 23, 2010) (showing the factors used to determine recidivism rate, and how to verify the information collected using official records) [perma.cc/C9FU-XQTJ].

147. *See id*. (using official public records to verify a defendant's prior convictions, employment status, and residential stability).

148. *See* Sonja B. Starr, *The New Profiling Shy Punishing on Poverty and Identity is Unconstitutional and Wrong*, 27 FED. SENT'G REP. 229, 230 (2015) (construing that by using risk scores based on socioeconomic status, the government endorses sentencing discrimination).

paying for this information, should be at the center of a solution that calls for accountability to limit racial bias in the algorithms created using people's information. Factors like employment history and residential stability can be categorized as socioeconomic information.[149] Sentencing based on socioeconomic generalizations is unconstitutional.[150] In the criminal justice system, there is an extensive line of Supreme Court jurisprudence applying special scrutiny to State actions that implement adverse treatment toward indigent defendants.[151]

Even though socioeconomic generalizations come from public information, they are used in a discriminatory way, which makes them unconstitutional.[152] When reviewing wealth-related classifications in the criminal justice system, the Court "requires careful inquiry into such factors as 'the nature of the individual interest affects, the extent to which it is affects, the rationality of the connection between legislative means and purpose, and the existence of alternative means for effectuating the purpose."[153] In *Bearden v. Georgia*[154] the State tried to revoke probation because the defendant failed to make payment for restitution; the defendant's previous sentence was probation and restitution.[155] The defendant stopped making payments because he ended up losing his job.[156] The Supreme Court rightfully rejected the State's

149. *See id*. (classifying the defendant's financial, housing, family, and employment history as socioeconomic factors).

150. *See id*. (contending that sentencing based on socioeconomic generalizations is unconstitutional and is often overlooked in the risk assessment debate because class-based distinctions do not receive heightened equal protection scrutiny).

151. *See id*. (referencing *Griffin v. Illinois*, a 1956 case saying that "equal justice for poor and rich, weak and powerful alike" is "the central aim of our entire judicial system," and stating that the "constitutional guaranties of due process and equal protection both call for procedures in criminal trials which allow no invidious discriminations").

152. *See id*. (pointing out that sentencing based on socioeconomic generalizations are unconstitutional).

153. *See* Bearden v. Georgia, 461 U.S. 660, 666–67 (1983).

154. Bearden v. Georgia, 461 U.S. 660 (1983).

155. *See id.* at 660 ("[P]ursuant to the Georgia First Offender's Act, [trial court] did not enter a judgment of guilt and sentenced petitioner to probation on the condition that he pay a $500 fine and $250 in restitution.").

156. *See id*. at 662—663 (noting that in an effort to pay his restitution, petitioner borrowed money from his parents after he was laid off from his job).

attempt to justify punishment, reasoning that the defendant made bona fide efforts to repay his debts, and the State could not classify him as dangerous simple because of his socioeconomic status.[157] Risk assessment tools are antithetical to the *Bearden* holding because they "lump [defendants] together with other poor persons and thereby classify [them] as dangerous."[158]

To recap— the criminal justice system uses algorithms from private companies who create these algorithms from data gathered from public sources.[159] Trade secrecy laws preclude the criminal justice system to investigate the reliability of the algorithms used to determine recidivism rates.[160] Some of the data collected from private companies that sell algorithms tell a story about a defendant's socioeconomic status.[161] While the algorithms include public information, the issue is that the criminal justice system is using data to discriminate against defendant's based on their socioeconomic status— which is unconstitutional.[162]

Therefore, private citizens in the United States should be worried on two fronts: private companies use people's private information to sell products, and private companies create algorithms to sell to the criminal justice system using people's public information and sentencing defendants based on their socioeconomic status.[163] Whether through private information or

157. *See id.* at 671 ("[T]he State cannot justify incarcerating a probationer who has demonstrated sufficient bona fide efforts to repay his debt to society, solely by lumping him together with other poor persons and thereby classifying him as dangerous.").

158. *See* Starr, *supra* note 148, at 231 (quoting the Supreme Court in *Bearden v. Georgia*, 461 U.S. 660, 666–67 (1983)).

159. *See* COLL. OF EDUC., CRIM. JUST., & HUM. SERVS, UNIV. OF CINCINNATI, *supra* note 146 (using public records to verify socioeconomic factors).

160. *See* Humerick, *supra* note 14, at 238 (criticizing how algorithms used by risk assessment tools are protected under trade secrecy laws).

161. *See id*. at 217 (categorizing defendants as low risk, medium risk, or high risk by using data collected by risk assessment tools).

162. *See* Starr, *supra* note 148, at 230–231 (using socioeconomic facts are unconstitutional because it is punishing defendants for lack of wealth).

163. *See* Paul M. Schwartz, *Property, Privacy, and Personal Data* 117 HARV. L. REV. 2055, 2094 (2003) (expressing concerns that increased data trade will increase personal data and create new harms to individuals); *see also* Humerick, *supra* note 14, at 224 (illustrating how "factors like socioeconomic status, employment status, and marital status" in risk assessments compound institutionalized discrimination).

public information that can be used in a discriminatory way, people have a reason to be alarmed at how their data can have serious implications on their livelihood and even their freedom.[164]

With no real power over who accesses their data, people need more agency over their own data through a disclosure framework.[165] With the Private Information Reporting System, individuals may enter the platform, see who can access their personal data, and restrict access to any company.[166] The opt-in framework is meaningful because users must visit website and affirmatively allow companies to access their data by accepting cookies; but for extra security, this Note suggest a secondary step, providing users a central space to sign-on and choose to opt out of where their data is being used.[167] The central space also applies to public information that may be used for discriminatory purposes—restricting risk assessment tools from gaining access and accumulating discriminatory data against defendants to predict recidivism.

### *VI. Solving the Data Access Problem*

There are serious concerns over how companies and the government can access individuals' data.[168] Search engines can

164. *See* Julie E. Cohen, *Examined Lives; Informational Privacy and the Subject as Object,* 52 STAN. L. REV. 1373, 1391 (1999) ("Recognizing property in personally-identified data risks enabling more, not less, trade and producing less, not more, privacy.").

165. *See* Jay P. Kesan et. al., *Information Privacy and Data Control in Cloud Computing: Consumer, Privacy Preferences and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 346 (2013) (urging transparency and empower consumers to make privacy decisions through a centralized disclosure system).

166. *See id.* at 346–347 (proposing that under the right of data control, consumers would have the ability to view, challenge, and remove data companies collect).

167. *See id.* (using a personal profile, users can control whether companies can use their data).

168. *See id*. at 379 (comparing the governments method of collecting and using individuals' data online to a Panopticon—a tower utilized by prisons where guards can monitor all the prison cells without the prisoners knowing they are being observed); *see also* Brooke Auxier et, al., *Americans and Privacy: Concerned Confused and Feeling Lack of Control Over Their Personal Information,* PEW RSCH. CTR. (Nov. 15, 2019) (recognizing that 79% of Americans reported being concerned about the way their data is being used by companies) [perma.cc/45QL-RPK8].

package collateral data created by inputting queries into the system and sell them to companies to improve their marketing.[169] Further, the justice system buys data from third parties, resulting in discrimination against communities of color.[170] Part VI addresses these concerns through a disclosure-based solution.

### *A. Disclosure-Based Solutions*

This Note proposes that a disclosure-based solution is the most tenable solution to reign in companies' data overreach and give people more power over their data. The disclosure-based answer is a combination of rights in the market-based and legislation-based solution. It views data as property, granting users complete control and using both opt-in and opt-out structures. The disclosure-based framework offers a centralized platform—the Private Information Reporting System ("PIRS")—serving as a space where users can conveniently access their data. PIRS differs from solutions found in the CCPA and the GDPR because California and Europe's privacy framework is decentralized— calling for users to agree to how their privacy is used by visiting companies' websites. PIRS will not eliminate the step of visiting websites and opting for their data to be used. Instead, PIRS will be a second step where users' decisions from the websites they visit; and information on where their data is held will also show up on PIRS.

Further, the FTC is in the best position to oversee the PIRS. This Section explains why the FTC is the best place to oversee the PIRS. While the FTC is fit to lead the PIRS, people might have a tough time trusting the government overseeing their data. Therefore, this Section discusses various ways to increase consumer trust to ensure that peoples' data is safe and secure.

---

169. *See* ZUBOFF *supra* note 1, at 54 (touching on the lucrativeness of the behavioral data market where companies sell users' data).

170. *See* Humerick, *supra* note 14, at 214 (examining the racial bias that exists in the data used by risk assessment tools).

*1. The Private Information Reporting System*

From the market-based solution, people should have property interests over their data.[171] As contended above, property is information, and data fits well into the property law framework.[172] Dealing with data under property offers more power and control for individuals than they would get under privacy law. Further, the CCPA and GDPR provide ways for individuals to bring private causes of action against companies that overstep and use their data without permission.[173] Typically, an opt-in framework is more robust than opting out because before companies can use people's data, the individual would have to agree to it affirmatively. However, with a centralized platform—PIRS— opting out would be sufficient because individuals can have their data in one place instead of going to the business's website to restrict access.

Proponents of a centralized data protection system contend that an opt-in system would be tenable.[174] However, an opt-in structure for PIRS would be inefficient because the system serves as a second-step space after the user has already decided to opt-in by agreeing to cookies on a business' webpage.

PIRS allows people to view and remove information from various online platforms. People will be able to restrict access to collateral data from search engines. Further data used in predictive sentencing, like socioeconomic factors, can be restricted on the grounds of unconstitutionality.[175]

171. *See* Harris, *supra* note 70, at 225 (contending that with property interests in their data, people will indeed be empowered to control their personal information).

172. *See* Fairfield, *supra* note 94, at 135 ("[P]roperty is information.").

173. *See* Harris, *supra* note 70, at 223 (noting that both the CCPA and GDPR offer ways for consumers to have a private cause of action to vindicate their rights).

174. *See* Kesan et. al., *supra* note 165, at 347 (supporting the Fair Credit Reporting Act's opt-in model).

175. *See* Starr, *supra* note 148, at 235 (sentencing people based on socioeconomic factors is unconstitutional).

### *2. The Federal Trade Commission May Oversee the Private Information Reporting System*

The FTC is the de facto federal data protection authority in the United States.[176] The FTC exercises its data protection authority under Section 5 of the Federal Trade Commission Act gives the FTC ("Section 5").[177] Section 5 prohibits "unfair or deceptive acts or practices in or affecting commerce—" which forms the basis of FTC privacy law.[178] In the absence of a federal data protection statute, Section 5 grants FTC's authority to police unreasonably lax data protection practices by companies.[179]

By the terms of Section 5, the FTC addresses data protection by the "deceptive statements" and "unfairness" legal theories to punish deceptive statements and unfairness employed by companies in their course of business—particularly webpages.[180] The unfairness legal theory is favorable to address internet privacy, framing the FTC's capabilities to oversee PIRS.

---

176. *See* Maxwell E. Loos, *Exposure as Distortion: Deciphering "Substantial Injury" for FTC Data Security Actions*, 87 GEO. WASH. L. REV. ARGUENDO 42, 43 (2019) (protecting consumers by preventing "unfair deceptive acts" in commerce, challenging companies when their unreasonable data security practices unfairly expose sensitive consumer information).

177. *See id*. at 44 (granting the FTC authority to prohibit "unfair or deceptive acts or practices in or affecting commerce").

178. Federal Trade Commission Act § 5, codified as 15 U.S.C. § 45 (2018); *see generally* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND PRIVACY (2016) (enacting the Wheeler-Lea Amendments of the Federal Trade Commission Act in 1938, Congress expanded the power of the Federal Trade Commission, resulting in focusing on preventing unfairness and deception); *see also* 15 U.S.C. § 45(a)(2)

> The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except banks, savings and loan institutions . . . Federal credit unions . . . common carriers subject to the Acts to regulate commerce, air carriers and foreign air carriers . . . and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.

179. *See* Loos, *supra* note 176, at 44 (granting FTC the authority to police data protections under the unfair practices legal theory).

180. 15 U.S.C. § 45.

*a. Deceptive Statements*

The Commission articulates three key elements to conclude that a business made a deceptive statement: there must be "(1) a representation, omission, or practice that is likely to mislead a consumer; (2) the interpretation of that act or practice is considered from the perspective of a reasonable consumer; and (3) the representation must be material."[181] The FTC is not required to evaluate the entire business's practices, and may analyze a single ad, evaluating the "entire advertisement, transaction of course of dealing."[182] Further, each website page may fall under the course of dealing with consumers visiting them, and the FTC considers disclosures made on such pages as material.[183] From this, the FTC may consider misleading both express and implied claims and omissions about a business's services.[184] Also, the FTC considers several factors in determining whether the webpage includes implied representations and omissions, such as other representations made, the order and context in which they were made, the nature of the claim, the heart of the transactions, and surveys from consumers to determine how individuals interpret an implied claim or omission.[185]

*b. Unfairness*

The Commission has authority to prevent objectionable acts and practices under the "unfairness" legal theory.[186] The FTC applies a three-pronged test to determine whether a business's online practices are unfair: the injury must be unfair, it must be

181. *See* HOOFNAGLE, *supra* note 178, at 123 (listing the Commission's elements that qualify deceptive statements).

182. *Id*. at 124.

183. *See id*. (considering websites to fall under course of dealing and material while evaluating deceptive statements).

184. *See id*. (discussing that the FTC may consider express and implied claims and omissions about a business's practices as misleading).

185. *See id*. (naming the factors that the FTC considers when determining whether a company's representations are deceptive).

186. *See id*. at 130 (identifying the "unfairness" element as an independent legal theory under which the Commission may use to prevent reprehensible acts and practices).

substantial, and the injury must not be outweighed by countervailing benefits to competition or consumers produced by the practice, and it must be an injury that could not have been reasonably avoided.[187]

Substantial injury may materialize in the form of monetary harm or coercion into purchasing unwanted goods or services.[188] When it comes to the practices in the data market place there is substantial injury because targeted marketing is based on behavioral manipulation— which brings us to the anecdote at the beginning of this note: would you have gone to the mall that day, and buy snacks at Starbucks but for Pokémon Go?

To classify the online business practice as unfair the practice must not be outweighed by countervailing benefits.[189] During the evaluation, the Commission considers costs to the business and consumer, burdens on society from increased paperwork and regulation, burdens on the flow of information, and incentives for innovation.[190]

Finally, declaring the online business practice as unfair hinges on whether the consumer may practically avoid participating in the business's call to participate.[191] In the internet age, people need cyberspace to navigate the physical world properly; therefore, altogether avoiding these platforms is virtually impossible.[192]

---

187. *See id.* at 132 (demonstrating the three-pronged test to evaluate a business' potential unfair online practices).

188. *See id.* (explaining how monetary harm and coercion may amount to substantial injury).

189. *See id.* at 132 (noting that the injury must be "injurious in its net effects").

190. *See id.* at 132 (outlining that countervailing benefits must not outweigh the business practice in question).

191. *See id.* (determining whether the user may find alternatives to the business' services to avoid the harm done by that business).

192. *See* Laura Hoxworth, *Why Internet Access is a Human Right—and What We Can Do About It*, UVA TODAY (Feb. 5, 2021) (classifying internet access as an essential service, lack of which leads to a digital divide and intensifying education gaps with low-income and communities of color suffering the most) [perma.cc/3PYX-7B6N].

Ultimately companies prefer the unfairness legal theory versus the deceptive one.[193] That's because unfairness is a complete block against the business practice. At the same time, the deceptive legal theory will allow for business practice if the company simply provides better notice and consent procedures.[194] Unfairness practices are harder to overcome even when the consumer is told about them.[195]

### *c. The Unfairness Legal Theory and Online Privacy*

The FTC embraces five fair information practices for how companies should handle data:[196]

1. Notice: data collectors must disclose their information practices before collecting personal information from consumers;

2. Choice: consumers must be given options concerning whether and how personal information collected from them may be used for purposes beyond those for which the information was provided;

3. Access: consumers should be able to view and contest the accuracy and completeness of data collected about them; and

4. Security: data collectors must take reasonable steps to ensure that information collected from consumers is accurate and secure from unauthorized use.

Even though the FTC endorses self-regulatory approaches to promote fair information practices, the Commission has threatened the internet industry to endorse legislation to ensure these practices.[197] Despite FTC's threats and the public's support for the idea of increased privacy, several factors counter serious

193. *See* HOOFNAGLE, *supra* note 178, at 160 (demonstrating that companies prefer cases evaluated under the unfairness legal theory rather than the deceptive one).

194. *See id*. (explaining unfair practices are more difficult to justify versus deceptive statements).

195. *See id*. at 160 (proposing that even when consumers are notifies about the unfair practices and the business works on fixing them, the unfairness practices are still harder to overcome than deceptive statements).

196. *See id*. at 153 (underlining five fair information practices as best practices on how companies should handle users' data).

197. *See id*. (acknowledging that self-regulatory approaches are common as an alternative to codes and regulations).

movement toward heightened privacy over individuals' data: costs imposed on well-defined interests like law enforcement, employers, and national security.[198] Groups representing these interests argue that increased protection over people's data will lead to criminals being able to hide their past wrongs.[199] Revisiting the judicial system, these arguments should not stand. Instead, our efforts should be focused on rehabilitating people, so their history should not be counted against them after they pay their debts to society.

The FTC's authority under Section 5 to address data protection issues allows the Commission to oversee the centralized data protection system, and in doing so, the FTC has the potential to address the distrust that consumers have toward the government. The rest of the note addresses the roots of doubt, how the data marketplace disadvantaged minorities from low socioeconomic status, and how lessons from Do Not Call lists can be easily transferred to Do Not Track lists for data, resulting in greater trust and power over individuals' data.

### *3. Increasing Consumer Trust for Minorities by Adopting the Do Not Track List Framework.*

The United States often relies on self-regulatory systems regarding policy rules.[200] Self-regulation is a type of governance where businesses are entrusted with defining and enforcing rules and their scope.[201] Self-regulatory programs may be reliable because, in most situations, fear of the government or legislation

198. *See id*. (reflecting on the factors that keep policies around data protection from progressing because of the various interest groups that have a stake in normalcy).

199. *See id.* at 153 (rebuking interest groups that defend current attitudes toward increased data protection).

200. *See id*. at 175 (referencing examples such as privacy standards and the American Institute of Certified Public Accountants' Generally Accepted Privacy Standards).

201. *See id*. (showing how businesses are left to govern their own industry practices).

causes businesses to self-regulate.[202] However, the downside to self-regulation is that companies themselves draft the rules and can change them.[203] Further, self-regulation may improperly favor the interests of vital participants in the system— the businesses that create the rules rather than the consumers.[204] Therefore, government agencies may need to step in and make regulations to balance the power between companies and consumers.[205] The Commissions Telemarketing Sales Rule ("TSR") is an example of how the FTC creates regulations to make sure businesses are not abusing their strength over consumers.[206]

The FTC's Telemarketing Sales Rule ("TSR") prohibits calls to consumers who ask not to be called again.[207] Consumers who do not wish for telemarketers to reach them must voluntarily register their telephone numbers on the national Do Not Call Registry, and telemarketers must adjust their call lists to remove any customer who opted out of receiving calls.[208] Under the TSR, consumers also have the right to opt-out of calls from systems that automate telemarketing calls.[209]

The disclosure-based solution is analogous to the Do Not Call Registry enforced through the TSR. Instead of a "Do Not Call List" framework, the disclosure-based solution would use a "Do Not Track List," where users may use the centralized platform to opt

202. *See id.* (attributing the success of self-regulatory programs to fears of problematic government regulations and to the efficiencies that occur when businesses' rely on practices to govern conduct in particular industries).

203. *See id*. at 176 (noting how the ability to draft rules and determine how and when they change them poses the risk that businesses will promote industry interests at the expense of the consumer).

204. *See id*. (acknowledging the power imbalance in self-regulatory systems where the businesses make the rules, and consumers have to accommodate).

205. *See id*. at 175 (pointing out that external for from the government to regulate businesses may be necessary when companies take advantage of consumers).

206. *See* 16 C.F.R. § 310.4(b)(5)(B)(ii)(B) (giving consumers power by creating rules about how telemarketers may contact consumers).

207. *See id.* (creating an opt-out mechanism where customers may request for telemarketers to place requesting customers on a Do Not Call List).

208. *See* § 310.4 (b)(1)(iii)(A) (requiring the consumer to place their name on the Do Not Call lists).

209. *See id*. (mandating that automated telemarketing calls must provide an 'opt-out' mechanism so consumers can communicate their desire for removal from the call list).

out of companies using their data to be included on a Do Not Track list even after they opted in. Using the opt-in measures from the GDPR, users may affirmatively grant companies the right to sell users' data. The system will automatically send information on whether the user allowed or prohibited the business from selling the user's information to the centralized platform. The user's opt-in status will be kept in the business's record and the PIRS, allowing the user to opt-out and change the status through the PIRS platform.

*a. Revisiting the Opt-in and Opt-out approaches*

An opt-out system by itself does not offer strong recourse for consumers in protecting their data.[210] In reality, businesses prefer an opt-out system of consent because it burdens the consumer to act to restrict businesses' power over their data.[211] Further, opt-out structures incentivize companies to hide the option, thus, imposing transaction costs and dissuading its use.[212] For example, AT&T researched and found that it could discourage users from opting out by designing letters explaining how to opt-out from arbitration in complicated ways, so few users took advantage of opting out.[213] Further, the effects of opting out are unevenly distributed, with minorities from low-socioeconomic communities benefiting from these effects.[214] For example, Suntasia Marketing, a Florida-based telemarketing company, deceptively marketed a series of negative-options programs.[215] Suntasia got users to reveal

210. *See* HOOFNAGLE, *supra* note 178, at 181 (burdening users to act to object to data collection or use, as opposed to placing the burden on businesses to request access and allowing users to approve or deny affirmatively).

211. *See id*. (preferring the opt-out structure because it places more burden on the consumer, limiting transaction costs for businesses).

212. *See id*. at 183 (hiding the option to discourage users from utilizing opt-out structures).

213. *See id*. (looking to AT&T which sent very detailed letters, complicating the opt-out process, discouraging users from opting out).

214. *See id*. at 184 (explaining the negative implications of default opt-out structures on minorities from low-income communities).

215. *See Suntasia Marketing Defendants Pay More than $16 Million to Settle FTC Charges,* F.T.C. (Jan. 13, 2019) (discussing how the massive telemarketing scheme defrauded users for profit) [perma.cc/97FD-WM87].

their checking account numbers in exchange for "free" trial offers.[216]

Suntasia's goal was to get as much account information as possible to charge small amounts from thousands of accounts fraudulently.[217] Suntasia's negative-options programs split its consumers into two groups: users who had to opt-in to continue their subscription and those who had to opt-out to end the subscription.[218] Almost all customers in the opt-in group let their subscriptions cancel.[219] Only forty percent of those in the opt-out group ended up canceling their subscriptions.[220] Further, minorities from low-socioeconomic-status (low-SES) areas were 8% less likely to opt out than whites in high-SES areas.[221] Thus, default opt-out options can cause many consumers to stay enrolled in an outright scam.

### *b. Apple Pay's Cryptographic Token Analogy: Anonymizing Purchaser's Information*

The "Do Not Track" concept works well with a telemarketing situation but has limitations for data protection online. Companies can use the Do Not Track list to identify consumers by separating them into buckets— those who opt-in to companies using their data and those who do not. Therefore, the disclosure-based solution requires a higher level of anonymity. Apple Pay's Cryptographic Token offers a framework to anonymize users who refuse to be tracked by businesses' web pages.

Apple Pay is a mobile payment technology that offers users a secure way to pay for goods and services through iOS apps,

---

216. *See* HOOFNAGLE, *supra* note 178, at 184 (exposing user checking account numbers).

217. *See id*. (defrauding consumers to collect information on user checking accounts).

218. *See id*. (requiring users to opt-in to keep their subscription while collecting information on their checking accounts).

219. *See id*. (showing that customers in the opt-in group chose not to opt-in, thus allowing their subscription to expire).

220. *See id*. (identifying that less than half of the opt-out group took affirmative action to cancel their subscriptions).

221. *See id*. (demonstrating that minorities are at a disadvantage in opt-out structures).

watchOS apps, and websites on Safari web browsers.[222] Apple Pay automatically encrypts users' payment information when users make payments through Apple Pay to prevent third parties from accessing it.[223] To ensure anonymity Apple Pay sends payment requests to the Secure Element.[224] The Secure Element then adds the payment data for the specific debit or credit card and merchant, creating an encrypted payment token.[225] Then, the ticket goes through Apple's servers, where it is re-encrypted using the business app's Payment Processing Certificate. Finally, the servers pass the token back to the app for processing.[226] The app can use the business team to pass the encrypted payment to a third-party payment provider to decrypt and process the payment while maintaining the user's personal information.

Using Apple Pay's Cryptographic Token structure, the Private Information Reporting System may maintain user anonymity if a user opts out of businesses collecting his data. The Cryptographic Token structure prevents companies from inadvertently identifying users based on whether they allow or prohibit companies from using their data. The way all this would work is (1) a user visits a website; (2) the user chooses to opt-in, allowing the website to collect their personal information; (3) the user's choice is sent to and recorded on their PIRS profile; (4) If the user changes their mind on giving the webpage access to their personal information, they may restrict access with a click of a button; (5) the Cryptographic Token initiates, sending it to the website, pulling the user's information and anonymizing the user's identity whenever they use the website. Since PIRS distributes the cryptographic token, the system will hold information on which websites the user visits while maintaining anonymity regarding business web pages.

---

222. *See About Apple Pay*, APPLE (explaining Apple Pay's functions) [perma.cc/K2XT-6RZX].

223. *See id*. (encrypting user information immediately when a purchase is initiated).

224. *See id*. (indicating that Secure Element is a dedicated chip on the user's device).

225. *See id*. (describing the role of Secure Element in transactions involving Apple Pay).

226. *See id*. (relying on the re-encryption process so the businesses receiving payment may process their payments without identifying the customer directly).

### *c. Addressing the Private Information Reporting System's Limitations*

The major limitation of PIRS is that consumers do not trust the government to handle their data.[227] The government must work on restoring trust among its citizens so that they enroll in the data protection system. The cryptographic token structure is the first step toward building that trust. The government must overcome the worry about getting hacked before users feel comfortable with the platform. This Note does not discuss ways to overcome the hacking issue, but a cryptographic token is a starting place for users to maintain anonymity to lessen the worry. Future research will be required to find solutions, potentially using blockchain technology to solve hacking issues and increase consumer trust.[228]

## *VII. Conclusion*

The data marketplace leaves individuals vulnerable with no meaningful opportunity to control who can access their personal information.[229] Private companies buy and sell people's information to manipulate their behavior through targeted marketing.[230] The justice system uses risk assessment tools which rely on historically racist data to issue sentences to defendants, leaving minorities from low-socioeconomic communities vulnerable.[231] Treating data as property, and adopting a centralized data disclosure system are important steps to empower people's control over their own data, and resolving behavioral manipulation and discrimination in sentencing. These solutions,

227. *See* David Forsey & Mieke Eoyang, *Surveillance and Encryption*, 2 (2016) (addressing limitations regarding consumer trust and data privacy).

228. *See* Harris, *supra* note 70, at 225 (discussing the role of blockchain technology to increase consumer trust when it comes to data protection).

229. *See* ZUBOFF, *supra* note 1, at 8 (demonstrating the individuals' role in the data marketplace as resources producing data—the commodity— which companies and the justice system purchase).

230. *See id.* at 7 (stating that surveillance capitalism is the unilateral claim over human experience as a free raw material translating into behavioral data).

231. *See* Starr, *supra* note 148, at 230 (construing that by using risk scores based on socioeconomic status, the government endorses sentencing discrimination).

though ambitious, pair well with existing data protection legislation such as the CCPA and GDPR and may protect minorities in the grander data protection framework.