Vanderbilt Journal of Entertainment & Technology Law

Volume 24
Issue 4 *Summer 2022*

Article 2

2016

Where Copyright Meets Privacy in the Big Data Era: Access to and Control Over User Data in Agriculture and the Role of Copyright

Tesh W. Dagne

Where Copyright Meets Privacy in the Big Data Era: Access to and Control Over User Data in Agriculture and the Role of Copyright

*Tesh W. Dagne**

ABSTRACT

The application of big data in different sectors of the economy and its transformative value has recently attracted considerable attention. However, this transformation, driven by the application of advanced technologies that utilize big data—such as the Internet of Things (IoT), artificial intelligence (AI), and software systems—raises concerns about access to and control over the user data that results from the uptake in using digital technologies. This Article examines the role different legal regimes have in framing access to and control over various forms of user data from the perspective of technology users in the agriculture sector. This Article then goes on to inquire whether copyright law in unpublished works can serve as a model for a new form of data regulation that shifts ownership claims towards ensuring access and controlling disclosure.

The current regime regulating access to and controlling user data is the Fair Information Practices model, implemented primarily through private ordering in contractual arrangement—specifically agreements establishing the relationship between users and technology providers, data intermediaries, and data platforms. This Article seeks to provide a framework that recognizes and protects data originators' privacy and economic interests in user data by proposing a trust model of data

* LL. B, LL.M, JSD, Associate Professor, Thompson Rivers University Faculty of Law, Canada. The author would like to thank Professor Margaret Chon and Professor Chidi Oguamanam for their insightful feedback. Early draft of the Article was presented at the 2021 IP Scholars Conference, the 2021 Southeastern Association of Law Schools (SEALS) Conference, and the 2021 M3 Intellectual Property Scholars Workshop. The author appreciates the feedback and suggestions received from participants in these forums. In addition, the author acknowledges feedback from the editorial team of the Vanderbilt Journal of Entertainment and Technology Law. All errors remain those of the author.

sharing. It does so by studying the normative roots underpinning copyright protection of unpublished works under the doctrine of joint authorship in copyright law. Based on these normative roots, this Article argues that a sui generis *legislative framework can be enacted at the federal level, both in Canada and the United States, in order to cater to the interests of technology users regarding data they originate, particularly in terms of activity data, such as farm-operation data and technical data in the form of agronomy data. The Article identifies rights to control disclosure and access data as two minimum rights, which new legislation ought to recognize as flowing from users' authorship of data and their categorization as users of works under copyright.*

TABLE OF CONTENTS

I. INTRODUCTION

The phenomenon of "big data" and its accompanying "datafication" have become significant trends in everyday life.[1] With the application of advanced technologies and the connections that these technologies demonstrate in their deployment on different spheres, new issues in areas of law governing user data have been brought to the forefront of several types of law: copyright law,[2] data privacy protection law,[3] and contract law concerning access to and control over data.[4]

This Article examines the intersection between copyright law and privacy law in the utilization of user data.[5] After demonstrating the inadequacy of protection of the rights and interests of technology users under the current fragmented and unclear legal regimes that address

---

1. *See* VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 6 (2013). The term "datafication" is commonly used to refer to the transformation of information or knowledge about people into a commodity, whereas "big data" describes the practice of drawing new and valuable insights from large datasets to extract value. *Id.* at 6, 15.

2. *See* Sylvia Zhang, *Who Owns the Data Generated by Your Smart Car?* 32 HARV. J.L. & TECH. 299, 305–09 (2018); Shannon L. Ferrell, *Legal Issues on the Farm Data Frontier, Part I: Managing First-Degree Relationships in Farm Data Transfers*, 21 DRAKE J. AGRIC. L. 13, 29–31 (2016).

3. *See generally* Jacob Strobel, *Agriculture Precision Farming: Who Owns the Property of Information? Is it the Farmer, the Company Who Helps Consult the Farmer on How to Use Information the Best, or the Mechanical Company Who Built the Technology Itself?* 19 DRAKE J. AGRIC. L. 239 (2014) (discussing data privacy issues in agriculture); Michael E. Sykuta, *Big Data in Agriculture: Property Rights, Privacy and Competition in Ag Data Services*, 19 INT'L FOOD & AGRIBUSINESS MGMT. REV. 57 (2016) (discussing privacy, ownership, and use of farm data).

4. *See generally* Simone van der Burg, Leanne Wiseman & Jovana Krkeljas, *Trust in Farm Data Sharing: Reflections on the EU Code of Conduct for Agricultural Data Sharing*, 23 ETHICS & INFO. TECH. 185 (2021), https://doi.org/10.1007/s10676-020-09543-1 (last visited May 24, 2021) (discussing how the European Union encourages transparency in using agricultural data via contracts); Ashley Ellixson, Terry W. Griffin, Shannon Ferrell & Paul Goeringer, *Legal and Economic Implications of Farm Data: Ownership and Possible Protections*, 24 DRAKE J. AGRIC. L. 49 (2019) (discussing how farm data may be protectable as a trade secret). Though of limited significance, user data can also be controlled through trade secret law (referred to as confidential information law in Canada). *See* Brian Leopold, *Forecasting Change: Examining the Future of Agricultural Data Processors and Ownership Rights*, 44 J. CORP. L. 403, 415–16 (2018–2019).

5. The term "privacy" is subject to multiple definitions. In its traditional legal definition, privacy's contours range from the right to be left alone, to the right to be free from unreasonable government searches and seizures, the right to have one's home free from certain trespasses and surveillance, and the right to make certain essential human decisions without government interference. *See Privacy*, BLACK'S LAW DICTIONARY (11th ed. 2019). This Article is concerned with legal entitlements to information that bring only one type of privacy concern: control over technology user data. *See* discussion *infra* accompanying note 174. "User data" is defined in this Article broadly as encompassing different categories of data that arise from technology users' activities in diverse spheres, such as agriculture, health, education, etc. *See* discussion *infra* Section II.B. Also, the term "user" in this article should be distinguished from its use in copyright scholarship as juxtaposed to "owner" of copyright.

accessibility, availability, and control over data, this Article proposes a data governance approach of regulating user data under a *sui generis* regime, modeled on copyright. Under this model, the law recognizes technology users as stakeholders in data. As such, they are protected against exploitative, contract-based arrangements through entitlements that allow users to exercise more robust control over the use of their data. The doctrinal foundations of joint authorship in copyright, which recognize the contribution of collaborators,[6] justify protecting the data originator's privacy and economic interests in user data. The model also has a normative basis in authors' copyright claims for the unauthorized, public dissemination of private, unpublished works that are revelatory of an author's identity.

The question of access to and control over data in the big data era, as discussed in this Article, arises with respect to all types and categories of technology user data. This Article, however, will focus specifically on agricultural data because in most jurisdictions, including Canada and the United States, there is no legal regime dedicated to regulating access to or control over agricultural data, unlike other categories of data such as financial or health.[7] Moreover, a focus on agriculture highlights the broad reach of "big data" and "datafication," as agriculture has been significantly disrupted by big data application despite being one of "the most traditional of traditional industries."[8] The impact of big data in this space provides a great setting to study

6. *See* 17 U.S.C. § 101 (A joint work is "work prepared by two or more authors with the intention that their contributions be merged into inseparable or interdependent parts of a unitary whole.").

7. *See* Ellixson et al., *supra* note 4, at 52. In the United States, the Federal Gramm-Leach-Bliley Act regulates the practices of financial institutions in data sharing. Pub. L. No. 106–102, 113 Stat. 1338 (1999) (codified in scattered sections of 12, 15 U.S.C.). In Canada, financial data is generally regulated like other data collected by the private sector in the course of commerce under the Personal Information Protection and Electronic Documents Act (PIPEDA), although certain provisions of the Canada Bank Act may apply. PIPEDA, S.C. 2000, c 5 (Can.); Canada Bank Act, S.C. 1991, c 46 (Can.). In the United States, legislation such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), provides federal-level regulation of health data whereas in Canada, provinces and territories have their own legislative framework for protecting the privacy of personal information (PI), or personal health information (PHI) that is dedicated to regulating health data. Pub. L. No. 104–191, 110 Stat. 1936 (1996) (codified in scattered sections of 26, 29, 42 U.S.C.); *see Healthcare Privacy Legislation in Canada*, COLLEAGA, https://www.colleaga.org/article/healthcare-privacy-legislation-canada [https://perma.cc/9HBP-TCK8**]** (last visited Feb. 22, 2022).

8. Leonard Brody, *The Great Rewrite: Digital Reinvention*, FORBES (Sept. 19, 2018, 12:34 PM), https://www.forbes.com/sites/kpmg/2018/09/19/the-great-rewrite-digital-reinvention/?sh=4de3ce183a8a [https://perma.cc/6JZX-Y6ST]; J.E. Relf-Eckstein, Anna T. Ballantyne & Peter W.B. Phillips, *Farming Reimagined: A Case Study of Autonomous Farm Equipment and Creating an Innovation Opportunity Space for Broadacre Smart Farming*, NJAS – WAGENINGEN J. LIFE SCIS., Dec. 2019, at 2.

the role of copyright law as an instrument of reigning in access to and control over data.

In fact, little has been written about the connection between agriculture and copyright, unlike the relationship between copyright and other sectors, such as education. To the extent that scholars have addressed intellectual property (IP) issues in agriculture, the relationship has been characterized by a concern with limited areas of law, such as patents in agrobiotechnology and breeders' rights in plant resources.[9] However, as demonstrated by the considerable media attention given recently to the potential use of big data applications in agriculture, the big data phenomenon has a specific context of application in what is often referred to as digital agriculture or precision farming, in which copyright is invoked as an instrument of control over data.[10]

Similar to the emergence of digital health and digital biology, digital agriculture involves using technology and data collection to inform more efficient, timely, and site-specific farm practices.[11] In this

---

9. *See generally* Keith Aoki, *Food Forethought: Intergenerational Equity and Global Food Supply—Past, Present, and Futur*e, 2011 WIS. L. REV. 399 (2011) (discussing intellectual property rights in plant genetic resources); Chidi Oguamanam, *Agro-Biodiversity and Food Security: Biotechnology and Traditional Agricultural Practices at the Periphery of International Intellectual Property Regime Complex*, 1 MICH. ST. L. REV. 215 (2007) (discussing intellectual property regarding agro-biodiversity and food insecurity); Zachary Lerner, *Rethinking What Agriculture Could Use: A Proposed Heightened Utility Standard for Genetically Modified Food Patents*, 55 U. KAN. L. REV. 991 (2007) (discussing patent law regarding GM agriculture); Benjamin M. Cole, Brent J. Horton & Ryan Vacca, *Food for Thought: Genetically Modified Seeds as De Facto Standard-Essential Patents*, 85 U. COLO. L. REV. 313 (2014) (discussing patent licensing for genetically modified seeds); Jay Dratler, Jr., *Food Patents: The Unintended Consequences*, 8 AKRON INTELL. PROP. J. 1 (2015) (discussing patent law relating to food); Tesh Dagne, *Protecting Traditional Knowledge in International Intellectual Property Law: Imperatives for Protection and Choice of Modalities*, 14 J. MARSHALL REV. INTELL. PROP. L. 25 (2014) (discussing the protection of traditional knowledge through intellectual property law).

10. *See, e.g.*, Norman Mayersohn, *How High Tech Is Transforming One of the Oldest Jobs: Farming*, N.Y. TIMES, https://www.nytimes.com/2019/09/06/business/farming-technology-agriculture.html [https://perma.cc/T9YH-G5JM] (June 13, 2020); Dan Maycock, *The New Data Wave In Agriculture*, FORBES (Dec. 11, 2020, 7:20 AM), https://www.forbes.com/sites/forbestechcouncil/2020/12/11/the-new-data-wave-in-agriculture/ [https://perma.cc/RN3Z-T77W]; Aaron Pressman, *A.I. Gets Gown in the Dirt as Precision Agriculture Takes Off*, FORTUNE (Oct. 5, 2020, 7:00 AM), https://fortune.com/2020/10/05/a-i-precision-agriculture-deere/ [https://perma.cc/GL9B-GC93]; Raviv Itzhaky, *Artificial Intelligence and Precision Farming: The Dawn of the Next Agricultural Revolution*, FORBES (Jan. 7, 2021, 7:50 AM), https://www.forbes.com/sites/forbestechcouncil/2021/01/07/artificial-intelligence-and-precision-farming-the-dawn-of-the-next-agricultural-revolution/ [https://perma.cc/V84E-3BGR].

11. *See generally* Bertalan Meskó, Zsófia Drobni, Éva Bényei, Bence Gergely & Zsuzsanna Győrffy, *Digital Health Is a Cultural Transformation of Traditional Healthcare*, 3 MHEALTH 38, 38 (2017) (discussing the emerging role of disruptive technology in the practice of medicine). "Digital biology" refers to the emergence of "the tsunami of genomic information … in research laboratories the world over," derived from physical genetic resources using the next generation

respect, access to and control over technology users' data have become the new frontiers of competition among stakeholders in the evolving agricultural landscape, defined by the interconnection between machinery, digital technology, software, and big data applications.[12] For example, a farmer incorporating digital agriculture methods may use a state-of-the-art combine harvester to harvest a season's crop.[13] Such machinery is equipped with technology to steer itself.[14] It has AI sensors that collect all kinds of data on soil moisture levels, soil nutrients, the location of different crop types, and the volume of crops harvested.[15] The farmer can track all of these categories of data and the corresponding agronomic practices, field notes, and other information using a farm management app on a tablet, like the MyJohnDeere app.[16] This data is typically uploaded onto the cloud (i.e., software and services that run on the Internet, instead of locally on a computer) and shared

technologies. Peter W. B. Phillips, Stuart J. Smyth & Jeremy de Beer, *Access and Benefit-Sharing in the Age of Digital Biology*, *in* GENETIC RESOURCES, JUSTICE AND RECONCILIATION 181–95 (Chidi Oguamanam ed., 2018); *see also* Section II.B (discussing the sphere of activities and technologies describing "digital agriculture").

12. Various scholarly works address access to and control over agricultural data. *See generally* Neal Rasmussen, *From Precision Agriculture to Market Manipulation: A New Frontier in the Legal Community*, 17 MINN. J.L. SCI. & TECH. 489 (2016) (discussing ownership of agricultural data in the commodities market); Sykuta, *supra* note 3 (discussing industry guidelines concerning data privacy and security for farmers and ag data service providers); John Soares, *The New Frontier: How Sharing of Big Data in Agriculture Interferes with the Protection of Farmers' Ownership Rights Over Their Data*, 26 SAN JOAQUIN AGRIC. L. REV. 229 (2016–2017) (discussing ambiguities of ownership over agricultural data between farmers and agricultural companies); Strobel, *supra* note 3 (discussing data privacy rights for precision agriculture farmers); Ellixson et al., *supra* note 4 (discussing farmers' ability to own farm data); Leopold, *supra* note 5 (discussing privacy and data concerns, specifically regarding property rights, for local farmers due to agricultural data innovations).

13. Scott Carpenter, *Access to Big Data Turns Farm Machine Makers into Tech Firms*, FORBES (Dec. 31, 2020, 10:56 PM), https://www.forbes.com/sites/scottcarpenter/ [https://perma.cc/766M-MQSP]. The scenarios and discussion of digital agriculture in this Article are set in the context of smallholder farmers that are key sources of food and agriculture in the world, as opposed to industrial farmers, although the task of defining "smallholder farmer" is difficult due to the heterogeneity of the group. *See* Devangana Kalita, Freida M'Cormack & Jonas Heirman, *A Literature Review on Farmer Voice* 8 (ALINE, Working Paper No. 3, 2012).

14. Tanya M. Anandan, *Cultivating Robotics and AI for Sustainable Agriculture*, ASS'N. ADVANCING AUTOMATION (July 22, 2019), https://www.automate.org/industry-insights/cultivating-robotics-and-ai-for-sustainable-agriculture [https://perma.cc/HWF8-RCDX].

15. Natalie Gagliordi, *How Self-Driving Tractors, AI, and precision Agriculture Will Save Us from the Impending Food Crisis*, TECHREPUBLIC (Dec. 12, 2018, 7:50 AM), https://www.techrepublic.com/article/how-self-driving-tractors-ai-and-precision-agriculture-will-save-us-from-the-impending-food-crisis/ [https://perma.cc/EB77-ZE4U].

16. *Id.*

with the company that owns the app, i.e., John Deere.[17] Through an AI application integrated with the app to process the collected historical data, the farmer will usually receive recommendations for the following year's harvest.[18]

The data collected during the farmer's use of the high-tech farm equipment is of significant interest for many reasons; if the farmer in the above example rents the land, that data could be sold to the landowner so that the landowner can charge the farmer based on the land's productivity.[19] The data could also be used to assess how specific varieties of seed and hybrids belonging to affiliates of John Deere are cultivated on such farm fields.[20] The data could also be used to recommend the company's preferred agricultural inputs (e.g., pesticides and herbicides) for the farm.[21] Moreover, the data could be sold to other actors in the agribusiness value chain, who could either determine the price of products or target the farmer in their advertisements based on the detailed data collected.[22] Likewise, hedgers and speculators in the commodity market are interested in this data.[23] As a result, there is a growing market for data of this kind among brokers (also called data intermediaries) who specialize in collecting and then selling data to whoever is willing to buy it.[24] In addition, the data could simply be

17. *See* Laurie Bedord, *John Deere Addresses the Ongoing Risks of Living in a Digital World*, SUCCESSFUL FARMING (Apr. 23, 2021), https://www.agriculture.com/news/technology/john-deere-addresses-the-risks-of-living-in-a-digital-world [https://perma.cc/P4BM-RXD7].

18. *See* Directorate General for Parliamentary Rsch. Servs., *Precision Agriculture and the Future of Farming in Europe: Annex 1: Technical Horizon Scan*, at 16 (2016), https://www.europarl.europa.eu/RegData/etudes/STUD/2016/581892/EPRS_STU(2016)581892_EN.pdf [https://perma.cc/SHS3-HGMG].

19. *Fixed and Flexible Cash Rent Agreements for Your Farm*, PURDUE UNIV. CTR. FOR COM. AGRIC. (Dec. 1, 2011), https://ag.purdue.edu/commercialag/home/resource/2011/12/fixed-and-flexible-cash-rent-agreements-for-your-farm/ [https://perma.cc/NH7Y-YLYN].

20. *See* Eric Rosenbaum, *Deere's Farm Version of Facial Recognition Is Coming to Gields in 2021*, CNBC (Dec. 10, 2020, 11:11 PM), https://www.cnbc.com/2020/12/10/deeres-farm-version-of-facial-recognition-is-coming-to-fields-in-2021.html#:~:text=Deere's%20farm%20version%20of%20facial%20recognition%20is%20coming%20to%20fields%20in%202021,Published%20Thu%2C%20Dec&text=Five%20years%20after%20acquiring%20the,on%20farms%20in%20summer%202021 [https://perma.cc/8YVZ-GQ7M].

21. *See Factory Fresh*, ECONOMIST: TECH. Q., https://www.economist.com/technology-quarterly/2016-06-09/factory-fresh [https://perma.cc/5U7E-M668] (last visited Feb. 19, 2021).

22. *See generally* ALEXANDER ANDRASON & FRANCOIS VAN SCHALKWYK, OPPORTUNE NICHES IN DATA ECOSYSTEMS: OPEN DATA INTERMEDIARIES IN THE AGRICULTURE SECTOR IN GHANA (2017), https://papers.ssrn.com/abstract=2949722 [https://perma.cc/797A-N2MQ] (select "Download this Paper") (studying the emergence of open data intermediaries in the agriculture sector of Ghana).

23. *See* Rasmussen, *supra* note 12, at 503.

24. Lois Beckett, Pro Publica, *Big Data Brokers: They Know Everything About You and Sell It to the Highest Bidder*, GIZMODO (Mar. 18, 2013, 10:11 AM), https://gizmodo.com/big-data-brokers-they-know-everything-about-you-and-se-5991070 [https://perma.cc/Z7QV-TDF6]; Yael

stored indefinitely for undefined purposes in the future.[25] These various uses of agricultural data give rise to a range of legal issues that vary based on the type of agricultural data involved.

The dominant mechanism for regulating access to and control over user data is private ordering via contract-based ownership arrangements which allocate the various rights and duties of users in their relationship with technology providers, data intermediaries, and data platforms.[26] In general, questions arise over whether such standard-form contracts, governed by conventional principles of contract law, are adequate to protect the interests of data originators due to three major problems: (1) practical difficulties inherent in making privacy choices, (2) structural power imbalances, and (3) inherent legal limitations that make contractual arrangements for access and control over data ineffective. This contract-based ownership structure is often reinforced through copyright assertions, which underlie claims of how data are accessed, controlled, and shared.[27] Data collectors and processors assert proprietary and ownership control over data, limiting the originators' access to it.[28] Even though privacy regimes cater to technology users' interests in their personal data, such regimes are not generally relevant to data originators – such as farmers – once the data is aggregated, anonymized, or de-identified.[29] Even in the absence of aggregation and de-identification, the scope of what constitutes "personal data" under privacy regimes does not correspond with agricultural data in many circumstances.[30] Besides, data could be observed from technology users or inferred and derived from the data they provide or the technology they use.[31] In this context, this Article addresses the question: What recourse do technology users such as farmers have to ensure access to the vast amount of data that originates

---

Grauer, *What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?*, VICE (Mar. 27, 2018, 9:00 AM), https://www.vice.com/en/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection [https://perma.cc/K3GS-4KKQ].

25. *Cf.* Jacob Bunge, *Big Data Comes to the Farm, Sowing Mistrust*, WALL ST. J. (Feb. 25, 2014, 10:38 PM), https://www.wsj.com/articles/SB10001424052702304450904579369283869192124 [https://perma.cc/D55C-5MP6] (enumerating farmers' fears about potential future uses of big data).

26. *See* discussion *infra* Part V.

27. *See* discussion *infra* Section V.B.

28. *See generally* Pamela Andanda, *Towards a Paradigm Shift in Governing Data Access and Related Intellectual Property Rights in Big Data and Health-Related Research*, 50 IIC – INT'L REV. INTELL. PROP. & COMPETITION L. 1052 (2019) (discussing how data collectors and processors approach data ownership and access in the healthcare setting).

29. *See* discussion *infra* Section V.B.

30. *See* discussion *infra* Section V.B.

31. *See* Ferrell, *supra* note 2, at 16.

from their use of technology, and how do users control the transfer and sharing of such data in a manner that may not be prejudicial to their interests?

Given the high stakes of technology-based activity for users such as farmers and the food system overall, user data in a specific context of application, such as agriculture, has a special and unique significance for society—compared to, for example, the importance of social media data to social media users.[32] Boilerplate contract mechanisms of data access, control, and sharing between technology users, technology, or platform providers cannot address peculiar problems in different contexts of data applications because the impact of big data and datafication differ based on context.[33] For the same reason, traditional data privacy regimes are insufficient to address the concerns elicited by the digitization and datafication of different sectors.[34] This Article aims to show that in an increasingly complex user-data ecosystem, copyright plays a vital role as an instrument of control over data handled by upstream actors (i.e., data collectors, processors, and aggregators).

Copyright law grants certain economic and moral rights to individuals identified as "authors."[35] Although authorship is primarily defined through an individual's efforts to create copyrightable work, the normative roots of joint authorship doctrine reveal that non-copyrightable works can also be authored.[36] Thus, it is argued that a *sui generis* legal regime could be enacted to entitle "authors" of non-copyrightable works, which are integrated with collaborative works covered by copyright, to certain rights. When data collectors, processors, and aggregators assert copyright ownership over user data through contractual entitlement, the application of copyright law, or use of technology protection measures (TPMs), the data originators should be recognized as contributors to the authorship of such data and be entitled to certain rights.[37] Such recognition is necessary to provide the requisite basis for trust in data sharing, thereby assuring technology

32. *See infra* text accompanying notes 432–36.

33. *See* Kevin E. Davis & Florencia Marotta-Wurgler, *Contracting for Personal Data*, 94 N.Y.U. L. REV. 1 (2019).

34. *See infra* Section V.B. (discussing the inadequacy of data privacy regimes to protect agricultural data).

35. *See* 17 U.S.C. § 102(a).

36. *See* discussion *infra* Section VI.C.

37. TPMs include such things as encryption, passwords, and access controls that are used to block or limit access to a work, or certain actions with respect to the work (e.g., copying). *See* Dean S. Marks & Bruce H. Turnbull, *Technical Protection Measures: The Intersection of Technology, Law and Commercial Licenses*, 46 J. COPYRIGHT SOC'Y U.S.A. 563, 597–98 (1998).

users of their right to access and control data sourced from them.[38] Given the globally pervasive nature of the big data phenomenon,[39] the discussion refers to users' data access and control issues in other jurisdictions. Still, the focus of the inquiry is limited to the legal frameworks of the United States and Canada.

This Article is structured as follows: Part II sets the stage by describing the transformative effect of the big data phenomenon in the deployment of advanced technologies while also defining user data that results from it as the primary subject of analysis. The discussion aims to establish the backdrop against which issues of access and control over user data arise by identifying key players and actors in the user data ecosystem based on specific examples. Part III subsequently sets out the legal questions concerning user data by demonstrating the significance and relevance of the questions, using as an example the ongoing dispute in the American poultry industry where sharing user data with third parties without user consent resulted in litigation. Part IV grounds the Article in the trust model of privacy as opposed to the traditional Fair Information Practices model.

Part V then explores the contract mechanisms and privacy regimes that govern access to and control over user data. While noting that contractual arrangements for data-sharing tend to be exploitative and riddled with power imbalances, the discussion shows that user data often lies outside the remit of privacy regimes, thereby resulting in the lack of recourse to data originators in guaranteeing access and securing control.

The discussion in Part VI attempts to lay out a framework for users' claims to data grounded in the normative roots of copyright doctrines, which cater to the privacy interests of authors of copyrightable works. While demonstrating data originators' lack of

---

38. In theories of privacy, trust, and trustworthiness are emphasized as alternatives to earlier theories that are based on the model of fair information practices—a model which focuses on notice to end users and end-user choice, mainly through contracts. *See generally* Christopher W. Savage, *Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy*, 22 STAN. TECH. L. REV. 95 (2019) (arguing that trust is best viewed as a common-pool resource for the online ecosystem to manage); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016) (arguing that privacy can and should be thought of as enabling trust in essential information relationships); Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952 (2017) (arguing that lawmakers should provide more than "Fair Information Practices" in privacy law).

39. *See generally* JAMES MANYIKA, MICHAEL CHUI, BRAD BROWN, JACQUES BUGHIN, RICHARD DOBBS, CHARLES ROXBURGH & ANGELA HUNG BYERS, MCKINSEY GLOB. INST., BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY (2011), https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/big%20data%20the%20next%20frontier%20for%20innovation/mgi_big_data_exec_summary.pdf [https://perma.cc/CB6K-UVLV (providing an overview of the proliferation of big data).

recourse to access and control of data under existing copyright, the discussion also reveals how recent jurisprudential developments enable the appropriation of user data as processed data and in aggregated form, thereby reinforcing the assertion of rights by data collectors, processors, and aggregators at the expense of data originators.[40] In proposing the adoption of a *sui generis* legal framework modeled on copyright law to protect technology users, the discussion in Part VI justifies the assertion that authorship of data has a basis in the doctrine of joint authorship, recognizing the contribution of non-copyrightable works in a joint work.

The argument advanced in this Article is that in circumstances where data collectors, processors, and aggregators assert copyright ownership over user data—whether based on a contractual entitlement or an underlying copyright claim to the work—technology users should be entitled to certain rights that mimic those granted to a contributor to a joint work under copyright. Based on conclusions drawn from such analysis, Part VII defines the nature and content of a potential legislative framework for user data, identifying the minimum right to control data disclosure and access as entitlements that such a framework should accord to users. Lastly, Part VIII offers conclusions and highlights issues for further inquiry concerning different data sets.

II. USER DATA IN THE BIG DATA ERA IN AGRICULTURE

A. The Big Data Landscape

There is presently no working definition for the term "big data."[41] The classic definition of big data comes from a 2001 Gartner report that anchored the definition on several data-specific characteristics called the "three Vs" of big data: volume, velocity, and variety.[42] The report proposed that volume refers to the amount of data, velocity to how rapidly data are produced, and variety to the diversity of the data formats.[43] From a technological point of view, the "three Vs" definition of big data is taken as "high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making,

40. *See* discussion *infra* Section II.B. (discussing various data categories).

41. Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773, 794 (2015).

42. DOUG LANEY, META GROUP, 3D DATA MANAGEMENT: CONTROLLING DATA VOLUME, VELOCITY, AND VARIETY 1 (2001).

43. *Id.* at 1, 2.

and process automation."[44] Later, the concept was expanded to include a fourth V, veracity, which refers to "the level of reliability associated with certain types of data" that brings issues of trust and uncertainty regarding the data and the outcome of the data analysis.[45] According to Cukier and Mayer-Schoenberger, "[b]ig data is also characterized by the ability to render into data many aspects of the world that have never been quantified before; … 'datafication.'"[46] Datafication is commonly understood as putting a phenomenon "in a quantified format so it can be tabulated and analyzed."[47]

Datafication is manifested in a variety of forms. In earlier times, datafication existed when "a relatively small volume of analog data was produced and made available through a limited number of channels."[48] The phenomenon of big data builds on these early forms of datafication by adding new technological units for data collection in the form of near and remote sensors mounted on devices and machinery in a technological infrastructure generally referred to as the Internet of Things (IoT).[49] The IoT technologies collect and aggregate data from multiple data sources in the digital landscape, taking the form of connected cars, wearables, home systems, home appliances, digital assistants, and other technologies.[50] It is, for example, suggested that there will be at least 240 sensors on a new combine harvester and

---

44. *Information Technology Glossary: Big Data*, GARTNER, https://www.gartner.com/it-glossary/big-data/ [https://perma.cc/N2AP-SNXU] (last visited Feb. 21, 2022); Neil M. Richards & Jonathan King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 394 (2014).

45. Francesco Gullo, Giovanni Ponti, Andrea Tagarelli, Salvatore Cuomo, Pasquale De Michele & Francesco Piccialli, *Handling Uncertainty in Clustering Art-Exhibition Visting Styles*, *in* BIG DATA TECHNOLOGIES AND APPLICATIONS 54, 54 (Jason J. Jung & Pankoo Kim eds., 2017).

46. Kenneth Cukier & Viktor Mayer-Schoenberger, *The Rise of Big Data: How It's Changing the Way We Think About the World*, 92 FOREIGN AFFS. 28, 29 (2013).

47. MAYER-SCHÖNBERGER & CUKIER, *supra* note 1, at 78.

48. U.N. GLOB. PULSE, BIG DATA FOR DEVELOPMENT: CHALLENGES & OPPORTUNITIES 8 (2012), https://unglobalpulse.org/wp-content/uploads/2012/05/BigDataforDevelopment-UNGlobalPulseMay2012.pdf [https://perma.cc/D7LC-2VY4]. An example of these early forms of datafication would be data collected from farmers through geographic information (GI) system and as global positioning systems (GPS) for the site-specific management of farm. *See* Mark Shepherd, James A. Turner, Bruce Small & David Wheeler, *Priorities for Science to Overcome Hurdles Thwarting the Full Promise of the 'Digital Agriculture' Revolution*, 100 J. SCI. FOOD & AGRIC. 5083, 5083 (2018); Nicoleta Tantalaki, Stavros Souravlas & Manos Roumeliotis, *Data-Driven Decision Making in Precision Agriculture: The Rise of Big Data in Agricultural Systems*, 20 J. AGRIC. & FOOD INFO. 344, 348 (2019).

49. *See, e.g.*, Muhammad S. Farooq, Shamyla Riaz, Adnan Abid, Tariq Umer & Yousaf B. Zikria, *Role of IoT Technology in Agriculture: A Systematic Literature Review*, 9 ELECS. 319, 319–20 (2020).

50. *See* Ramnath Balasubramanian, Ari Libarikian & Doug McElhaney, *Insurance 2030––The Impact of AI on the Future of Insurance*, MCKINSEY & CO. (Mar. 12, 2021), https://www.mckinsey.com/industries/financial-services/our-insights/insurance-2030-the-impact-of-ai-on-the-future-of-insurance [https://perma.cc/2EXT-C754].

upwards of sixty sensors on a new, sizeable, state-of-the-art tractor.[51] These sensors collect all kinds of data in their respective applications, such as soil moisture levels, soil nutrients, location of crop types, and volume of harvested crops.[52]

The digital landscape precipitated by IoT technologies is increasingly transformed by the emergence of software apps and digital platforms in various applications, which embrace AI-based data analytics (i.e., the capability to analyze big data).[53] With the deployment of AI techniques such as machine learning, data analytics are increasingly applied to future decision-making processes in health, agriculture, consumer market, education, and other sectors for predictive and prescriptive analysis.[54] Numerous technology actors have emerged in such diverse sectors to solve various problems using AI, blockchain, and cloud computing.[55] In agriculture, for example, major seed, agrochemical, and equipment suppliers have become technology actors by developing their own data analytics platforms.[56]

Leveraging the potential of big data for growth and innovation in this growing landscape requires finding a balance between diverse interests in data. To properly understand the diverse interests attached to data actuated by big data, it is first necessary to identify the various categories of data generated and collected, and then to define the ecosystem of actors with a stake in these categories of data.

B. Categories of User Data

User data in this Article can be understood as encompassing diverse categories of data stemming from individuals' use of technology that has data collection capability in general, instead of the narrower

---

51. J. E. Relf-Eckstein, Anna T. Ballantyne & Peter W. B. Phillips, *Farming Reimagined: A Case Study of Autonomous Farm Equipment and Creating an Innovation Opportunity Space for Broadacre Smart Farming*, NJAS – WAGENINGEN J. LIFE SCIS., Dec. 2019, at 3.

52. *Id.* at 1.

53. Shepherd et al., *supra* note 48, at 5085.

54. *See* JACQUES BUGHIN, ERIC HAZAN, SREE RAMASWAMY, MICHAEL CHUI, TERA ALLAS, PETER DAHLSTROM, NICOLAUS HENKE & MONICA TRENCH, ARTIFICIAL INTELLIGENCE: THE NEXT DIGITAL FRONTIER?, MCKINSEY & CO. 22 (2017), https://www.mckinsey.com/~/media/mckinsey/industries/advanced%20electronics/our%20insights/how%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/mgi-artificial-intelligence-discussion-paper.ashx [https://perma.cc/8SM3-TRCR].

55. *See infra* Section II.C.

56. Syngenta, Bayer, BASF, Agricum and DuPont Pioneer's Encirca have all made a name for themselves as data holders and data specialists. *See* Jason Davidson, *Bayer, Monsanto and Big Data: Who Will Control Our Food System in the Era of Digital Agriculture and Mega-Mergers?*, Friends of the Earth (2018), https://foe.org/blog/bayer-monsanto-big-data-will-control-food-system-era-digital-agriculture-mega-mergers/ (last visited May 24, 2021).

category of personal data, as often understood in data protection law.[57] The web of interests surrounding user data can be distinguished according to the various data categories relating to the origin of the data. User data in various sectors become subject to multiple forms of control (e.g., privacy, technical, and ownership control) by different actors as it transitions through the chain of value additions after initial collection.[58] Therefore, it is essential to categorize the different varieties of user data based on the source. Legal entitlements to data are determined through the value added at the point of origin in each case.

The first category of user data in the era of big data is technical data. Technical data are collected using sensors and tracking technologies in digital applications, such as wearable technologies for humans (e.g., Fitbit), global positioning systems deployed on a farm, yield monitors, and variable rate application systems that result in highly detailed digital data.[59] Typical examples of technical data would be agronomic data (collected about a farm using state-of-the-art sensors mounted on farm equipment), animal monitors, and tracking technologies to measure soil quality and nutrients, moisture levels, and crop yields, *inter alia*.[60] Machinery that is now typically equipped with digital sensors includes tractors, harvesters, sprayers, seeders, and irrigation systems.[61]

The second category of data is activity data, which encompasses things like farm operation data and daily nutrition and diet data.[62] Unlike the aforementioned technical data, which are automatically collected through sensors, activity data are often entered into a software system through keystrokes.[63] For example, farm operation data are data about the farmer's activities captured using a growing

57. *See* discussion *infra* Section V.B defining "personal data" under privacy regimes.

58. Lee Rainie & Janna Anderson, *Code-Dependent: Pros and Cons of the Algorithm Age*, PEW RSCH. CENTER. (Feb. 8, 2017), https://www.pewresearch.org/internet/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age/ [https://perma.cc/YS7C-2H7Z].

59. Shane A. Lowe & Gearóid ÓLaighin, *Monitoring Human Health Behaviour in One's Living Environment: A Technological Review*, 36 MED. ENG'G & PHYSICS 147, 158–59 (2014), https://www.sciencedirect.com/science/article/abs/pii/S1350453313002567?via%3 [https://perma.cc/RSK7-MN33].

60. Imran Ali Lakhiar, Gao Jianmin, Tabinda Naz Syed, Farman Ali Chandio, Noman Ali Buttar & Waqar Ahmed Qureshi, *Monitoring and Control Systems in Agriculture Using Intelligent Sensor Techniques: A Review of the Aeroponic System*, 2018 JOURNAL OF SENSORS, Dec. 19, 2018, at 1-18, 1.1 (2018), https://www.hindawi.com/journals/js/2018/8672769/ [https://perma.cc/342M-KW95].

61. *Id.* at 12.

62. *Id.* at 5.

63. *See* Maria Temming, *Smartphones Put Your Privacy at Risk*, COMMONLIT (2018), https://www.commonlit.org/en/texts/smartphones-put-your-privacy-at-risk [https://perma.cc/2KLV-AW87].

number of farm management software applications and platforms, which can be accessed on mobile devices and tablets.[64] Farm management software and platforms transform and externalize farmers' knowledge and practice into data by capturing information that includes records of seeded acres, seed variety, spray dates, pesticide details, animal feed, etc.[65]

The third category of data is machine and device data. This is data automatically recorded during the performance and operation of machinery and incorporates information like engine run-time, speed, GPS location, and the performance of steering, hydraulics, and gearbox systems.[66] Machine data also includes service data, specifically data used for vehicle maintenance and repair.[67]

Meanwhile, technical data, activity data, and machine-and-device data make up what is conventionally referred to as "raw" data, in that it is directly related to the subject of data collection, such as a farm or the human body as a source.[68] Another category of data is often referred to as "cooked" or "processed" data, which is indirectly related to the farm, the human body, or the subject of data collection in general.[69] The distinction between raw data and processed data is based on a metaphorical explanation of the relationship between a set of data and its original source.[70] Raw data is unprocessed, whereas cooked data is processed and analyzed.[71] In reality, though, raw data are often shared

64. According to the *European Union Code of Conduct on Agricultural Data Sharing by Contractual Agreement*, farm operation data can consist of compliance data—the data required for control and enforcement by the competent authorities, as well as agri-supply data (input) relating to the nature, composition, and use of inputs, for example, fertilizer, feedstuffs, or plant protection products. *See* Comm. of Pro. Agric. Orgs., Gen. Confederation of Agric. Coops., Eur. Agric. Mach. Ass'n, Eur. Org. of Agric., Rural & Forestry Contractors, Eur. Seed Ass'n, Fertilizers Eur., Eur. Compound Feed Mfrs. Fed'n, Eur. Crop Prot. Ass'n, Eur. F. of Farm Animal Breeders & Eur. Council of Young Farmers, *EU Code of Conduct on Agricultural Data Sharing by Contractual Agreement*, 4–5, 14, 16 (2018), https://static1.squarespace.com/static/55e8e9ece4b09a2da6c9b923/t/5ae9bfb5aa4a990f066738d4/1525268407672/EU_Code_2018_AgDataSharing.pdf [https://perma.cc/ZF5S-JPLP] [hereinafter *EU Code of Conduct*].

65. *See* Tanha Talaviya, Dhara Shah, Nivedita Patel, Hiteshri Yagnik & Manan Shah, *Implementation of Artificial Intelligence in Agriculture for Optimisation of Irrigation and Application of Pesticides and Herbicides*, 4 A.I. AGRIC. 58, 59–69 (2020).

66. Tiffany Dowell, *Big Data on the Farm (Part I): What Is It?*, TEX. AGRIC. & MECH. AGRILIFE EXTENSION: TEX. AGRIC. L. BLOG (Sept. 1, 2015), https://agrilife.org/texasaglaw/2015/09/01/big-data-on-the-farm-part-i-what-is-it/ [https://perma.cc/M4NB-C4K3].

67. See *EU Code of Conduct*, *supra* note 65.

68. *See* Michael J. Madison, *Tools for Data Governance*, 1 TECH. AND & REGUL. 29, 39 (2020).

69. *Id.*

70. *Id.* at 31.

71. *Id.* at 39.

with either technology providers (TPs) or software and data platform operators through a cloud-based sharing system.[72] Usually, such raw data is processed using data analytics to extract insights relevant to the respective application, such as agricultural production through input-use optimization and better management of natural resources at the farm level.[73] But concerns about access to and control over data arise in legal and technical constraints, which farmers' and other stakeholders' access to processed data of this nature and their control over the destination of the technical data, activity data, and machine and device data. The question that arises here relates to how legal regimes surrounding access to and control over diverse user data sets affect data originators and other stakeholders in the respective data ecosystems. Nevertheless, before addressing this question, the following Section will briefly describe the actors with diverse interests in user data.

C. Participants in User Data Ecosystems

Once user data is collected from a source, such as a farm, it becomes a subject of interest to various stakeholders. The concept of the data ecosystem, derived from the idea of biological ecosystems, best explains the diverse interactions between the actors who contribute to constructing or manipulating data and their related technologies in a particular sector.[74] Technology users are the primary constituents of a data ecosystem.[75] They produce and consume data for their own use, such as making health, consumer, or on-farm decisions.[76]

For example, farmers utilize data to inform and guide decisions that will improve efficiency through more targeted on-farm inputs and

---

72. *Id.* at 41.

73. Alfons Weersink, Evan Fraser, David Pannell, Emily Duncan & Sarah Rotz, *Opportunities and Challenges for Big Data in Agricultural and Environmental Analysis*, 10 ANN. REV. RES. ECON. 19, 21 (2018).

74. Data ecosystem is defined as "a loose set of interacting actors that directly or indirectly consume, produce, or provide data and other related resources." Marcelo Iury S. Oliveira, Glória de Fátima Barros Lima & Bernadette Farias Lóscio, *Investigations into Data Ecosystems: A Systematic Mapping Study*, 61 KNOWLEDGE & INFO. SYS. 589, 604 (2019); *see* JOSHUA GELHAAR & BORIS OTTO, CHALLENGES IN THE EMERGENCE OF DATA ECOSYSTEMS 2 (2020), https://www.researchgate.net/publication/341930759_Challenges_in_the_Emergence_of_Data_Ecosystems [https://perma.cc/KJP9-D2XE]. For the application of data ecosystem approach in data ownership and control, *see* Teresa Scassa, *Ownership and Control over Publicly Accessible Platform Data*, 43 ONLINE INFO. REV. 986 (2019) [Scassa, hereinafter].

75. *See* Oliveira et al., *supra* note 74, at 601.

76. *See* David C. Rose, William J. Sutherland, Caroline Parker, Matt Lobley, Michael Winter, Carol Morris, Susan Twining, Charles Foulkes, Tatsuya Amano & Lynn V. Dicks, *Decision Support Tools for Agriculture: Towards Effective Design and Delivery*, 149 AGRIC. SYS. 165, 165–66 (2016).

automation applications.[77] And linking data on an individual farm basis will increase the productivity and profitability of farming operations by generating prescriptive and predictive insights for the field.[78] However, agricultural data has more pronounced benefits in the production value chain. In this context, value-chain actors such as insurers, storage, and transport logistics providers utilize agricultural data to improve their businesses and market position.[79] Additionally, retailers, processors, and consumers increasingly use technologies to ensure the traceability of products in niche and premium markets like the agricultural market.[80]

While technology users are the primary contributors to the data ecosystem, TPs and data intermediaries have also emerged as significant players. More specifically, TPs deliver hardware tools (such as smart tractors and feed systems) and accompanying software solutions aimed at mining, storing, and processing data.[81] Many such agricultural technology providers (ATPs) have, in fact, seized the opportunity to develop their own data storage and analytics platforms.[82]

Data intermediaries are entities that capitalize on the value of data in the so-called "data marketplace": a platform on which data products are traded.[83] Mostly taking place within an existing value network, such as the agriculture or health sector, data intermediaries match supply and demand for data suppliers and consumers who "use data to gain insights, develop applications, and make decisions."[84] Data

77. *See* Emma Jakku, Bruce Taylor, Aysha Fleming, Claire Mason, Simon Fielke, Chris Sounness & Peter Thorburn, *"If They Don't Tell Us What They Do with It, Why Would We Trust Them?" Trust, Transparency and Benefit-Sharing in Smart Farming*, NJAS – WAGENINGEN J. LIFE SCIS., Dec. 2019, at 4.

78. *Id.* at 5.

79. *Id.*

80. *See generally* ROBERT BARLOW, DREWE FERGUSON, MATTHEW GRACE, VOLKAN DEDEOGLU, ANITA SIKES, CIARA MCDONNELL & SAM BECKETT, DEFINING THE OVERARCHING REQUIREMENTS FOR AUTOMATED PRODUCT VERIFICATION AND THE DEVELOPMENT OF KEY INDUSTRY STANDARDS, FINAL REPORT (2020), https://www.mla.com.au/globalassets/mla-corporate/research-and-development/final-reports/2021/v.rda.2004-final-report.pdf [https://perma.cc/7R58-MYW3].

81. Linly Ku, *10 Agriculture Automation Companies Shaping the Future of Farming*, PLUG & PLAY (Oct. 6, 2021), https://www.plugandplaytechcenter.com/resources/10-agriculture-automation-companies-shaping-future-farming/ [https://perma.cc/C8RZ-79FA].

82. *See*, *e.g.*, Tobias Buck, *Bayer Keen to Shift Attention from Monsanto Woe to Tech Vision*, FIN. TIMES (Jan. 24, 2019), https://www.ft.com/content/63942794-1b32-11e9-9e64-d150b3105d21 [https://perma.cc/4XBA-LPE7].

83. Markus Spiekermann, *Data Marketplaces: Trends and Monetisation of Data Goods*, 54 INTERECONOMICS 208, 210 (2019).

84. Jeremiah Baarbé, Meghan Blom & Jeremy de Beer, *A Data Commons for Food Security* 8 (Afr. Innovation Rsch., Working Paper No. 7, 2019), https://jeremydebeer.ca/wp-content/uploads/2017/08/A-Data-Commons-for-Food-Security-WP-7.pdf [https://perma.cc/F2JF-SRKT].

intermediaries comprise data platforms, vendors, and consumers. The category of intermediaries referred to as "data platforms" enables others to upload and sell their data products, subject to varying licensing models.[85] Data vendors (also called data brokers, data aggregators, consolidators, or resellers) gather data into privately-held infrastructures and offer it to others, mainly for a given fee.[86]

Data intermediaries can gather data from both public and private sources.[87] They then scale "small data" and mash them with big data "to construct a suite of derived data products, wherein value is added through integration and data analytics, creating profiles of individuals, groups and places, and predictions."[88] In agriculture, for example, data consumers in the data marketplace may be comprised of the farmers themselves, agricultural input providers, and various actors in the agricultural product value chain (such as wholesalers, futures traders, and hedgers).[89]

Indeed, this type of data provides more value for technology users once it is converted into information suitable for decision-making (using analytic data techniques) than it does if stored in silos.[90] For example, ATPs and data intermediaries often offer farmers data-based "prescriptions" of future farming for a fee, in a pattern that has gained traction as "prescriptive planting."[91] Farmers are required to share

---

85. *See* Annabelle Gawer, *Bridging Differing Perspectives on Technological Platforms: Toward an Integrative Framework*, 43 RSCH. POL'Y 1239, 1240–43 (2014).

86. See generally Fabian Schomm, Florian Stahl & Gottfried Vossen, *Marketplaces for Data: An Initial Survey*, 42 SPECIAL INT. GRP. ON MGMT. DATA REC. 15, 16 (2013); *see also* Laura Palk & Krishnamurty Muralidhar, *A Free Ride: Data Brokers' Rent-Seeking Behavior and the Future of Data Inequality*, 20 VAND. J. ENT. & TECH. L. 779, 810 (2018) (exploring how the commoditization of research data could further inequality in accessing credible data).

87. Rob Kitchin & Tracey P. Lauriault, *Small Data in the Era of Big Data*, 80 GEOJOURNAL 463, 472 (2015).

88. *Id.*

89. *See* COMM. ON A FRAMEWORK FOR ASSESSING THE HEALTH, ENV'T, & SOC. EFFECTS OF THE FOOD SYS., FOOD & NUTRITION BD., BD. ON AGRIC. & NAT. RES., INST. OF MED. & NAT'L RSCH. COUNCIL, A FRAMEWORK FOR ASSESSING EFFECTS OF THE FOOD SYSTEM 11 (Malden C. Nesheim, Maria Oria & Peggy Tsai Yih eds., 2015), https://www.ncbi.nlm.nih.gov/books/NBK305181/pdf/Bookshelf_NBK305181.pdf [https://perma.cc/G6EG-7YDB].

90. *See* Terry W. Griffin, Tyler B. Mark, Shannon Ferrell, Todd Janzen, Gregory Ibendahl, Jeff D. Bennett, Jacob L. Maurer & Aleksan Shanoyan, *Big Data Considerations for Rural Property Professionals*, 2016 J. AM. SOC'Y FARM MANAGERS & RURAL APPRAISERS 167, 169 (2016).

91. Lyndsey Gilpin, *How Big Data Is Going to Help Feed Nine Billion People by 2050*, TECHREPUBLIC (May 9, 2014, 5:02 AM), http://www.techrepublic.com/article/how-big-data-is-going-to-help-feed-9-billion-people-by-2050/ [https://perma.cc/9NSG-DYJM]; Jacob Bunge, *Big Data Comes to the Farm, Sowing Mistrust*, WALL ST. J. (Feb. 25, 2014, 10:38 PM), https://www.wsj.com/articles/SB10001424052702304450904579369283869192124

their agricultural data with ATPs, data platforms, and intermediaries who "process" raw agricultural data to offer solutions and insights, which can then inform and provide guidance in farming decisions.[92]

There is a long history of increased concentration and burgeoning alliances among TPs, data platforms, and various service and product providers that are often built on ensuring access to the different categories of user data.[93] For example, in health, Google recently acquired Fitbit, a pioneer in creating wearable devices and immersive wellness experiences.[94] Google also made a deal for access to patient records from the hospital chain HCA—which operates 181 hospitals and more than two thousand healthcare sites in twenty-one states—so Google can develop healthcare algorithms.[95] Backed by big hospitals, fourteen US health systems recently formed a company to aggregate and sell de-identified data.[96]

Similarly, in agriculture, John Deere collaborates with each of the so-called "Big Six" agricultural input firms for a direct data access gate: BASF, Bayer, Dow, DuPont, Monsanto, and Syngenta.[97]

[https://perma.cc/63LN-FKX5] (discussing how companies are racing to offer prescriptive services to farmers using the data generated from their operations).

92. *See* Zachary R. Trail, *Rights in a Cloud of Dust: The Value and Qualities of Farm Data and How Its Property Rights Should Be Viewed Moving Forward*, 71 ARK. L. REV. 319, 320 (2018).

93. *See* PAT MOONEY, ETC GROUP, BLOCKING THE CHAIN: INDUSTRIAL FOOD CHAIN CONCENTRATION, BIG DATA PLATFORMS AND FOOD SOVEREIGNTY SOLUTIONS 31 (2018), https://www.etcgroup.org/sites/www.etcgroup.org/files/files/blockingthechain_english_web.pdf [https://perma.cc/74AV-GVXX]; Pat Mooney & ETC Group, *The Changing Agribusiness Climate: Corporate Concentration, Agricultural Inputs, Innovation and Climate Change*, 2 CANADIAN FOOD STUD. 117, 118–19 (2015).

94. *See* Rick Osterloh, *Google Completes Fitbit Acquisition*, GOOGLE: THE KEYWORD (Jan. 14, 2021), https://blog.google/products/devices-services/fitbit-acquisition/ [https://perma.cc/9DDJ-779G].

95. *See* Melanie Evans, *Google Strikes Deal with Hospital Chain to Develop Healthcare Algorithms*, WALL ST. J. (May 26, 2021, 4:34 PM), https://www.wsj.com/articles/google-strikes-deal-with-hospital-chain-to-develop-healthcare-algorithms-11622030401 [https://perma.cc/DQ8Y-VDPX].

96. *See* Casey Ross, *Backed by Big Hospitals, a Former Microsoft Executive Wades into the Messy Business of Selling Patient Data*, STAT NEWS (Feb. 17, 2021), https://www.statnews.com/2021/02/17/truveta-patient-data-terry-myerson/ [https://perma.cc/7AH4-A42V].

97. John Deere came to an agreement with the Climate Company to let machines from the former interact with advisory services from the latter. Press Release, Deere & Co., The Climate Corp. & Monsanto, John Deere and the Climate Corporation Expand Precision and Digital Agriculture Options for Farmers (Nov. 3, 2015), https://www.businesswire.com/news/home/20151103005453/en/John-Deere-and-the-Climate-Corporation-Expand-Precision-and-Digital-Agriculture-Options-for-Farmers [https://perma.cc/XHX6-T6KV]. This agreement was investigated by the US District Court for the Northern District of Illinois from the perspective of antitrust concerns, and eventually, parties cancelled the agreement. *See* Complaint at 12, 17, United States v. Deere & Co., No 1:16-cv-08515 (N.D. Ill. Aug. 31, 2016); Press Release, Monsanto Co., Monsanto Terminates Agreement for Sale

Moreover, major agricultural input providers have engaged in the development, acquisition, and investment of data platforms.[98] For example, Monsanto's subsidiary, the Climate Corporation, offers FieldView, an interface that makes agronomic advice available to farmers and interacts with agricultural machines.[99] Bayer has launched a similar service called FieldManager, while BASF uses the Maglis interface and DowDuPont the Encirca platform.[100]

Mergers and reciprocal relationships across TPs, service and product providers, data intermediaries, and data platforms raise significant competition governance and antitrust issues, which are explored elsewhere.[101] A problem that is pertinent to this Article–which has not received a level of attention proportional to the stakes involved[102] —is the question of data access and control among data originators, such as farmers who produce data, and the many other players who collect, aggregate, process, and utilize such data to improve

---

of Precision Planting Equipment Business (May 1, 2017), https://www.businesswire.com/news/home/20170501006241/en/Monsanto-Terminates-Agreement-for-Sale-of-Precision-Planting-Equipment-Business [https://perma.cc/4NTJ-3FTW].

98. *See, e.g.*, *FieldView Brochure*, CLIMATE FIELDVIEW, https://fieldviewbrochure.com [https://perma.cc/AU9Q-BHLS] (last visited May 25, 2021); Press Release, BASF, BASF Launches Maglis, a New Online Platform to Help Farmers Improve Crop Management (Mar. 3, 2016), https://www.basf.com/global/en/media/news-releases/2016/03/p-16-140.html [https://perma.cc/4KH9-QYKV]; *Granular*, PIONEER, https://www.pioneer.com/home/site/us/encirca/ [https://perma.cc/2FUW-6VDZ] (last visited May 25, 2021).

99. *FieldView Brochure*, *supra* note 98.

100. *Field Manager*, XARVIO, https://www.xarvio.com/us/en/products/field-manager.html [https://perma.cc/UA2S-QUED] (last visited Mar. 13, 2022); Press Release, BASF, *supra* note 98; *Granular*, *supra* note 98. Field Manager was divested to BASF as in the scope of the remedy package of the Bayer/Monsanto decision. *See* Press Release, BASF, BASF Closes Acquisition of Business and Assets from Bayer (Aug. 1, 2018), https://www.basf.com/global/en/media/news-releases/2018/08/p-18-285.html [https://perma.cc/LX2F-TDZS].

101. Can Atik & Bertin Martens, *Competition Problems and Governance of Non-personal Agricultural Machine Data: Comparing Voluntary Initiatives in the US and EU* 15 (Tilburg L. & Econ. Ctr., Discussion Paper No. 031, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3766293 [https://perma.cc/W6CS-CCKD] (select "Open PDF in Browser"); Ioannis Lianos & Dmitry Katalevsky, *Merger Activity in the Factors of Production Segments of the Food Value Chain: A Critical Assessment of the Bayer/Monsanto Merger* 1 (Univ. Coll. London Ctr. for L., Econ. & Soc'y, Pol'y Paper No. 1, 2017), https://www.researchgate.net/publication/336665790_Merger_Activity_in_the_Factors_of_Production_Segments_of_the_Food_Value_Chain_-_A_Critical_Assessment_of_the_BayerMonsanto_merger [https://perma.cc/XE7Q-4258]; MAURICE E. STUCKE & ALLEN P. GRUNES, THE KONKURRENZ GRP., AN UPDATED ANTITRUST REVIEW OF THE BAYER-MONSANTO MERGER 1 (2018), https://www.farmaid.org/wp-content/uploads/2018/03/An_Updated_Antitrust_Review_of_the_Bayer-Monsanto_Merger-03.06.2018.pdf [https://perma.cc/8AXQ-GTM3]; Tom Verdonk, *Planting the Seeds of Market Power: Digital Agriculture, Farmers' Autonomy, and the Role of Competition Policy*, *in* REGULATING NEW TECHNOLOGIES IN UNCERTAIN TIMES 105, 112–16 (Leonie Reins ed., 2019).

102. *See* Kelly Bronson & Irena Knezevic, *The Digital Divide and How It Matters for Canadian Food System Equity*, 44 CANADIAN J. COMMC'N POL'Y PORTAL 63, 64 (2019).

their business and market position. For example, there is a growing concern that the concentration of agricultural data in the hands of just a few large companies could privilege these companies at the expense of farmers, thereby endangering both competition in the agri-food sector and the provision of certain essential public goods through agriculture.[103]

III. ACCESS TO AND CONTROL OVER USER DATA: THE RECOURSE THAT IS AVAILABLE TO DATA ORIGINATORS

Given the centrality of big data to the transformative effect of the current digital economy, significant questions arise about who should have access to the vast amount of data that results from individuals' use of technology in different contexts and who controls the destination of this data. For example, other agricultural actors—who capitalize on digital agriculture to influence farm decisions and claim a share in the benefits of farm operations – increasingly threaten farmers' access to and control over agricultural data.[104] Despite the abundance of data that is generated through digital agriculture activities, counterintuitively, farmers are increasingly faced with "data drought."[105] In this respect, digital agriculture brings additional concerns into the distribution of power and autonomy in agricultural systems on account of access to and control over data.

Many authors and commentators in the social sciences have pointed out that control over massive datasets could give TPs, data intermediaries, data platforms, and others who access these datasets an unfair competitive advantage in the marketplace.[106] For example, employers, insurance companies, pharmaceutical data mining companies, drug manufacturers, and medical researchers all want access to patients' data to conduct research, assist treatment, provide coverage, assess opportunities, process claims, and market products.[107]

---

103. *See* Katarzyna Kosior, *Towards a New Data Economy for EU Agriculture*, 23 STUDIA EUROPEJSKIE - STUD. EUR. AFFS. 91, 92–93 (2019); Bronson & Knezevic, *supra* note 102, at 65.

104. *See* Atik & Martens, *supra* note 101.

105. *See* Shely Aronov, *Can Farmers Beat the Data Drought?*, FORBES (Jan. 19, 2021, 8:30 AM), https://www.forbes.com/sites/forbestechcouncil/2021/01/19/can-farmers-beat-the-data-drought/?sh=44bee18c14ef [https://perma.cc/VYX7-P8BE].

106. *See* Sykuta, *supra* note 3, at 59; Keith Coble, Shannon Ferrell & Terry Griffin, *Big Data in Agriculture: A Challenge for the Future*, 40 APPLIED ECON. PERSPS. & POL'Y 79, 84 (2018); Leopold, *supra* note 4, at 408; Jody L. Ferris, *Data Privacy and Protection in the Agriculture Industry: Is Federal Regulation Necessary?*, 18 MINN. J.L. SCI. & TECH. 309, 309 (2017).

107. *See* N. Nina Zivanovic, *Medical Information as a Hot Commodity: The Need for Stronger Protection of Patient Health Information*, 19 INTELL. PROP. L. BULL. 183, 183 (2014); *see also* Jianyan Fang, *Health Data at Your Fingertips: Federal Regulatory Proposals for*

Agribusinesses could use data to inform their pricing models for seeds and inputs, depending on the farmer's historical yield data. Similarly, ATPs could sell yield data to commodity traders where the equipment harvests thousands of acres of cropland each year.[108] A legal question arises in these particular examples: How can technology users such as farmers protect data collected from their fields? If this data falls into the hands of competitors or other actors in the agricultural value chain, it could give them an unfair competitive edge through, for example, the discovery of farmer's planting practices, fertilizer use, and pricing.

This question presupposes an asymmetric access and control relationship between data originators and the actors who collect and process this data. Such asymmetry is illustrated in an antitrust lawsuit currently ongoing within the US poultry industry concerning price-fixing allegations based on access to agricultural data.[109] Agri Stats is a database company that gathers information from 95 percent of poultry processors.[110] It tracks twenty-two million birds a day and provides data on the number of egg-laying hens that are on a competitor's farm.[111] This data consequently allows one to predict the number of eggs laid, hatched, and ultimately reared on that farm, all of which are key markers of future production.[112] The data, which includes exhaustive information about the internal operations of the biggest poultry corporations (e.g., bird sizes, product mixes, and financial returns at participating plants), is made available in a monthly report that can only be accessed through an Agri Stats subscription.[113] Several lawsuits by farmers, retailers, and distributors are pending against poultry processors on the ground that these companies have colluded by using information from Agri Stats to keep farmers' wages down while simultaneously inflating bird prices.[114] Although Agri Stats refutes the

---

Consumer-Generated Mobile Health Data, 4 GEO. L. TECH. REV. 125, 135–36 (2019) (describing the ways companies use consumer data).

108. *See* Sam Bloch, *If Farmers Sold Their Data Instead of Giving It Away, Would Anybody Buy?*, THE COUNTER (July 19, 2018, 1:12 PM), https://thecounter.org/farmobile-farm-data/ [https://perma.cc/E9X8-U38A].

109. Christopher Leonard, *Is the Chicken Industry Rigged? Inside Agri Stats, the Poultry Business's Secretive Info-Sharing Service*, BLOOMBERG BUSINESSWEEK (Feb. 15, 2017, 10:00 AM), https://www.bloomberg.com/news/features/2017-02-15/is-the-chicken-industry-rigged [https://perma.cc/7S69-64LU].

110. *Id.*

111. *Id.*

112. *Id.*

113. *Id.*

114. *See* Leah Douglas, *Big Food Versus Big Chicken: Lawsuits Allege Processors Conspired to Fix Bird Prices*, NPR (Feb. 6, 2018, 6:38 PM), https://www.npr.org/sections/thesalt/2018/02/06/583806552/big-food-versus-big-chicken-lawsuits-allege-processors-conspired-to-fix-bird-pri [https://perma.cc/G9GG-YPCU].

allegation of collusion in the antitrust claim,[115] a pertinent question raised in this Article concerns the recourse available to farmers in ensuring access to and control over the kind of agricultural data provided by Agri Stats to chicken processors. Similar scenarios in other domains of the agricultural sector could unfold with agricultural data generated through the digitization of agriculture, and any number of other sectors, given the increasing shift toward data and datafication across the board, as shown in the discussion in the previous Part.[116]

The legal discussion surrounding user data is often concerned with data privacy.[117] Nevertheless, a key element in the transactional relationship between technology users, TPs, data intermediaries, and data platforms relates to data ownership, which directly affects who controls and benefits from agricultural data. Access to user data is often discussed in the context of property—to own is to have access.[118] Thus, it is important to examine who owns user data and exercises access to and control over it, especially when data is shared with many actors in the specific data ecosystems, such as in digital agriculture.

IV. CREATING TRUST IN BIG DATA: INEFFECTIVENESS OF THE FAIR INFORMATION PRACTICES REGIME

In the era of big data, privacy norms have evolved to the extent that early principles governing the collection, use, and sharing of data are not considered up to the task of governing new privacy harms.[119] In the first wave of privacy protection during the age of personal computing in the 1970s, the Fair Information Practices (FIPs) emerged as model principles governing responsible data practices.[120] FIPs-based

115. *Id.*

116. *See supra* Section II.A.

117. *See* Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (and Why It Matters)*, N.Y. TIMES: WIRECUTTER (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/9CWY-E8NW].

118. Michael Carolan, *'Smart' Farming Techniques as Political Ontology: Access, Sovereignty and the Performance of Neoliberal and Not-So-Neoliberal Worlds*, 58 SOCIOLOGIA RURALIS 745, 759 (2018).

119. *See* Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 343, 343 (Jane K. Winn ed., 2006); Omer Tene, *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 OHIO STATE L.J. 1217, 1218–19 (2013) (arguing that even updated versions of the FIPs fail to update the definition of personal data, exacerbate the problematic central role of consent, remain rooted on a linear approach to data processing, and problematically continue to view information as "residing" in a jurisdiction).

120. *See generally* CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW: CORPORATE COMPLIANCE AND REGULATION (2d ed. 2007) (providing an overview of data protection laws in the European Union and United States).

approaches to regulating privacy incorporate a set of principles for protecting the privacy of individuals through principles such as data minimization, correction and deletion rights conferral, and industry self-regulation based on notice and consent.[121] The first wave of privacy protection focused on "rectifying mistakes that have contributed to ubiquitous commodification and corporate surveillance," and the second wave of privacy protection—which is currently ongoing—imposes some obligations on data collectors and processors.[122] Privacy protection in the second wave incorporates FIPs like completing privacy impact assessments (PIAs), hiring chief privacy officers (CPOs) and staff, conducting audits, writing and adhering to industry codes of conduct, self-certifying compliance, keeping records and paper trails, automating compliance, and developing internal processes for adjudicating customer rights.[123]

However, privacy scholars and policy makers have pointed out the limitations of the FIPs approach are generally due to its focus on atomistic, rather than holistic, personal autonomy and choice that rely on industries monitoring themselves through ongoing internal compliance to protect individuals' rights to access, correct, delete, and port information.[124] Waldman, a prominent privacy scholar, notes FIPs that have become common in the second wave of privacy "neither materially shift privacy law's political economy nor meaningfully limit the information economy's data-extractive business model."[125]

Therefore, critical privacy scholars have long advocated that privacy law should seek to guarantee values other than atomistic individual rights to privacy.[126] For example, Cohen notes that privacy has social value and "furthers fundamental public policy goals relating to liberal democratic citizenship, innovation, and human flourishing."[127] Nissenbaum conceptualizes privacy in terms of context-specific norms

121. *See* Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 952–53 (2017).

122. Ari Ezra Waldman, *The New Privacy Law*, 55 U.C. DAVIS L. REV. ONLINE 19, 23 (2021).

123. *Id.* at 23.

124. *See* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1905 (2013). *See generally* Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. REV. 543 (2000) (analyzing public-private partnerships in administrative law and approving of private actors as "regulatory resources, capable of producing accountability").

125. Waldman, *supra* note 122, at 22–23.

126. *Id.* at 40.

127. Cohen, *supra* note 124, at 1927.

of information flow.[128] Similarly, there is a growing scholarship that views privacy in relational terms of trust and trustworthiness.[129]

The context-specific information flow aspect of privacy and the value of trust are salient points with respect to the consideration of user-data governance as addressed in this Article. For example, in agricultural data governance, the importance of trust is demonstrated in the farmers' willingness, or lack thereof, to share their data with agribusinesses that develop digital technologies.[130] Studies show that farmers' are reluctant to share their data with technology developers because of the trust concerns arising from procedural worries about transparency and distributional concerns about who benefits from access to and use of farmers' data.[131] After analyzing the EU contractual model for agricultural data sharing through the lens of the literature on trust and contract agreements, Simone van der Burg and her co-authors argue that the contractual models risk protecting agribusinesses in accountability relationships instead of fostering trust, thereby disadvantaging farmers.[132] Lack of trust in agricultural data sharing is mentioned as a current barrier to the uptake of digital agriculture.[133]

In line with critical privacy scholars' attempt to look beyond the traditional model of FIPs, this Article aspires to ground data privacy governance on fostering trust relationships between data originators on the one hand and data collectors, processors, and users on the other. It demonstrates how copyright law can be leveraged to design an alternative *sui generis* framework for technology-user data that guarantees certain rights to be held by farmers as a basis for trust in data sharing.[134] Similar to trust-based proposals for regulating privacy that would impose on industries fiduciary duties of care and loyalty, as

---

128. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 3 (2010).

129. *See* Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11, 11 (2020); *see also* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 50 (2018) ("Information privacy . . . is really a social construct based on trust between social sharers . . . ."); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 456 (2016) ("Intellectual privacy rules produce trust in digital systems that enables engagement with ideas, political association, and truly free speech to flourish.").

130. *See* van der Burg et al., *supra* note 4.

131. Emma Jakku et al., *supra* note 77, at 6–7; *see also* Leanne Wiseman, Jay Sanderson, Airong Zhang & Emma Jakku, *Farmers and Their Data: An Examination of Farmers' Reluctance to Share Their Data Through the Lens of the Laws Impacting Smart Farming*, NJAS – WAGENINGEN J. LIFE SCIS., Dec. 2019, at 6–7.

132. *See* van der Burg et al., *supra* note 4.

133. Shepherd et al., *supra* note 48, at 5087.

134. *See infra* Part VI.

defined by the common law, this Article proposes the recognition of access rights and control of disclosure in copyrights that would form a basis for the transactional relationship between agricultural data ecosystem players.[135]

The discussion in the following Part makes a case for staking new ground for user-data governance by first addressing the nature of access to and control over user data and how the legal relationship between data originators and other actors who collect, process, and utilize such data is defined and protected under existing law. Then, after exploring the current state of the law and demonstrating the potential power imbalance it creates in favor of TPs, data intermediaries, and data platforms, the discussion centers on how the law should structure such a relationship by modeling copyright.

V. EXISTING MECHANISMS FOR ACCESS TO AND CONTROL OF DATA

To a large extent, contract law, data protection law (also called data privacy law), and ownership regimes govern the relationship between data originators and others who access and control data.[136] Contractual stipulations regulate the relationship between technology users functioning as data originators, such as farmers and other actors like data collectors, processors, and users, giving technology users a private cause of action against a contracting party concerning the type of data addressed by the relevant contract.[137] While privacy regimes generally serve the interests of data originators in accessing and controlling certain categories of data, some types of data may be subject to other actors' ownership interests.[138] The discussion in this Part explores the rights and interests of technology users under existing law and arrangements from the perspective of farmers' access and control over agricultural data.

135. *See* Neil M. Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 964–65; Balkin, *supra* note 129; Claudia E. Haupt, *Platforms as Trustees: Information Fiduciaries and the Value of Analogy*, 134 HARV. L. REV. F. 34, 34 (2020).

136. *See generally* Mark Bartholomew, *Intellectual Property's Lessons for Information Privacy*, 92 NEB. L. REV. 746 (2014) (discussing how property and intellectual property concepts map onto information privacy regulation).

137. *See* Davis & Marotta-Wurgler, *supra* note 33, at 682.

138. *See* discussion *infra* Section 5.B.

A. Contracting for User Data

The primary means by which user data is controlled, managed, and shared consist of private ordering mechanisms through terms-of-service agreements, including end-user licensing agreements (EULAs), privacy policies, terms of service, and other online contracts or disclaimers that technology users must agree to before installing software on their phones, tablets, or other hardware.[139] In general, questions arise over whether such standard-form contracts, governed by conventional principles of contract law, are adequate to protect the interests of data originators due to three major problems: practical difficulties inherent in making privacy choices, structural power imbalances, and inherent legal limitations that make ineffective contractual arrangements for access and control over data.

In terms of practical difficulties, data originators use data platforms to store and analyze their data without reading the contractual stipulations that outline which entities are granted access to their data.[140] A survey of farmers in Australia found that 74 percent of respondents "did not know much about the terms and conditions relating to data collection in their agreement with service providers."[141] These contracts usually define the terms of data collection, use, and transfer, and specify which entities are granted access to the farmers' individual and aggregated data.[142] Typically, in such contracts, farmers "own" their data.[143] Representatives for ATPs have publicly stated that farmers will continue to own whatever data are generated by or collected on their operations and can opt out of ATP cloud services if

139. *See* Davis & Marotta-Wurgler, *supra* note 33, at 663; Garrett Ledgerwood, *Virtually Liable*, 66 WASH. & LEE L. REV. 811, 815 (2009).

140. *See* Patricia Sanchez Abril, *Private Ordering: A Contractual Approach to Online Interpersonal Privacy*, 45 WAKE FOREST L. REV. 689, 704 (2010).

141. Wiseman et al., *supra* note 131, at 3.

142. *Id.* at 8.

143. For example, Climate FieldView, Bayor/Monsanto's platform, provides that, "[a]s between [the farmer] and Climate, [the farmer] own[s] all Customer Farm Data." *Climate FieldView Terms of Service*, CLIMATE FIELDVIEW https://climatefieldview.ca/legal/climate-fieldview-terms-of-service [https://perma.cc/97G5-J3Z3] (last updated July 30, 2021). John Deer's platform provides "[the farmers] retain all ownership rights in [their] content." *John Deere User Account Terms and Conditions*, JOHN DEERE, https://www.deere.com/en/privacy-and-data/myjohndeere/terms/ [https://perma.cc/8VM3-S8VP] (Nov. 1, 2021). *See also* Simone van der Burg, Marc-Jeroen Bogaardt & Sjaak Wolfert, *Ethics of Smart Farming: Current Questions and Directions for Responsible Innovation Towards the Future*, NJAS – WAGENINGEN J. LIFE SCIS., Dec. 2019 (discussing ethical challenges raised by smart farming and related to data ownership and access).

they so choose.[144] However, it is unclear what ownership of user data looks like once the data is de-identified (i.e., personally identifiable information is removed from the data) or to which party the data is transferred, even without de-identification.

In terms of structural power imbalances, data originators face information barriers that result in them ostensibly agreeing to have their data collected by corporations.[145] In a typical digital agriculture arrangement, data intermediaries and ATPs perpetually accumulate data from farmers, often in exchange for subscription fees for services on their platforms.[146] However, the value extracted from such data is rarely shared with those farmers.[147] Besides, farmers are usually also unknowingly accepting the terms of ATPs that control or benefit from digital agriculture.[148] In this respect, the power imbalance between data contributors and data aggregators is evidenced by the inability of farmers to negotiate the standard terms of large agribusiness data licenses that govern agricultural technology.[149] Furthermore, farmers may not have control over the data they generate since their use of such data will depend on third-party infrastructure and software.[150] In agreeing to the disclosure of data to third parties, data originators have

144. In its "Guiding Principles on Data and Privacy," for example, the Climate Corporation (a Bayer/Monsanto subsidiary that collects and analyzes agricultural data) has stated that a farmer's shared data will still be owned by the farmer and only used to deliver and improve on the services to which the farmer is subscribed. *See* Mike Stern, *The Climate Corporation Principles*, CLIMATE CORP., https://www.climate.com/static/cms/principles/ [https://perma.cc/C9NR-J9HP] (last visited May 27, 2021); *see also* Lina Khan, *Monsanto's Scary New Schemes: Why Does It Really Want All This Data?*, SALON (Dec. 29, 2013, 7:00 PM), https://www.salon.com/2013/12/29/monsantos_scary_new_scheme_why_does_it_really_want_all_this_data/ [https://perma.cc/H22Y-SGSV] (noting that Monsanto did not take a position on whether farmers own their data when asked).

145. Davis & Marotta-Wurgler, *supra* note 33, at 664 (arguing that in such standard form contracts for data collection, consumers face information barriers that lead them to misperceive or not fully internalize the nature and consequences of transactions).

146. *See* Bronson & Knezevic, *supra* note 102 (discussing the accumulation of data by agribusinesses and the inequity that causes).

147. *See* Wiseman et al., *supra* note 131, at 8.

148. Peter Waldman & Lydia Mulvany, *Farmers Fight John Deere Over Who Gets to Fix an $800,000 Tractor*, BLOOMBERG BUSINESSWEEK (Mar. 5, 2020, 4:00 AM), https://www.bloomberg.com/news/features/2020-03-05/farmers-fight-john-deere-over-who-gets-to-fix-an-800-000-tractor [https://perma.cc/5HS8-SEGX].

149. Wiseman et al., *supra* note 131, at 9.

150. Joseph Russo, *Data Privacy, Ownership in Precision Agriculture*, PRECISIONAG (Sept. 3, 2013), https://www.precisionag.com/digital-farming/data-management/data-privacy-ownership-in-precision-agriculture/ [https://perma.cc/5DRN-K5TK].

little sense of the universe of third parties who are likely to also have access to the data.[151]

Even without the practical difficulties of privacy control and structural power imbalances, contract law may pose a challenge to data originators' control of data. Given that the contractual protections apply only to original transacting parties, the data originators' consent in collecting data is not dispositive of their ability to access and control data.[152] In this case, contractual rights and duties that typically only bind the contracting parties may be of limited value when data is transferred to other parties.[153] It is contended that "[i]t is possible to 'own' [agricultural] data [as a matter binding between two contracting parties] but have little control over who and how the data is used."[154] In a trend that scholars of critical data studies characterize as "data grab" and which political economy scholars frame as the new "extraction," contractual arrangements are increasingly used to "dispossess" farmers of their agricultural data and the value it may generate.[155] This is often referred to as the "digital data divide," a divide between those who contribute data to gain actionable information in a usable form and those who control, aggregate, and share that data.[156]

The challenges of ensuring access to and control over data through contractual arrangements that uniquely privilege those who collect, process, and utilize data necessitates legal intervention to mandatorily regulate the collection, use, and ownership of data on behalf of data originators, such as farmers. In the absence of such a regulatory regime in agriculture, a set of instruments that incorporate voluntary rules and principles regarding ownership and control of agricultural data have emerged in the European Union, the United States, Australia, and New Zealand.[157] In the United States and

---

151. *See* Joseph Turow, Jennifer King, Chris Jay Hoofnatle, Amy Bleakley & Michael Hennessey, *Americans Reject Tailored Advertising and Three Activities that Enable It* 4 (Univ. Penn. Annenberg Sch. for Commc'n, Departmental Paper No. 9, 2009).

152. Patricia Sanchez Abril, *Private Ordering: A Contractual Approach to Online Interpersonal Privacy*, 45 WAKE FOREST L. REV. 689, 715–16 (2010).

153. Davis & Marotta-Wurgler, *supra* note 33, at 664–65.

154. Wiseman et. al, *supra* note 131, at 8.

155. *See* Alistair Fraser, *Land Grab/Data Grab: Precision Agriculture and Its New Horizons*, 46 J. PEASANT STUD. 893, 895–96 (2019) (discussing the concept of "data grab"); *see also* J. Sadawoski, *The Internet of Landlords: Digital Platforms and New Mechanisms of Rentier Capitalism*, 52 ANTIPODE 562, 570–71 (2020) (discussing data "extraction"); JULIE COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 48–49 (2019) (discussing the legal framework enabling the collecting and processing of personal data).

156. Mark Andrejevic, *The Big Data Divide*, 8 INT'L J. COMMC'N 1673, 1674 (2014).

157. *See generally EU Code of Conduct*, *supra* note 64 (providing general principles for sharing agricultural data in the European Union); *Privacy and Security Principles for Farm Data Agreement*, FARM & DAIRY (Nov. 20, 2014), https://www.farmanddairy.com/news/privacy-security-

Canada, Ag Data Transparent (ADT) aims to incentivize ATPs to increase transparency in data contracts by assessing and certifying data contracts between ATPs and farmers, thereby reflecting a set of principles as ADT.[158] These voluntary initiatives, particularly the EU and US rules and principles, seek to emulate the EU General Data Protection Regulation (GDPR) by assigning primary data "ownership" rights to farmers.[159] However, these rules and principles accept the primacy of contracts over proposed rights for farmers and may not, in their legal design, respond to the challenges of ensuring access to and control over data in the relationship between farmers and ATPs, even if adopted as legally binding laws.[160]

Therefore, it is necessary to examine any protection that data originators might have regarding access to and control over their data under legal regimes that mandatorily bind contracting parties in these circumstances. Hence, the question remains of whether data originators can assert a level of access to and control over user data under the privacy regime.

B. User Data and Privacy Regimes

An area of law that could enable technology users to assert control over and access the data they originate is data privacy law. The Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), the California Consumer Privacy Act (CCPA), and Europe's GDPR are examples of privacy legislation to regulate the collection, aggregation, and sharing of "personal data" generated by data originators who qualify as "data subjects."[161]

---

principles-farm-data-agreement/226798.html [https://perma.cc/JDZ9-RSLF] (describing the data collection privacy and security agreement formed by agribusinesses and groups representing American farmers); *Australian Farm Data Code*, NAT'L FARMERS' FED'N, https://nff.org.au/programs/australian-farm-data [https://perma.cc/TZ4T-N8WW] (describing guidance for service providers who manage data on behalf of Australian farmers); N.Z. FARM DATA CODE OF PRAC., FARM DATA CODE OF PRACTICE (2021), http://www.farmdatacode.org.nz/wp-content/uploads/2016/03/Farm-Data-Code-of-Practice-Version-1.1_lowres_singles.pdf [https://perma.cc/8C23-AL8C] (providing general principles for owning, processing, securing, storing, and sharing farm data in New Zealand).

158. *See What Does It Mean to Be Ag Data Transparent*, AG DATA TRANSPARENT, https://www.agdatatransparent.com/about [https://perma.cc/3BXG-UY8N] (last visited May 25, 2021).

159. Atik & Martens, *supra* note 101, at 5.

160. *See id.*

161. PIPEDA, S.C. 2000, c 5 (Can.); California Consumer Privacy Act (CCPA), CAL. CIV. CODE §§ 1798.100–1798.199.95 (West 2018); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard

User data, constituting technical data, such as agronomic data, activity data like farm operation data, and machine and device-generated data, can have aspects that qualify as "personal data."[162] Therefore, it is necessary to consider the relationship between user data in general and personal data to determine the scope of coverage of user data under personal data protection regimes.

Data privacy regimes generally center definitions of personal data on information "about" or "relating to" an "identified/identifiable individual."[163] An important task in determining the scope of personal data is to establish the connection between the information in question and an individual. The term "relating to" or "about" might be fulfilled whenever the data reveal an identified or identifiable person. But questions arise over whether "personal data" may be narrowly applied to circumstances—such as when the information pertains directly to a particular person, or broadly, such as when the information concerns objects, processes, or events in the first place but inferences can be made that relate indirectly to individuals.[164]

Canada's Office of the Privacy Commissioner has adopted a contextual approach to the scope of "about," which considers the context of the information collection, use, and disclosure.[165] Thus, it has been decided that the sales records of independent real estate agents constitute commercial information connected with the business being conducted and personal information concerning the individual real estate agents.[166] Photographing tenants' apartments without consent is likewise considered a violation of privacy if details of the apartments in

---

to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O. J. (L 119) [hereinafter Processing Personal Data].

162. *See supra* Section 2.B.

163. PIPEDA, S.C. 2000, c 5, s 2 (Can.) ("personal information means information about an identifiable individual."); CIV. § 1798.140(o)(1); Processing Personal Data, *supra* note 162, at 33. *See also* Normann Witzleb & Julian Wagner, *When Is Personal Data "About" or "Relating to" an Individual? A Comparison of Australian, Canadian, and EU Data Protection and Privacy Laws*, 4 CANADIAN J. COMPAR. & CONTEMP. L. 293, 294–95 (2018) (comparing definitions of "personal data" across jurisdictions).

164. *See* Witzleb & Wagner, *supra* note 163, at 294–95.

165. *The Privacy Commissioner of Canada's Position at the Conclusion of the Hearings on the Statutory Review of PIPEDA*, OFF. PRIV. COMM'R CAN., https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2007/sub_070222_03/ [https://perma.cc/7MAL-75CB] (last modified Feb. 22, 2007).

166. *See Real Estate Broker Publishes Names of Top Five Sales Representatives in a City*, OFF. PRIV. COMM'R CAN., https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2005/pipeda-2005-303/ [https://perma.cc/3FH5-MCJD] (last modified June 8, 2005) [hereinafter *Real Estate Broker*].

the photographs reveal something of the individual's personal nature.[167]

Based on these accounts, user data such as agricultural data containing agronomic information (including the nutrient content of farmland), farm operation data that include the farmer's activities (such as how frequently spraying is performed), and machine data comprising information about the frequency of using an item of farm equipment may qualify as personal data when they are attributed to an identified or identifiable individual.[168] Agricultural data of this nature can reveal the types of soil fertilizer used by a farmer on his or her farm as well as the farmer's practices and preferences.[169]

In judicial interpretations of the scope of personal data under PIPEDA, the Canadian courts have adopted a two-tiered determination of personal information based on the cumulative requirement for the information to be "about" an "identifiable individual."[170] In *Canada (Information Commissioner)*, the Federal Court of Appeal distinguished between information "about" an individual and information "about" something else by deciding that information can only be "about" an individual where it involves subjects that "engage [an individual's] right to privacy."[171] This right is said to connote "concepts of intimacy, identity, dignity, and integrity of the individual."[172] Accordingly, air traffic control recordings relating to air accidents investigated by the Canadian Transportation Accident Investigation and Safety Board were determined to be information "about the status of the aircraft, weather conditions, matters associated with air traffic control and the utterances of the pilots and controllers."[173] However, these recordings and transcripts did not engage individuals' right to privacy since they consisted of "non-personal information transmitted by an individual in

167. *Cf. id.* (finding that the disclosure of real estate sales representatives' names and number of houses sold without the representatives' consent violated Canadian law protecting personal information).

168. *Cf. id.* (finding that the disclosure of real estate sales representatives' names and number of houses sold without the representatives' consent violated Canadian law protecting personal information).

169. *See* Nathan DeLay, Nathaneal Thompson & James Mintert, *Farm Data Usage in Commercial Agriculture*, PURDUE UNIV. CTR. FOR COM. AGRIC. (Jan. 23, 2020), https://ag.purdue.edu/commercialag/home/resource/2020/01/farm-data-usage-in-commercial-agriculture/ [https://perma.cc/9KLS-3ZLS].

170. *See* Info. Comm'r v. Transp. Accident Investigation & Safety Bd., [2007] 1 F.C.R. 203, 224–28 (Can.).

171. *Id.* at 230.

172. *Id.*

173. *Id.*

job-related circumstances."[174] Hence, they "[did] not match the concept of 'privacy' and the values that concept [was] meant to protect."[175] Similarly, user data such as agricultural data—forming an inherent part of farmers' economic livelihood – could be held to be job-related and not strictly fall under the traditional notion of privacy. Although some form of agricultural data could qualify as personal data, the link that must be made between the information and the individual farmer would likely be subject to a case-by-case evaluation on whether it falls under the scope of PIPEDA.[176]

In this respect, the EU data protection regime better elaborates the level of linkage necessary for information to be considered "relating to" an individual.[177] According to the EU's Article 29 Working Party (an advisory body providing the most authoritative guidance on data), in order for data to "relate" to an individual, at least one of the following three elements needs to be present: content, purpose, or results.[178] The "content" element can be established when the information concerns a particular person in the most literal understanding of "relating to."[179] Meanwhile, the "purpose" element exists when the information is used or is likely to be used to evaluate, treat, or influence the status or behavior of an individual, compared to other individuals.[180] Regarding the "result" element, data can be considered to "relate" to an individual because its use is likely to affect that person's rights and interests, considering the specific circumstances.[181] This element is fulfilled if, at the minimum, an individual could be treated differently from others because of the processing of such data.[182]

---

174. *Id.*

175. *Id.*

176. *See* PIPEDA, S.C. 2000, c 5, ss 2–4 (Can.).

177. *See* Processing Personal Data, *supra* note 161, at 33.

178. The Working Party on the Prot. of Individuals with Regard to the Processing of Pers. Data, *Opinion 4/2007 on the Concept of Personal Data*, at 10 (June 20, 2007), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf [https://perma.cc/4EMG-UR5J] [hereinafter *Opinion 4/2007*]. Although the question of whether "about an individual" required a more direct link between the data and the individual than the formulation "relating to an . . . individual" remains debatable, for the purpose of this Article, the analysis relies on the "relating to" formulation given the jurisprudence is well developed as to its meaning under the EU GDPR. *See, e.g.*, Mark Burdon & Alissa McKillop, *The Google Street View Wi-Fi Scandal and Its Repercussions for Privacy Regulation*, 39 MONASH U. L. REV. 702, 712 (2013).

179. *See Opinion 4/2007*, *supra* note 178.

180. *See id.*

181. *Id.* at 11.

182. *Id.*

For agricultural data to be protected under privacy regimes, it must also be closely associated with the data subject.[183] This data subject must be identified or identifiable.[184] While the primary means of identifying a data subject is their name, the subject may also be identified by other means that render them "identifiable," such as personal identifiers like Internet Protocol addresses, geolocation, biometric data, or browsing history.[185] The existence (or non-existence,) of this possibility for identification distinguishes user data, such as agricultural data, from personal data.[186] Since agronomic and farm operation data primarily deal with farm-related information, the extent to which these data categories can be used to identify particular farmers will render them either personal or nonpersonal.[187]

According to Recital 26 of the EU GDPR, in order to determine whether a person is identifiable, "account should be taken of all the means likely reasonably to be used, such as singling out, either by the controller or by any other person to identify the natural person directly or indirectly."[188] Factors such as the cost of conducting this identification, the intended purpose of the identification, the structure of the processing, and interests at stake for the individuals concerned are taken into account when determining whether the subject is identifiable.[189] Where identification is not "reasonably likely," the information will be considered anonymized and fall outside the regime of protection.[190]

However, it is often difficult to determine the level of anonymization that information must be subject to before it is considered satisfactory. Canada's Privacy Commissioner has historically advanced the position that personal data falls within the scope of the privacy regime if "there is a serious possibility that someone

183. *See* Info. Comm'r v. Transp. Accident Investigation & Safety Bd., [2007] 1 F.C.R. 203, 230 (Can.); Witzleb & Wagner, *supra* note 163, at 294.

184. *See* Witzleb & Wagner, *supra* note 163, at 294.

185. *See* Müge Fazlioglu, *Beyond the "Nature" of Data: Obstacles to Protecting Sensitive Information in the European Union and the United States*, 46 FORDHAM URB. L.J. 271, 292–93 (2019).

186. *See id.* at 273; *Info. Comm'r*, [2007] 1 F.C.R. at 230 (Can.).

187. *See Info. Comm'r*, [2007] 1 F.C.R. at 230 (Can.); *Real Estate Broker*, *supra* note 166.

188. Processing Personal Data, *supra* note 161, at 5.

189. *Opinion 4/2007*, *supra* note 178, at 15.

190. *Id.* at 21; *see* IRISH DATA AUTH., GUIDANCE NOTE: GUIDANCE ON ANONYMISATION AND PSEUDONYMISATION 7 (2019), https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf [https://perma.cc/F54Y-56LK].

could identify the available information."[191] Nevertheless, courts have adopted a more practical "reasonable expectations" test, in which information is still considered to be about an "identifiable" individual "if it is reasonable to expect that an individual can be identified from the information in the issue, including when combined with information from sources otherwise available."[192] However, even though a vast amount of agricultural data can be "about" or "relating to" a technology user, such as a farmer, it likely cannot be protected as "personal data" under privacy regimes.[193] There are two reasons for this. First, data collectors often adopt a highly restrictive view of what constitutes personal data because of the cumulative requirements that data be "about … identified or identifiable" individuals.[194] Second, a vast amount of user data that can be considered "about" or "relating to" data originators, such as farmers, may easily be "de-identified" or "anonymized" at the moment of collection.[195]

Given the unreliability of anonymization techniques to bring about irreversible anonymization,[196] emerging data privacy regimes regulate "de-identified" data through the prohibition of re-identification, and set the standard for de-identification.[197] The CCPA defines the term "de-identified" as meaning "information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer. . . ."[198] In addition to the general prohibition against re-

191. *See Psychologist's Anonymized Peer Review Notes are the Personal Information of the Patient*, OFF OF THE PRIV. COMM'R OF CAN., https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-018/ [https://perma.cc/ZX2E-Z2QY] (June 18, 2010).

192. *See Info. Comm'r*, [2007] 1 F.C.R. at 227 (Can.).

193. *See Privacy Statement*, CLIMATE FIELDVIEW (Oct. 15, 2021), https://www.climatefieldview.ca/legal/privacy-statement/#2 [https://perma.cc/53MW-LZ4U]; *Anonymisation and Data Protection*, LONDON SCH. OF ECON. & POL. SCI., https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/guiAnoDatPro.pdf?from_serp=1 (last visited Feb. 17, 2022) [https://perma.cc/USV3-QQB9].

194. *See Privacy Statement*, *supra* note 193. For example, the FieldView farmer interface, produced by the Climate Corporation, restricts the definition of personal data to name, address, and other personal details of the farmer. *See id.*

195. *See Anonymisation and Data Protection*, *supra* note 193. Despite slight distinctions in terminology, the terms "de-identification" and "anonymization" can be used interchangeably, as both point towards the same goals. *See* Gilad Rosner, *De-Identification as Public Policy*, 3 J. DATA PROT. & PRIV. 1, 3 (2020).

196. Nadezhda Purtova, *The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law*, 10 L. INNOVATION & TECH. 40, 41 (2018); Robert Gellman, *The Deidentification Dilemma: A Legislative and Contractual Proposal*, 21 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 33, 39 (2010).

197. Gellman, *supra* note 196, at 35.

198. CAL. CIV. CODE § 1798.140(h) (West 2018).

identification—which is subject to certain exceptions—this definition makes it a requirement that de-identified data be protected against re-identification through technical safeguards and business processes, with no attempt to re-identify.[199] Once personal data has been de-identified, businesses have an unrestricted right to "[c]ollect, use, retain, sell, or disclose consumer information that is de-identified or in the aggregate consumer information."[200] Besides the restricted scope of what amounts to personal data from among the different categories of user data, the possibility of de-identifying data enables TPs, data intermediaries, and data platforms to render and use personal data outside the scope of privacy law.

The newly proposed Canadian Consumer Privacy Protection Act (CPPA), aimed at amending PIPEDA, also includes a definition of "de-identify" that is similar to that of CCPA.[201] In addition, it contains a general prohibition against re-identification, subject to certain exceptions, and requires that technical and administrative measures be implemented to ensure de-identification.[202] Unlike the CCPA, however, de-identified data appears to fall within the scope of the CPPA.[203] Hence, it could be subject to privacy principles as personal data.[204] Although it is unclear how much privacy-preserving control can be enjoyed in the case of user data that is "de-identified" under the CPPA, it would appear that data originators can enjoy privacy protection that is at least similar to that of "pseudonymized" data under the EU GDPR.[205]

To conclude, there are vast circumstances in which user data may fall outside the privacy law's remit. Technology users' data can be considered "nonpersonal data" if the data cannot be deemed to relate to an individual, or the individual cannot be identified or is

---

199. *Id.* § 1798.148(a).

200. *Id.* § 1798.145(a)(5).

201. *See* Bill C-11, *An Act to Enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to Make Consequential and Related Amendments to Other Acts*, 2d Sess, 43d Parl, 2020, cl. 2 (Can.).

202. *Id.* at cl. 75–74.

203. CAL. CIV. CODE § 1798.145(a)(5) (West 2022).

204. This can be deduced from the fact that, unlike the CCPA, there is no provision expressly excluding de-identified data from the scope of CPPA. *See id.*; Bill C-11 (Can.). In addition, the drafting of the CPPA suggests that de-identified data is within the scope of the law. Bill C-11, cl. 21, 22(1), 39(1) (Can.). For example, clauses 21, 22(1) and 39(1) contain new exceptions for research and development, prospective business transactions, and socially beneficial purposes. *Id.* These exceptions would not have been necessary if de-identified information were not subject to the CCPA.

205. MIKE HINTZE & KHALED EL EMAM, COMPARING THE BENEFITS OF PSEUDONYMIZATION AND ANONYMIZATION UNDER THE GDPR 4 (2017), https://iapp.org/media/pdf/resource_center/PA_WP2-Anonymous-pseudonymous-comparison.pdf [https://perma.cc/SDS5-UQYB].

unidentifiable.[206] In addition, user data in its various categories frequently cannot qualify as personal data, even though it may relate to individuals such as farmers as a manifestation of their farming activities. Such data is often held in aggregated datasets as de-identified data, with no possibility of identification at the time of initial processing.[207] TPs, data intermediaries, and data-platform operators assert control over data of this nature, collected from technology users, under proprietary forms of control.[208]

Data collectors, processors, and aggregators exercise access to and control over user data within an ownership framework in the form of copyrights, including "para copyright," rights through technological protection measures.[209] These are often justified on the basis of protecting investment in collecting, interpreting, processing, and, sometimes, the creation or generation of data.[210] In such circumstances where TPs, data intermediaries, and data platforms exercise access and control over data, the question addressed in this Article can be reformulated as: What recourse do technology users have to ensure access and control over user data that relates to them but is often under the ownership control of others through copyright? In this sense, the originators' claims for access to and control over user data fill a lacuna in the intersection of copyright and data privacy law. Such data does not fall under the existing privacy regime because it often does not qualify as "personal data."[211] Users cannot be considered to have property-like rights over technical data, despite developments regarding the tort of misappropriation in the United States.[212] Although technology users may have copyrights in some aspects of activity data,

206. *Id.* at 3.

207. *Id.*

208. *See, e.g.*, Kate Kay, *What Data Privacy Could Look Like in the Metaverse*, PROTOCOL (Feb. 16, 2022), https://www.protocol.com/enterprise/data-privacy-intermediaries-metaverse-web3 [https://perma.cc/9B92-9MAT].

209. *See* discussion of ownership of data *infra* Section 5.B. *See also* Dan L. Burk, *Anti-circumvention Misuse*, 50 UCLA L. REV. 1095, 1109 (2003) (characterizing technology protection measures as system of rights that extend far beyond copyright law).

210. TERESA SCASSA, DATA OWNERSHIP 5–15 (2018), https://www.cigionline.org/sites/default/files/documents/Paper%20no.187_2.pdf [https://perma.cc/N2BK-KVQU].

211. CAL. CIV. CODE § 1798.140 (West 2022).

212. In the era of big data, the closest property protection afforded to factual data relates to what is provided for "hot data" under the tort of misappropriation in the United States. *See* Victoria Smith Ekstrand & Christopher Roush, *From Hot News to Hot Data: The Rise of Fintech, the Ownership of Big Data, and the Future of the Hot News Doctrine*, 35 CARDOZO ARTS & ENT. L.J. 303, 305 (2017). This state law claim protects the ownership of discrete facts for a short period after publication. *See* Int'l News Serv. v. Associated Press, 248 U.S. 215, 257 (1918); Chi. Bd. Options Exch., Inc. v. Int'l Sec. Exch., LLC, 677 F.3d 1361, 1369 (Fed. Cir. 2012).

such as farm operation data,[213] it is not easy to assert these rights once the data is aggregated with other datasets. Machine, device, and technical data do not attract copyright in themselves either, given that they often purely represent factual reality.[214]

This Article advances the argument that in situations where data collectors, processors, and aggregators claim control over access to user data as "authors" of that data, there is a basis in copyright law jurisprudence to recognize technology users, such as farmers, as originators of the data that may "relate to" them but is covered under ownership claim in copyright.[215] Two reasons necessitate such a proposition. First, even though agricultural data does not qualify as personal data, if it does not identify an individual farmer,[216] it falls within the broader realm of farmers' privacy interests as individuals or group members. Inferences may be made of an individual farmer's activities based on group or subgroup data. However, current data protection frameworks do not recognize a group or collective rights.[217]

Second, the disclosure of agricultural data to third parties without the consent of data originators, such as farmers, brings economic concerns that are not covered under typical harms that privacy law is designed to protect.[218] These concerns could take either the form of unjust enrichment by data collectors and processors who control and exploit agricultural data through the exercise of copyright, or that of exploitation by actors in the agricultural value chain who position themselves in a better market position than farmers through the use of the farmers' data. Therefore, could copyright provide a basis for user groups, such as farmers, to access and control data?

The remainder of this Article will attempt to offer a basis for designing a *sui generis* legislation for recognizing the contribution of technology users as data originators. Data originators' entitlement to user data in such a framework has a normative basis in recognition of the contribution of putative authors to a collaborative work that is private in nature. It is later argued that copyright notions of the "joint

213. ZIWEN YU, ALBERT DE VRIES, YIANNIS AMPATZIDIS, & D. DANIEL SOKOL, WHO OWNS AND CONTROLS FARMING DATA? (2021), https://edis.ifas.ufl.edu/pdf/AE/AE564/AE564-Db30mdqk94.pdf [https://perma.cc/AVM4-KE62].

214. *See* discussion *infra* Section VI.B.i.

215. *See* discussion *infra* Section VI.B.i.

216. *See* HINTZE & EL EMAM, *supra* note 205.

217. *See* Alessandro Mantelero, P*ersonal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection*, 32 COMPUT. L. & SEC. REV. 238, 243 (2016).

218. In traditional privacy tort, disclosure of data is objected to because of the emotional harm it inflicts on the data subject. *See* Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1146 (2011).

authorship" of "unpublished works" provide such a normative basis for legal intervention.[219]

VI. WHERE COPYRIGHT MEETS PRIVACY: MODELING COPYRIGHT TO RECOGNIZE DATA ORIGINATORS' CLAIMS TO DATA

The relationship between copyright law and privacy law is generally held to be disparate.[220] But there are at least four circumstances in which copyright law intersects with privacy law. First, the enforcement of copyrights intersects with privacy interests associated with the Internet Protocol addresses of those suspected of copyright infringement.[221] Second, the privacy interest of an anonymous or pseudonymous author becomes an issue when he or she decides to exercise rights in copyright, such as lodging a claim, protecting a claim, or transferring the title of their work, particularly in the United States—where, for an author to file an infringement claim, their work must be registered with the Copyright Office.[222] These authors sacrifice their privacy if they decide to enforce their copyright.[223] Third, copyright law meets the privacy requirements with respect to the interests of individuals who are depicted in copyrighted works.[224] This scenario arises in situations where the individuals captured in a self-taken photograph (e.g., a "selfie"), or a photograph taken by someone else, find themselves publicly depicted in an unfavorable manner, whereupon they seek to remove their involvement.[225] Fourth, copyright goes in tandem with privacy

219. *See* discussion *infra* Section VI.C.ii.

220. *See* Pamela Samuelson, *Privacy as Intellectual Property?* 52 STAN. L. REV. 1125, 1146 (1999); FEDERICA GIOVANELLA, COPYRIGHT AND INFORMATION PRIVACY: CONFLICTING RIGHTS IN BALANCE 249 (2017); Margaret Ann Wilkinson, *The Copyright Regime and Data Protection Legislation*, *in* COPYRIGHT ADMINISTRATIVE INSTITUTIONS: CONFERENCE ORGANISED BY THE CENTRE DE RECHERCHE EN DROIT PUBLIC (CRDP) OF THE FACULTY OF LAW OF THE UNIVERSITE DE MONTREAL 77, 88 (Ysolde Gendreau ed., 2001).

221. See GIOVANELLA, *supra* note 220, at 136–37.

222. 17 U.S.C. § 411(a); Matthew J. Astle, *Help! I've Been Infringed and I Can't Sue!: New Approaches to Copyright Registration*, 41 U. MEM. L. REV. 449, 450 (2011). In Canada, registration of copyright is not required to bring suit; registration only serves to deny the defendant the defense of "innocent infringer" which is weighed in the assessment of damages. *See* Copyright Act, R.S.C. 1985, c C-42, ss 34, 39 (Can.); Milliken & Co. v. Interface Flooring Sys., Inc. (2000), 251 N.R. 358, para. 27 (noting that "[k]knowledge [of copyright] is to be inferred from the facts of the case and the burden of proving it rests upon the plaintiffs, unless the copyright in the work was duly registered under the Act").

223. Tom W. Bell, *Copyrights, Privacy, and the Blockchain*, 42 OHIO N.U.L. Rev. 439, 453 (2016).

224. Aislinn O'Connell, *Image Rights and Image Wrongs: Image-Based Sexual Abuse and Online Takedown*, 15 J. INTELL. PROP. L. & PRAC. 55, 58 (2020).

225. *See, e.g.*, *id.* at 58–59.

regarding the private nature of both unpublished works and works intended for specific demographics: the author either does not authorize publication at all, or authorizes a strictly limited publication of the work, respectively.[226]

In the first two circumstances, copyright and privacy conflict with each other.[227] In other words, copyright enforcement in such cases may result in the infringement of privacy rights.[228] However, in the latter two scenarios, copyright and privacy rights complement one another.[229] In other words, privacy interests are claimed as an infringement of copyright.[230] Such trends have received extensive skepticism due to the apparent incompatibility of the purposes and normative unfitness of the two categories of law.[231] Nevertheless, many scholars argue that using copyright for privacy purposes does not constitute a misuse of copyright but is a testimony to problematic gaps in privacy law.[232]

---

226. *See* Shyamkrishna Balganesh, *Privative Copyright*, 73 VAND. L. REV. 1, 44 (2020); Nita A. Farahany, *Searching Secrets*, 160 U. PA. L. REV. 1239, 1266 (2012).

227. *See* GIOVANELLA, *supra* note 220, at 136–37; Copyright Act, R.S.C. 1985, C-42, ss 34, 39 (Can.); Bell, *supra* note 224, at 453.

228. *See* GIOVANELLA, *supra* note 220, at 136–37; Bell, *supra* note 224, at 453.

229. *See* O'Connell, *supra* note 224, at 58; Balganesh, *supra* note 227, at 44.

230. *See* O'Connell, *supra* note 224, at 58; Balganesh, *supra* note 227, at 44.

231. *See* Eric Goldman & Jessica Silbey, *Copyright's Memory Hole*, 4 BYU L. REV. 929, 935 (2019) (arguing that copyright law should consider only economic concerns and free speech concerns given the basic perception that tort law is best suited for addressing privacy concerns, but recognizing the existence of domains where the use of copyright for general privacy purposes might be legitimate); Alfred Yen, *The Challenge of Following Good Advice About Copyright and the First Amendment*, 15 CHI.-KENT J. INTELL. PROP. 412, 413 (2016) (explaining that allowing a plaintiff to succeed on a copyright claim brought in the interest of personal privacy does not do much to protect the plaintiff's incentive to create); Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 220, 222 (2018) ("[T]hese enormous data sets have nothing to do with the creative artistic assets that copyright law serves to protect."); *see also* Jeanne C. Fromer, *Should the Law Care Why Intellectual Property Rights Have Been Asserted?*, 53 HOUS. L. REV. 549, 587 (2015) ("[A]ssertions of protection for markets beyond the protected market—be they in relation to privacy and reputational interests or more generally—raise the specter of great cost to society."); Pierre N. Leval, *Toward a Fair Use Standard*, 103 HARV. L. REV. 1105, 1130 (1990) ("[C]opyright law is grotesquely inappropriate to protect privacy and obviously was not fashioned to do so.").

232. *See* Balganesh, *supra* note 227 (arguing that the use of copyright law to protect the dignitary interest and harms of authors which privacy torts are unconcerned with, and thus, form a legitimate part of the copyright landscape); *see also* Margaret Chon, *Copyright's Other Functions*, 15 CHI.-KENT J. INTELL. PROP. 101, 103 (2016) (arguing that using copyright to protect certain privacy and other personal interests "should not be categorically excluded as beyond the legitimate purview of copyright's concerns"); Amanda Levendowski, *Using Copyright to Combat Revenge Porn*, 3 N.Y.U. J. INTELL. PROP. & ENT. L. 422, 441, 443 (2014) (justifying the use of copyright to fight nonconsensual pornography based upon the gaps in legal solutions available to victims); Andrew Gilden, *Copyright's Market Gibberish*, 94 WASH. U.L. REV. 1020, 1022 (2019) (arguing that copyright routinely protects noneconomic interests, including dignitary

In proposing a *sui generis* regime for data users modeled on copyright, the interest under consideration can be seen as "non-economic," given the narrow definition of the "economic interests" with which copyright concerns itself.[233] However, loss of privacy of user data "relating to," for example, farmers could eventually lead to actual economic harm that is not specific to the agricultural data itself as a work.[234] Given that user data falls outside privacy regimes in many circumstances, technology users' claims for access to and control over aggregated user data rely on the economic loss associated with the data —instead of privacy values in the data—in the tort context.[235] As such, the claim for access to and control over user data may be doctrinally consistent with copyright in the broad framework of economic harm, but as the following discussion shows, the claim arises from dignitary interest and autonomy considerations that copyright is designed to protect.[236]

Consequently, the next question is: What basis is there in jurisprudence to support the use of copyright for privacy in modeling copyright for *sui generis* law? This inquiry requires a brief examination of the circumstances in which privacy is protected through copyright. Given that privacy interests in copyright arise from an inherently authorial claim,[237] the following Section will examine developments in the doctrine of joint authorship as a basis for data governance among copyright holders regarding aggregated agricultural data and farmers. There subsequently follows a discussion of rights derived from copyright law, which a legal intervention should incorporate in supporting technology users' claims for access to and control over data.

---

harms, but masks this protection in the language of the market); Deirdre Keller, *Copyright to the Rescue: Should Copyright Protect Privacy?*, 20 UCLA J.L. & TECH 1, 36–37 (2016) (finding protection of privacy through copyright legitimate but suggesting that U.S. law recognize a moral right of disclosure).

233. Copyright protects copyright owners from economic harm from market substitution. *See* Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 590 (1994).

234. *See supra* Section 5.B.

235. Privacy in tort context refers to "privacy" in its "traditional" sense of "an imagined sphere 'of seclusion and protection from others (the public).'" MEGAN RICHARDSON, ADVANCED INTRODUCTION TO PRIVACY LAW 11 (2020). Such use of privacy contrasts with the way "privacy" is "quite often used (especially in the United States) to denote control over personal information more broadly" (the parallel language of the later context of privacy in Europe and Canada is "data protection"). *See id.*

236. See *supra* discussion accompanying note 212.

237. 17 U.S.C. §102.

A. Use of Copyright for Privacy

There are two sets of individuals whose privacy interests are already enforced under copyright law: authors of unpublished works and individuals depicted in copyrighted works.[238] The jurisprudential roots underlying these privacy protections come from the UK Chancery Court's landmark 1818 opinion in *Gee v. Pritchard*.[239] This case concerned the privacy of private letters sent between family members.[240] Plaintiff sought an injunction against the Defendant who intended to publish a letter Plaintiff had written him.[241] Lord Eldon concluded that adequate protection against the Defendant's intended publication could be found in the common law property right in unpublished works, repudiating an argument that the publication would be restrained because "that the publication of the letters by Defendant, was a breach of private confidence, or violation of the right and interest of the Plaintiff therein, and was intended to wound her feelings, and could have no other effect."[242] Quoting Lord Chancellor Hardwicke from the earlier case *Pope v. Curl*, he proceeded: "The receiver of a letter has, at most, a joint property with the writer, and the possession does not give him a license to publish."[243]

These early English precedents and principles have been cited with approval and relied upon in US cases.[244] In the late nineteenth century, Justices Warren and Brandeis argued, in their seminal article, that common law copyright provided individuals with an absolute right to prevent the unauthorized publication of their unpublished works.[245] Thus, common law copyright provided the author of an unpublished work with exclusive control over the work's publication, enabling individuals to enjoin the publication of letters, diaries, property lists, etc.[246] The common law protection of unpublished works was subsequently subsumed under copyright, notably in the United States,

---

238. See O'Connell, *supra* note 224; Balganesh, *supra* note 226.

239. *Gee v. Pritchard* [1818] 36 Eng. Rep. 670, 674–75.

240. *Id.* at 670.

241. *Id.*

242. *Id.* at 671.

243. Pope v. Curl [1741] 26 Eng. Rep. 608, 608 (emphasis added).

244. *See, e.g.*, Denis v. LeClerc, 1 Mart. (o.s.) 297, 301 (Orleans 1811); Woolsey v. Judd, 11 How. Pr. 49, 58 (N.Y. Sup. Ct. 1855).

245. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

246. *See* Stephen B. Thau, *Copyright, Privacy, and Fair Use*, 24 HOFSTRA L. REV. 1, 25 (1995).

with the passing of the Copyright Act of 1976 as an exclusive right of public "distribut[ion]."[247]

Some essential features of the doctrinal roots of the statutory right of public distribution (referred to as publication right in Canada) have relevance for modeling copyright for data governance, as proposed in this Article. [248] Significantly, the rationale for protection deviates from copyright law's traditional principles and assumptions about the "creative incentive" and is, instead, based on non-economic considerations that Balganesh describes as "'privative' claims."[249] The protection is "driven by the desire to prevent *any* distribution of the work because of the noneconomic harm [under copyright law] that such dissemination is likely to cause them."[250] In this sense, the law protects against any harm arising from the "mere dissemination or use of the protected work without the creator's authorization," rather than any harm from acts of expression of an appropriative nature, such as unauthorized copying.[251] The harm against which the author is protected in such "privative claims" is distinguished from the protection currently provided by moral rights because "the interference with the author's autonomy occurs not through any harm *to* the work [which is the case in moral rights], but quite distinctively instead *through* the work."[252] Thus, "privative claims," which are currently recognized primarily under copyright's distribution rights, constitute self-standing redresses to a "disseminative harm" that is often wrongfully seen as parasitic on the "appropriative harm," which has copyright's economic basis as its rationale.[253]

The implication of recognizing the self-standing nature of redress against dissemination in copyright's exclusive right to public

---

247. 17 U.S.C. § 106(3); *see also* SUBCOMM. ON PATS., TRADEMARKS, & COPYRIGHTS OF S. COMM. ON THE JUDICIARY, 86TH CONG., COPYRIGHT LAW REVISION: PROTECTION OF UNPUBLISHED WORKS 8 (Comm. Print 1961) (written by William S. Strauss) (discussing the significance of publication in delineating statutory and common law copyright protection).

248. In Canada, the equivalent right with respect to unpublished works is referred to as "the right to publish." *See* Copyright Act, R.S.C. 1985, c C-42, s 2.2(1) (Can.). There seems to be slight differences between the two rights, as in the US publication occurs only when the possession of works is transferred to the public whereas in Canada, making copies available to the public is sufficient. *Compare* 17 U.S.C. § 101 ("'Publication' is the distribution of copies or phonorecords of a work to the public by sale or other transfer of ownership, or by rental, lease, or lending."), *with* Copyright Act, R.S.C. 1985, c C-42, s 2.2(1) (Can.) ("For the purposes of this Act, *publication* means . . . making copies of a work available to the public . . . .").

249. Balganesh, *supra* note 226.

250. *Id.* at 3.

251. *Id.* at 7.

252. *Id.* at 6. (noting that "the reputational harm [that moral rights protect] is fairly unique in that it is limited to the author's reputation *as manifested in the work*").

253. *Id.* at 11.

distribution is that, normatively, the privacy interests to be protected fall within the panoply of legitimate copyright harms.[254] These privacy interests emanate from the very act of authorship, rather than under the tort of privacy.[255] The nature of the interests involved in common law copyright, now incorporated under the public distribution right, cannot be covered by privacy torts, given situations "where the subject exercises a critical role in the production of the content that is made public and then chooses to control whether and when to disseminate it."[256] Balganesh clarifies this point, noting "the subject's autonomy is not just about self-representation to the public but instead about self-representation to the public as *author*" and as such, questions arising over the appropriate scope of authorship are not the concern of privacy torts.[257] Balganesh argues that privative claims may be understood as simulating the working of a lesser-known moral right: the right of disclosure, which is recognized and protected in civil law jurisdictions.[258] Currently, the law in the United States and Canada recognizes the moral rights of attribution and integrity; these two rights are recognized in the Berne Convention.[259] US Congress was initially aware of the disclosure right and made a conscious decision to avoid recognizing it; the situation could be different in Canada, though, given the roots of the Copyright Act as derived from common law tradition and Continental civil law.[260]

Thus, the right of disclosure could be recognized and protected as an aspect of the public-distribution right for works excluded from copyright post-1976 because of the copyrightability criteria adopted at the time. In this respect, it is essential to note that early uses of copyright to protect privacy arose from "the private nature of the

254. *Id.* at 11–12.

255. *Id.* at 33.

256. *Id.* at 27.

257. *Id.*

258. *Id.* at 34.

259. *See* Berne Convention for the Protection of Literary and Artistic Works, art. 6bis, Sept. 9, 1886, 25 U.S.T. 1241; 1161 U.N.T.S. 3 (amended Sept. 28, 1979) ("Independently of the author's economic rights, and even after the transfer of the said rights, the author shall have the right to claim authorship of the work and to object to any distortion, mutilation, or other modification of, or other derogatory action in relation to, the said work, which would be prejudicial to his honor or reputation."). The United States ratified the Berne Convention in 1988. Berne Convention Implementation Act of 1988, Pub. L. No. 100-568, 102 Stat. 2853 (codified in scattered sections of 17 U.S.C.).

260. SUBCOMM. ON PATS., TRADEMARKS, & COPYRIGHTS OF S. COMM. ON THE JUDICIARY, 86TH CONG., COPYRIGHT LAW REVISION: THE MORAL RIGHTS OF THE AUTHOR 115 (Comm. Print 1960) (written by William S. Strauss); Théberge v Galerie d'Art du Petit Champlain Inc., [2002] 2 S.C.R. 336, para. 116 (Can.) ("[I]t is important to recall that Canadian copyright law derives from multiple sources and draws on both common law tradition and continental civil law concepts.").

expression that induces its personality-infused content. . . in the nature of private communications," and not necessarily from the statutory requirement that the expressions be "*original* works of authorship."[261] There were trends in which US courts focused "on the process of authorship without having to examine or assess the product of that process—that is, the content of the work."[262] As such, common law copyright could protect privacy interests in raw data, even if the data do not meet the tests of "originality".[263]

A hurdle to modeling a *sui generis* user data governance regime based on privative copyright claims arises from such claims relying exclusively on authorship.[264] In privative claims, "the work is. . . quite genuinely a work of authorship in that there is a salient causal connection between the creator and the expression at issue, but the particular content imbues that authorship with a subjectively personal dimension."[265] In recent jurisprudence involving the use of copyright to prevent unfavorable depictions, for example, the copyright remedy only applies to situations where the person depicted is the copyright holder—either the subject of the image is the photographer (as in a selfie), or the copyright has been transferred to the subject.[266]

In the modeling of copyright as an instrument of user-data governance that recognizes the rights of data originators based on privative copyright, how can technology users assume an "authorial" claim over user data, especially aggregated data that falls outside of data protection law? In a privative copyright framework, this Article argues that the relationship between parties who exercise ownership rights over data under copyright law and data originators who seek access to and control over such data should rely on recognizing technology users as authors of such data. This proposition requires a determination of the following two questions: (1) When does data qualify for copyright protection and thereby become a subject of

---

261. *See* 17 U.S.C. § 102(a). Canada's Copyright Act has a similar requirement and states that copyright subsists "in every original literary, dramatic, musical and artistic work." *See* Copyright Act R.S.C. 1985, c C-42, s 5 (Can.).

262. Balganesh, *supra* note 226, at 37.

263. *See* Thau, *supra* note 246, at 1 (noting that common law copyright could allow "one who had a catalog of private possessions to prevent the catalog itself from being distributed, notwithstanding the fact that the catalog had little or no intellectual substance").

264. Balganesh, *supra* note 226, at 12.

265. Balganesh, *supra* note 226, at 12.

266. *See* Default Judgment, Doe v. Elam, No. 2:14-cv-09788-PSG-SS (C.D. Cal., Apr. 4, 2018) (finding that the plaintiff registered copyright over her intimate selfie pictures such that her copyright infringement action was successful); Balsey v. LFP, Inc., 691 F.3d 747, 756 (6th Cir. 2012) (finding copyright infringement by a magazine that published photos of plaintiff in a wet t-shirt contest).

ownership? (2) If user data does not qualify for copyright, how do data originators assume authorship status? After analyzing the question of when data qualifies for copyright protection, first in the context of user data that directly originates from technology users, and then in the context of aggregated user data, the discussion that follows addresses the question of when data originators might assume "authorial" status.

B. Copyright and Ownership of Big Data

Copyright is the preeminent regime for the ownership of ideas expressed in a fixed medium.[267] As such, it becomes a prime candidate for the ownership of data expressed either by keystroke such as in the context of activity data or by a machine that incorporates sensors. Could data originators exercise a level of control over user data as authors of copyrightable work as an aspect of privative copyright?

This Section first addresses whether copyright exists over data, based on the distinction made by the law between facts and data, and ideas and expressions, in addition to the requirement of human authorship. In so doing, a gap is demonstrated in recognizing the contribution of data originators to data that sometimes becomes the subject of copyright, either as a compilation or as a work in the form of processed data.

i. Copyrightability of User Data

In both Canada and the United States, case law has established that copyright protection only extends to the expression of ideas rather than the underlying ideas or facts.[268] To the extent that data equates with facts, as Justice Brandeis famously stated in his dissent in *International News Service,* "[t]he general rule of law is, that the noblest of human productions—knowledge, truths ascertained, conceptions and ideas—after voluntary communication to others, are free as the air to common use."[269] The US Supreme Court in *Feist Publications v. Rural Telephone Service* ("*Feist*") further elaborates the nature of facts based on the idea- and fact-expression dichotomy stating, "the fact/expression dichotomy limits severely the scope of protection in fact-based works

267. *See generally* MARSHALL LEAFFER, UNDERSTANDING COPYRIGHT LAW (Carolina Acad. Press, 7th ed. 2019) (providing an overview of copyright case law and legislative developments).

268. *See* CCH Canadian Ltd. v. L. Soc'y Upper Can., [2004] 1 S.C.R. 339, para. 25 (Can.) (noting that facts are in the public domain as "trite law"); Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 348 (1991) (noting that "[a]ll facts—scientific, historical, biographical, and news of the day" may not be copyrighted and are part of the public domain available to every person).

269. Int'l News Serv. v. Associated Press, 248 U.S. 215, 250 (1918) (Brandeis, J., dissenting).

[. . .] copyright is limited to those aspects of the work—termed 'expression'—that display the stamp of the author's originality." [270]
User data, such as technical data in the form of agronomic data, often is composed of data concerning conditions of farmland and collected using various precision farming technologies and state-of-the-art sensors.[271] Farm machinery generates large volumes of objective data in order to generate more personalized or spatially precise information for decision-making on a farm.[272] Data such as soil analysis results, nutrient information, plant populations, and animal monitoring consist of an objective representation of facts about the relevant individuals, soil, plants, or animals.[273] Copyright does not protect such data sets because they fall in the realm of facts.[274]

However, it is less clear whether data is always indistinguishable from facts, and whether copyright protection extends to data.[275] In *New York Mercantile Exchange, Inc. (NYMEX) v. Intercontinental Exchange, Inc.* ("*Intercontinental Exchange*"), the US Court of Appeals for the Second Circuit considered whether copyright protection exists in the individual price values that NYMEX sets as settlement prices for its own futures contracts and hybrid commodity instruments.[276] The court considered the question of whether NYMEX could receive copyright protection in its settlement prices, relying on the issue of whether settlement prices were figures that merely existed within the marketplace and subsequently discovered by NYMEX, or whether NYMEX created its settlement prices.[277] The court ultimately determined not to provide copyright protection, arguing that the merger doctrine must apply.[278] The merger doctrine, broadly recognized in the United States and Canada, upholds that when a work of authorship is incapable of being expressed as a practical matter in more than one or

---

270. *Feist*, 499 U.S. at 349.

271. Sjaak Wolfert, Lan Ge, Cor Verdouw & Marc-Jean Bogarrdt, *Big Data in Smart Farming – A Review*, 153 AGRIC. SYS. 69, 70 (2017).

272. *See id.* at 72.

273. *See id.*

274. *See* 17 U.S.C. § 102(a).

275. For conceptual distinction between facts and data, see SCASSA, *supra* note 210 at 3–4 (noting the distinction between representative data from implied and derived data and observing that implied and derived data may be treated differently in both Canada and the United States). *See also* Justin Hughes, *Created Facts and the Flawed Ontology of Copyright Law*, 83 NOTRE DAME L. REV. 43 (2007) (arguing that original expressions that generate facts once adopted by social convention should be protected to incentivize the creation of the expression and the generated facts).

276. N.Y. Mercantile Exch., Inc v. Intercont'l, Inc., 497 F.3d 109, 110 (2d Cir. 2007).

277. *Id.* at 114.

278. *Id.* at 118.

a small number of ways, such work is "merged" with the idea that is expressed.[279] However, it noted that the matter of whether settlement prices are "discovered" or "created" was a "close question;" it would not "decide whether settlement prices are unoriginal" and was "particularly reluctant to hold, as a matter of law, that [NYMEX]… discover[ed] the settlement prices."[280]

Similarly, the court in *BanxCorp v. Costco Wholesale Corp.* seemed open to the possibility that copyright could extend to "raw data that have been converted into a final value through the use of an original formula," depending on the "degree of consensus and objectivity that attaches to the formula."[281] In considering the originality of—and thus the possibility of extending copyright protection to—calculated percentages, the court explained that "the more acceptance a financial measure obtains (i.e., the more successful it is), the more 'fact-like' it becomes."[282]

In both *BanxCorp* and *Intercontinental Exchange*, the ultimate decision relied on the application of the merger doctrine.[283] The data cannot be protected by copyright law.[284] Notably, the data under consideration in both cases constituted an authored work of expression; therefore, it could be covered by copyright as an authored work.[285] However, considering that these data represented the idea behind the analytics that led to their creation, extending copyright protection would have been tantamount to granting a monopoly over the idea.[286] Thus, copyright can protect data if the process through which it is created fulfills the legal requirements of creation as an original expression.

US jurisprudence on the copyrightability of raw and processed data is consistent with the decisions in Canada. In *Geophysical Service, Inc. v. Encana Corp.,*[287] the Alberta Court of Queen's Bench categorized seismic data about the ocean floor into field and processed data.[288] The field data were described as "[t]he original recorded geophysical data,

279. *See* Pamela Samuelson, *Reconceptualizing Copyright's Merger Doctrine*, 63 J. COPYRIGHT SOC'Y U.S.A. 417, 417 (2016); Red Label Vacations, Inc. v. 411 Travel Buys Ltd., [2015] 18 F.C.R. 473, para. 98 (Can.) ("[W]hen an idea can be expressed in only a limited number of ways, then its expression is not protected as the threshold of originality is not met.").

280. *N.Y. Mercantile*, 497 F.3d at 116.

281. BanxCorp v. Costco Wholesale Corp., 978 F. Supp. 2d 280, 300 (S.D.N.Y. 2013).

282. *Id.* at 303.

283. *Id.* at 311; *N.Y. Mercantile*, 497 F.3d at 118.

284. *N.Y. Mercantile*, 497 F.3d at 118.

285. *See* SCASSA, *supra* note 210, at 8.

286. *See id*. at 8–9.

287. Geophysical Serv. Inc. v. EnCana Corp., 2016 ABQB 230, para. 115 (Can.).

288. *Id.*

sometimes referred to as basic or raw data, together with the description of the complete recording parameters."[289] Justice Eidsvik decided that field data constitutes a literary work as a "compilation" and meets the "skill and judgment" test of originality that the Canadian Supreme Court laid out in *CCH Canadian Ltd.* ("*CCH Canada*").[290] Given that originality in compilation works lies in the "selection or arrangement of data," copyright does not exist in the field of raw data itself when it comes to field data.[291] Here, the judge defined "processed data" as "any product derived, generated or created from the data, including, but not limited to any and all processed and reprocessed data, interpretations, maps or analyses, regardless of the form or medium on which it is displayed or stored."[292] She wrote:

> [a]s for the processed data, the processors exercise skill and judgment in the decisions they make to create a usable product from the [raw] data… [t]he evidence is clear that the processed product can be quite different depending on the skill of the processor and that exploration companies have their favorite processors who create the best quality product for their purposes.[293]

Making a distinction between raw and processed data as to the type of "skills and judgment" exercised—with raw data, the skill and judgment concerning "the collection, arrangement, distillation, and compilation," and with processed data, "the decisions [made] to create a usable product from the field data"— Justice Eidsvik recognized copyright in the processed data itself but excluded raw data from copyrightability.[294] Therefore, as applied in US and Canadian jurisprudence, data that merely represents objective facts does not have copyright protection; instead, copyright subsists in the compilation of such data. Moreover, data processed from raw data can attract copyright, depending on the process of its creation. In this respect, it begs the question: given that compilations and processed data are theoretically copyrightable, why can these works be denied protection on the basis of how they are created?

---

289. *Id*. at para. 47.

290. *Id*. at paras. 74, 77–78; CCH Canadian Ltd. v. L. Soc'y Upper Can., [2004] 1 S.C.R. 339, para. 16 (Can.).

291. Geophysical Serv. Inc. v. EnCana Corp., 2016 ABQB 230, para. 77 (Can.) ("[D]ata becomes a 'work' when it is compiled. One ping from a hydrophone would not suffice; it is the collection, arrangement, distillation and compilation that creates the work."); Copyright Act, R.S.C. 1985, c C-42, s 2 (Can.) (defining "compilation" as "a work resulting from the selection or arrangement of literary, dramatic, musical or artistic works or parts thereof, or . . . a work resulting from the selection or arrangement of data").

292. *Geophysical*, 2016 ABQB 230 at para. 58 (Can.).

293. *Id*. at para. 83.

294. *See* SCASSA, *supra* note 210, at 10.

As discussed in Part II, most user data is collected by AI-enabled sensors and processed by AI-based data analytics.[295] For the product of data collection and data processing to enjoy copyright as a "work" distinguishable from facts, it must be authored by a human.[296] If a fully automated process has generated the data without human involvement, such data will not be covered by copyright.[297] There is currently an extensive debate about the fate of AI-generated works, where AI generates works otherwise copyrightable but lack human authorship.[298] Nevertheless, AI simply being involved in creation will not necessarily result in a denial of copyright to the resulting work.[299] In the above-mentioned US and Canada cases, the data under consideration were generated by either non-AI algorithms in settlement prices and calculated percentages or by complex processes, such as those used to collect underwater seismic data.[300] Thus, some categories of data, such as technical and machine data, are not necessarily excluded from copyright simply because they are automatically collected through sensors.

Based on the recent jurisprudence,[301] user data in the form of activity data—such as farm operation data, which originates in farmers'

---

295. *See supra* Part II; *How Big Data and Artificial Intelligence Are Transforming Business*, INSIGHT (May 28, 2021), https://www.insight.com/en_US/content-and-resources/2021/how-big-data-and-artificial-intelligence-are-transforming-business.html [https://perma.cc/7VVL-F7WP].

296. *See* Urantia Found. v. Maaherra, 114 F.3d 955, 958 (9th Cir. 1997) ("[S]ome element of human creativity must have occurred in order for the book to be copyrightable."). The United States Copyright Office will refuse to register a claim that lacks human authorship. *See* U.S. COPYRIGHT OFF., COMPENDIUM OF U.S. COPYRIGHT OFFICE PRACTICES § 608 (3d ed. 2021), https://www.copyright.gov/comp3/docs/compendium.pdf [https://perma.cc/4M2L-VHYE] [hereinafter COMPENDIUM OF U.S. COPYRIGHT OFFICE PRACTICES]; *see also* Pamela Samuelson, *Allocating Ownership Rights in Computer-Generated Works*, 47 PITT. L. REV. 1186, 1224 (1986) ("[I]f there is no human author of such a work [computer-generated works], how can any human be motivated to create it? The copyright system assumes that society awards a set of exclusive rights to authors for limited times in order to motivate them to be creative.").

297. *See Telstra Corp. Ltd. v. Phone Directories Co. Pty. Ltd.* [2010] FCA 44 (8 February 2010) (Austl.). The High Court of Australia denied copyright protection for telephone directories that were created by automated process, on the ground that such process lacks human authorship. *See id.*

298. Jared Vasconcellos Grubow, *O.K. Computer: The Devolution of Human Creativity and Granting Musical Copyrights to Artificially Intelligent Joint Authors*, 40 CARDOZO L. REV. 387, 420 (2018). (arguing that the "promotion of progress is best served by giving AIs rights and regulating them").

299. *See* SCASSA, *supra* note 210, at 9–10.

300. *See Urantia Found.*, 114 F.3d at 956–59; Scassa, *supra* note 210, at 9–10.

301. *See generally* Tesh W. Dagne, *Embracing the Data Revolution for Development: Rights-based Governance for Farm Data in the Context of African Indigenous Farmers*, 25 J.L. SOC. JUST. & GLOB. DEVELOP. 16 (2021) (discussing the typical legal analysis of farm data as intellectual property).

operations or associated activities—may be eligible for copyright protection. The value attached to such data arises from farmers' knowledge and practices, which in some contexts, are acquired from the farmers' role as custodians of a systemic body of knowledge, accumulated experience, informal experiments, and understanding of the environment.[302] Farmers exercise their skill and judgment when entering their operation data into a data platform or software to create the activity data.[303] Data-sharing agreements typically recognize farmers' rights to the same extent as recognized by law but require farmers to grant the platform owners "a non-exclusive license to access, use, reproduce, display, modify and prepare derivative works."[304] However, given the exploitative nature of such contracts in the face of the existing power imbalance,[305] the relevant question is: How can data originators assert control over this data so it is not transferred to third parties without consent? After sharing their valuable data with platform operators, could data originators demand access to processed data that have been mixed with technical and machine data? Current law does not provide sufficient answers to these questions; hence, this Article's proposal for a new *sui generis* regime.

The other category of user data—machine and device data—may have unique significance in big-data applications like farm machinery and equipment, but its related ownership questions are not as unique. Questions surrounding the ownership and control of machine data are present in the automotive industry, specifically concerning smart cars, and have motivated the EU's proposal to recognize the rights of data producers.[306]

Currently, it is uncertain who owns machine-and-device data: the equipment manufacturer, the equipment owner, or no one. Machine-and-device data is categorized as an objective representation of facts and is therefore uncopyrightable.[307] While this data is stored in cloud

302. This is the case with the practice of agriculture by indigenous peoples and local communities. *See generally id.* (discussing the typical legal analysis of farm data as intellectual property).

303. See Madeline Turland & Peter Slade, *Farmers' Willingness to Participate in a Big Data Platform*, 36 AGRIBUSINESS 20, 20–22 (2019).

304. *See, e.g.*, *Climate FieldView Terms of Service*, *supra* note 143.

305. *See generally* van der Burg et al., *supra* note 4 (discussing how the European Union encourages transparency in using agricultural data via contracts).

306. *See* P.B. HUGENHOLTZ, DATA PROPERTY: UNWELCOME GUEST IN THE HOUSE OF IP 1 (2017), https://pure.uva.nl/ws/files/16856245/Data_property_Muenster.pdf [https://perma.cc/EVJ3-TLV3] (noting that the EU's calls for the introduction of a novel property right in data are in response to demands from the automotive industry).

307. *See* Jeffrey Johnson, *What Works Cannot Be Copyright Protected?*, FREE ADVICE, https://www.freeadvice.com/legal/what-works-cannot-be-copyright-protected/

storage or on a computer hard drive, such storage does not give rise to copyright protection available to compilations because the automatic collection and arrangement of machine-and-device data is purely mechanical.[308] In typical terms of use agreements, equipment users such as farmers can opt out of sharing machine data.[309] However, users can also be discouraged from opting out of data sharing. Opting out may mean that software updates and upgrades are not received. Often, equipment manufacturers embed licensed onboard software that requires upgrades and exclusive servicing by the manufacturer's affiliates contingent on data sharing.[310]

In addition, equipment manufacturers often secure themselves as the de facto owners of machine data by controlling access to the data through proprietary software, which collects, stores, and transmits the data.[311] As John Deere stated in a 2015 filing with the US Copyright Office, the farmers acquired "an implied license" to operate their tractors and had no right to access such software.[312] Moreover, this software often incorporates barriers as TPMs.[313] The *Canadian Copyright Act* and the *US Digital Millennium Copyright Act* (DMCA) include anticircumvention provisions that prohibit circumventing TPMs to access data without the permission of the software owner.[314] These mechanisms curtail users' ability to access diagnostic data for

---

[https://perma.cc/R3FK-ZJNG] (July 16, 2021); *see also* Jack Vaughan, *Machine Data*, TECH-TARGET, https://internetofthingsagenda.techtarget.com/definition/machine-data [https://perma.cc/66CW-GRW8] (last updated Dec. 2014) (defining and providing examples of machine data).

308. *See* COMPENDIUM OF U.S. COPYRIGHT OFFICE PRACTICES, *supra* note 296, at §§ 727–727.3.

309. *See* JOHN DEERE, JOHN DEERE PRIVACY POLICY ON DATA NOTICE 2 (2022), https://www.deere.com/assets/pdfs/common/privacy-and-data/mjd-privacy-notice/mjd-privacy-notice_r2_5.25.18_en_EN.pdf [https://perma.cc/5FRL-225V] ("To remove dealer access to Machine Data from machines in your account you must do both of the following: remove Service ADVISOR™ Remote access for each machine from the Terminal Settings tab in the Operations Center and remove access to machine notifications and advisors from the Partner Access tab in Operations Center.").

310. AUSTL. FARM INST., THE IMPLICATIONS FOR DIGITAL AGRICULTURE AND BIG DATA FOR AUSTRALIAN AGRICULTURE 44 (2016), https://www.crdc.com.au/sites/default/files/pdf/Big_Data_Report_web.pdf [https://perma.cc/P94P-3RLE].

311. *See* Zhang, *supra* note 2, at 316.

312. John Deere, Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201, at 6 (2015), https://www.copyright.gov/1201/2015/comments-032715/class%2021/John_Deere_Class21_1201_2014.pdf [https://perma.cc/MFR3-4PBF].

313. *See generally* Ian R Kerr, Alana Maurushat & Christian S. Tacit, *Technical Protection Measures: Tilting at Copyright's Windmill*, 34 OTTAWA L. REV. 7 (2003) (providing an overview of technological protection measures).

314. Copyright Act, R.S.C. 1985, c C-42, s 41.1(1) (Can.) ("No person shall circumvent a technological protection measure. . . ."); 17 U.S.C. § 1201(a)(1)(A) ("[N]o person shall circumvent a technological measure that effectively controls access to a work protected under this title.").

repairing and maintaining equipment, such as tractors and farm implements.

Given the inaccessibility of the nearest urban centers where a tractor dealer could service their equipment, farmers have a unique capacity for self-reliance; they depend on their own ability, or the abilities of their neighbors, to service and maintain their equipment.[315] In consideration of this, the US Copyright Office issued a recommendation in 2015 to exempt the software embedded in motorized vehicles from the DMCA to save farmers from liability.[316] Nevertheless, equipment manufacturers, such as John Deere, have begun to incorporate a license agreement prohibiting new tractor owners from tampering with the "security measures" in embedded software, contractually bypassing the regulatory exemption and forcing farmers to seek repairs from licensed John Deere dealers.[317]

As a result, in a highly publicized move, farmers started to "hack their tractors" to repair their equipment through "software [that] is cracked in Eastern European countries such as Poland and Ukraine and then sold back to farmers in the United States."[318] Farmers were able to purchase the necessary diagnostic tools and cables to utilize the software in making repairs.[319] Others resorted to buying forty-year-old tractors that still function and are more repairable than new models.[320] The problem fueled a "right-to-repair" movement, which resulted in the introduction of legislation in twenty states and a call by two Democratic

---

315. *One in Five Americans Live in Rural Areas*, U. S. CENSUS BUREAU (Aug. 9, 2017), https://www.census.gov/library/stories/2017/08/rural-america.html#:~:text=One%20in%20Five%20Americans%20Live%20in%20Rural%20Areas&text=About%2060%20million%20people%2C%20or,different%20things%20to%20different%20people [https://perma.cc/U86J-WEXB] (noting that rural areas comprise 97 percent of US land mass with roughly 19 percent of the population, while urban centers make up only 3 percent of the US land mass but are home to more than 80 percent of the population).

316. *See* MARIA A. PALLANTE, REGISTER OF COPYRIGHTS & DIR., U.S. COPYRIGHT OFF., SECTION 1201 RULEMAKING: SIXTH TRIENNIAL PROCEEDING TO DETERMINE EXEMPTIONS TO THE PROHIBITION ON CIRCUMVENTION 1 (2015), https://cdn.loc.gov/copyright/1201/2015/registers-recommendation.pdf [https://perma.cc/33MG-GSVN].

317. *See* JOHN DEERE, LICENSE AGREEMENT FOR JOHN DEERE EMBEDDED SOFTWARE 1 (2021), https://www.deere.com/assets/pdfs/common/privacy-and-data/docs/agreement_pdfs/english/2016-10-28-Embedded-Software-EULA.pdf [https://perma.cc/258Z-BS84].

318. Jason Koebler, *Why American Farmers Are Hacking Their Tractors with Ukrainian Firmware*, VICE (Mar. 21, 2017, 3:17 PM), https://www.vice.com/en/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware [https://perma.cc/A6VF-DXNQ].

319. Stef Schrader, *Farmers Are Having to Hack Their Own Tractors Just to Make Repairs*, DRIVE (Feb. 9, 2021), https://www.thedrive.com/news/39158/farmers-are-having-to-hack-their-own-tractors-just-to-make-repairs [https://perma.cc/3SEQ-QP4Q].

320. Matthew Gault, *Farmers Are Buying 40-Year-Old Tractors Because They're Actually Repairable*, VICE (Jan. 7, 2020, 9:57 AM), https://www.vice.com/en/article/bvgx9w/farmers-are-buying-40-year-old-tractors-because-theyre-actually-repairable [https://perma.cc/8CQ9-57KZ].

presidential candidates (Elizabeth Warren and Bernie Sanders) for federal legislation to give farmers the right to fix their own tractors and equipment.[321] In early July 2021, President Biden issued an executive order, which requires equipment and device manufacturers to publicly post the diagnostic tools and documentation (containing machine-and-device data) for technology users to use to fix products when they break.[322] In Canada, a right to repair bill was introduced by the Ontario legislature but voted down.[323] Moreover, while similar legislation was introduced in Quebec, a private members bill—Bill C-272, which proposes that a "right of repair" be added to section 41 of the Copyright Act—was voted on unanimously upon second reading on June 2, 2021.[324]

Users originate most types of data, whether as technical data containing vital information about the farm, livestock, and the human body, *inter alia*, or as activity data, such as farm operation data that reveals farmers' know-how in the practice and management of agriculture.[325] As equipment, machines, and devices become more sophisticated, the incorporation of IoT technology facilitates the production of a vast amount of machine and device data. However, copyright would not extend to technical or machine-and-device data.[326] Even though copyright could subsist over activity data, contractual stipulations bypass the practical means of asserting this right.[327]

Nevertheless, once shared with data collectors, user data becomes a subject of appropriation through forms of ownership and technical control.[328] The discussion in this Section has shown how such control presents an obstacle to technology users' self-reliance and independence by denying them access to machine data. Thus, public policy needs to

---

321. Matthew Gault, *Bernie Sanders Calls for a National Right-to-Repair Law for Farmers*, VICE (May. 5, 2019, 4:48 PM), https://www.vice.com/en/article/8xzqmp/bernie-sanders-calls-for-a-national-right-to-repair-law-for-farmers [https://perma.cc/JH5V-28NG].

322. Erin Carson, *FTC Votes to Fight Illegal Restrictions on Right to Repair*, CNET (July 22, 2021, 7:30 AM), https://www.cnet.com/news/politics/ftc-votes-to-fight-illegal-restrictions-on-right-to-repair/ [https://perma.cc/J37E-42XR].

323. Shruti Shekar, *Right to Repair Bill Failed, but Liberal Ontario MPP Wants to Push to Take It Federally*, MOBILESYRUP (May 3, 2019, 3:58 PM), https://mobilesyrup.com/2019/05/03/michael-coteau-right-repair-bill/ [https://perma.cc/P2L4-RAAZ].

324. Anthony Rosborough, *A Canadian Right to Repair Bill Sees 330-0 Vote, as Measure Clears Key Hurdle*, REPAIR.ORG (June 3, 2021), https://www.repair.org/blog/2021/6/3/a-canadian-right-to-repair-bill-sees-330-0-vote-as-measure-clears-key-hurdle [https://perma.cc/X68S-Y2R4].

325. Jakku et al., *supra* note 77, at 1–2.

326. SETH GREENSTEIN & DAVID GOLDEN, THE INTERNET OF THINGS: IMPLICATIONS FOR COPYRIGHT AND PRIVACY 3–18 (2018), https://constantinecannon.com/wp-content/uploads/2018/04/IoT-Presentation-Greenstein-Golden-20180418.pdf [https://perma.cc/7P3X-TRH4].

327. *See* discussion *supra* Section V.A.

328. *Climate FieldView Terms of Service*, *supra* note 143.

guarantee users access to machine-and-device data while empowering them to maintain control over activity data. Furthermore, control over technical data, such as agronomic data, is paramount given the detrimental effect of potentially disclosing such data to third parties. The discussion thus far demonstrates a gap in recognizing the value generated by data for its originators.

In contrast, such data sometimes becomes the subject of copyright by data collectors and processors, either as a compilation or in the form of processed data.[329] This trend is exacerbated in circumstances where copyright is clearly asserted in user data that is de-identified and aggregated. The following discussion uncovers such scenarios.

ii. Copyrightability of Aggregated Data

As shown in the above discussion, contractual stipulations between data originators and data collectors often assign ownership of "aggregated or anonymized data" to data collectors.[330] The question here is whether there is any basis in law underlying such a contractual claim of ownership of aggregated user data. The assertion of ownership over such data is based on the claim that it constitutes independent work once it is processed and generated by a computer software system.[331] Once user data is shared with data collectors and processed with data analytics and computer-software systems, will copyright subsist over the data and result in collectors' copyright ownership of such data?

The answer to this question will depend on the processing that goes into the data, which determines whether a copyright may subsist either as a "compilation" or a data form. In both cases, illustrated in the

---

329. *Data Collections and Copyright*, FED'N UNIV. AUSTL., https://federation.edu.au/library/about-the-library/copyright/A-Z-copyright-guide/data-collections-and-copyright [https://perma.cc/YCJ4-XQMU] (last visited Mar. 2, 2022).

330. *See, e.g.*, *Climate FieldView Terms of Service*, *supra* note 143 ("We own any works we generate ("Climate Generated Works"), including data, tools, analyses, results, estimates, prescriptions, recommendations and other information generated, published, displayed, transmitted or made available to you in or by the FieldView Services . . . whether or not the Climate Generated Works are related to personal data, Customer Farm Data or Third Party. Climate Generated Works include "Aggregated or Anonymized Information," which is information that has been aggregated or anonymized such that it is not personally identifiable to you by a person using reasonable skills. Aggregated or Anonymized Information is not considered Customer Farm Data.").

331. *See, e.g.*, AGWORLD, AGWORLD MASTER SUBSCRIPTION AGREEMENT 5 (2020), https://agworld-marketing.s3.amazonaws.com/MSA-2020-02-22.pdf [https://perma.cc/EQB6-4FP5] ("We own and will hold copyright in the particular formats and manner of presentation We use to display and present Your Data.").

above discussion, the test relies on whether the process of creating the compilation, or data, satisfies originality, with both tests distinguishing between facts, data, and the doctrine of merger fulfilled.[332] The process of creating or compiling the data must also involve human authorship.[333] The question of when originality exists in the compilation of aggregated data was most recently addressed by Canada's Federal Court of Appeal in *Toronto Real Estate Board (TREB) v. Commissioner of Competition*,[334] which agreed with the earlier ruling of the Competition Tribunal in which:

> The Tribunal considered a number of criteria relevant to the determination of originality (paragraphs 737-738 and 740-745). Those included the process of data entry and its "almost instantaneous" appearance in the database. It found that "TREB's specific compilation of data from real estate listings amounts to a mechanical exercise" (TR at para. 740). We find, on these facts, that the originality threshold was not met.[335]

In this case, TREB operates a database system that contains property information, including addresses, price lists, and photographs of real estate listings.[336] Information is added to the database on an ongoing basis by real estate brokers, who contribute data each time a property is listed with them.[337] Members of TREB receive full access to the database via an electronic feed.[338] They may make these data available through their websites.[339] Simultaneously, some data available in the database are not distributed via the data feed; TREB allows members to share such data by fax, email, or telephone, restricting the sharing of some of the data through "virtual office" websites, which are accessible to clients.[340]

TREB claimed that its restriction consisted only of enforcing its copyright interest in its compiled database.[341] This claim was dismissed because the compilation failed to meet the tests of originality, as quoted above.[342] Besides originality, the Federal Court of Appeal offered certain guidelines relevant for assessing the existence of copyright over

---

332. *See* discussion *supra* Section VI.B.i.

333. *See* discussion *supra* Section VI.B.i.

334. Toronto Real Estate Bd. v. Comm'r of Competition, [2018] 3 F.C.R. 563, paras. 185–88 (Can.).

335. *Id.* at para. 194.

336. *Id.* at para. 5.

337. *Id.*

338. *Id.* at para. 2.

339. *Id.*

340. *Id.* at para. 6.

341. *See id.* at para 2.

342. *See id.* at paras. 194–95.

aggregated agricultural data.[343] Most relevant, the court stated that while "TREB's contracts with third parties refer to its copyright, . . . that does not amount to proving the degree of skill, judgment or labor needed to show originality and to satisfy the copyright requirements."[344] In user data, contractual stipulations often refer to aggregated data generated by software and computer systems as copyrightable works.[345] However, though contractually binding to the user, such provisions in themselves do not prove originality under copyright.[346]

This Canadian jurisprudence on originality requirements in the compilation of aggregated data is consistent with US jurisprudence.[347] In a decision rendered in the wake of the US Supreme Court decision in *Feist Publications, Inc. v. Rural Telephone Service Company*, which held that copyright does not subsist in the information contained in a phone directory,[348] the Second Circuit found copyright in a compendium of projections of used car valuations.[349]

Often, contractual provisions for data sharing provide for the sweeping assertion of copyrights over aggregated agricultural data generated by software and computer systems.[350] In relation to the dispute in which a group of American chicken farmers brought class actions in consideration of the potential harm posed by improperly sharing agricultural data,[351] Agri Stats, the operator of the agricultural data-sharing app, regarded the data collected from farmers as the company's "confidential and proprietary information."[352] As a matter of business practice, TPs, data intermediaries, and data platforms make such data accessible to anyone through subscription fees.[353] Thus, technology users are forced to accept "click-through licenses" to gain

343. *Id*. at paras. 187–95.

344. *Id.* at para. 195.

345. For example, Climate FieldView uses the copyright word "works" in referring to its software-generated content. *Climate FieldView Terms of Service*, *supra* note 143 ("We own any works we generate ("Climate Generated Works"), including data.").

346. *Toronto Real Estate Bd.*, [2018] 3 F.C.R. 563 at para. 196 (Can.).

347. *Id.* at para. 184.

348. Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 363–64 (1991).

349. CCC Info. Servs. v. MacLean Hunter Mkt. Reps., Inc., 44 F.3d 61, 63 (2d Cir. 1994); *see also* Mason v. Montgomery Data, Inc., 967 F.2d 135, 140–42 (5th Cir. 1992) (holding that a compilation of real estate ownership data superimposed on maps was protectible because the compiler made independent choices "to select information from numerous and sometimes conflicting sources" such as various public records and combined the data onto "an effective pictorial expression").

350. Wiseman et al., *supra* note 131, at 8.

351. *See Douglas*, *supra* note 114.

352. Leonard, *supra* note 109.

353. *See id.*

access to the data.[354] Consequently, data collectors, processors, and aggregators effectively exercise copyright ownership over the aggregated data.

Given that recent jurisprudential developments provide the possibility for copyright claims to processed data and compilation of raw data,[355] there are circumstances where copyright may indeed exist over aggregated data. For ATPs, data intermediaries, and data platforms, for example, the assertion of rights over agricultural data, whether through contracts or copyright, relies on the ground that such data, once collected and aggregated, lies outside the scope of "personal data"—the ownership of which is often clearly stipulated in contracts as belonging to farmers.[356] In addition to a narrow scope of recognition of "personal data" in the agreements,[357] legal protection under privacy regimes is sidestepped in aggregated data because such data are de-identified.[358] Setting aside the failure of de-identification techniques and the possibility of re-identification through advanced processing,[359] aggregated data may still be considered "relating to" farmers' personal data and yet be owned by data collectors.[360]

As noted above, in "privative" copyright jurisprudence, there is a basis for recognizing copyright-based privacy rights to objects that do not meet the statutory requirements of original expression.[361] Thus, even when user data may be excluded from the scope of copyright, there is a jurisprudential basis for recognizing originators' rights in data that could similarly be implemented in other legislation that is modeled on copyright.[362]

---

354. William W. Fisher III, *Property and Contract on the Internet*, 73 CHI-KENT L. REV. 1203, 1245 (1998).

355. *See supra* notes 335–50 and accompanying text.

356. *See supra* text accompanying notes 215–17.

357. *See* discussion *supra* Section V.B.

358. *See supra* text accompanying note 200.

359. *See* Yves-Alexandre De Montjoye, Laura Radaellivivek, Kumar Singhand & Alex "Sandy" Pentland, *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, 347 SCI. 536, 537 (2015).

360. For a discussion of when agricultural data may be "relating to" farmers in discussion, see *supra* text accompanying notes 193–95. *See also Climate FieldView Terms of Service*, *supra* note 143 ("We own any works we generate ("Climate Generated Works"), including data . . . whether or not the Climate Generated Works are related to personal data, Customer Farm Data or Third Party.").

361. *See supra* text accompanying notes 248–53.

362. *See supra* text accompanying notes 248–53; Jane C. Ginsburg, *No "Sweat"? Copyright and Other Protection of Works of Information After* Feist v. Rural Telephone, 92 COLUM. L. REV. 338, 383 (1992) (arguing that works of information excluded from the 1976 Copyright Statute following the tests of originality adopted in *Feist* should be covered by an anticopying statute that departs in significant ways from the traditional copyright scheme).

In what ways could a legal relationship between originators of either processed or aggregated data and data collectors and processors who enjoy ownership over such data be established? This Article advances the argument that even though user data rarely meets copyright law's statutory criteria, such as the originality test, their incorporation in aggregated and processed datasets should nonetheless lead to the creation of a "joint authorship" type relationship over such data that has become subject to copyright, entitling data originators to certain rights.[363] The following discussion elaborates on this argument in light of the doctrine of joint authorship, which makes it suitable for recognizing data originators' contribution of user data to "works" that data collectors and processors hold under copyright.

C. Joint Authorship as a Basis of Relationship

In its origin, copyright assigns authorship to the individual under the construct of the author's solitary, romantic genius.[364] However, conceived in individualistic and solitary terms, the assumption underlying the definition of author under copyright law did not consider the complex process of creation, which depends on a multiplicity of production methods.[365] As Professor Chon notes, "the dual effects of digitization and networking" have exposed the limits of what is considered work and who the author is under traditional copyright principles.[366] As discussed above, the evolving jurisprudence has opened doors to the possibility of data copyrightability, particularly regarding processed data in the form of aggregated data as "works."[367] For a legal framework to enable proper data governance, which recognizes originators' contribution to such "work" under the normative model of privative copyright, the doctrine of joint authorship may be invoked as providing the normative basis to justify certain authorial rights.[368]

Notably, copyright rules relating to joint authorship were developed entirely in an incremental, common-law fashion until the

---

363. *See* discussion *infra* Section VI.C.

364. *See* Peter Jaszi, *Toward a Theory of Copyright: Metamorphosis of "Authorship"*, 1991 DUKE L.J. 455, 462–63 (1991); Martha Woodmansee, *The Genius and the Copyright: Economic and Legal Conditions of the Emergence of the "Author"*, 17 EIGHTEENTH-CENTURY STUD. 425, 426 (1984).

365. *See* Margaret Chon, *New Wine Bursting from Old Bottles: Collaborative Internet Art, Joint Works, and Entrepreneurship*, 7 OR. L. Rev. 257, 264 (1996).

366. *Id.* at 258.

367. *See* discussion *supra* Section VI.B.i.

368. Balganesh, *supra* note 227, at 22–23.

passing of the US Copyright Act of 1976, which, for the first time, dealt with joint authorship through the definition of "joint work."[369] In accordance with the Copyright Act, works produced through collaboration become "joint works," and so the question often arises of what contribution from a putative author qualifies as a work of joint authorship.[370] Despite variation in the wording of the statutes and judicial tests—which later developed in both the United States and Canada—joint authorship arises if there is (i) collaboration between the authors in furtherance of a common design to create the work, or (ii) from each a significant original contribution to the expression of the work, consisting of "inseparable or interdependent parts of a unitary whole" (or in Canada "not distinct" from the other's contribution).[371] In the United States, there is also a statutory requirement of "intention," which the courts have construed as requiring the putative joint authors to have "collaborative intent,"[372] "shared . . . intent,"[373] or "intent to create a joint work."[374]

Although the determination of joint authorship based on the above requirements has made the doctrine hazy in "scenarios where one collaborator's contributions are inextricably tied to those of another,"

369. Copyright Act of 1976, Pub. L. No. 94-553, § 101, 90 Stat 2541 (codified at 17 U.S.C. § 101) ("A 'joint work' is a work prepared by two or more authors with the intention that their contributions be merged into inseparable or interdependent parts of a unitary whole."). While the first US copyright statute, the Copyright Act of 1790, uses the phrase "author or authors" in multiple places, it made no special allowances for joint authorship, nor did it specify how such joint authorship was to be determined. *See* Copyright Act of 1790, 1 Stat 124 (1790) (repealed 1831). The Copyright Act of 1909 focused entirely on a singular "author" throughout. *See* Copyright Act of 1909, Pub. L. No. 60-349, 35 Stat 1075 (1909) (repealed 1976); Shyamkrishna Balganesh, *Unplanned Coauthorship*, 100 VA. L. REV. 1683, 1685 n.10 (2014). In Canada, a "work of joint authorship" is "a work produced by the collaboration of two or more authors in which the contribution of one author is not distinct from the contribution of the other author or authors." Copyright Act, R.S.C. 1985, c C-42, s 2 (Can.).

370. *See* Elena Cooper, *Joint Authorship in Comparative Perspective:* Levy v. Rutley *and Divergence Between the UK and USA*, 62 J. COPYRIGHT SOC'Y U.S.A. 245, 247 (2015); David Vaver, *Recent Copyright Law Developments: More Reform?*, 22 INTELL. PROP. J. 1, 1 (2010).

371. 17 U.S.C. § 101; Copyright Act, R.S.C. 1985, c C-42, s 2 (Can.); *see* Vaver, *supra* note 371, at 2–3.

372. 17 U.S.C. § 101; *e.g.*, Eckert v. Hurley Chi. Co., Inc., 638 F. Supp. 699, 704 (N.D. Ill. 1986).

373. *E.g.*, Aalmuhammed v. Lee, 202 F.3d 1227, 1234 (9th Cir. 2000); Ulloa v. Universal Music & Video Distrib. Corp.,
303 F. Supp. 2d 409, 418 (S.D.N.Y. 2004) (citing Childress v. Taylor, 945 F.2d 500, 509 (2d Cir. 1991)).

374. *E.g.*, Janky v. Lake Cnty. Convention & Visitors Bureau, 576 F.3d 356, 362 (7th Cir. 2009) (citing Erickson v. Trinity Theatre, Inc., 13 F.3d 1061, 1068, 1071 (7th Cir. 1994)); Weissman v. Freeman, 868 F.2d 1313, 1327 (2d Cir. 1989) (Pierce, J., concurring); Papa's-June Music, Inc. v. McLean, 921 F. Supp. 1154, 1157 (S.D.N.Y. 1996) (citing *Childress*, 945 F.2d at 507–08).

the *raison d'être* for the requirement of intention can be replaced by a "collaborative impulse."[375] In such circumstances, there arises what is referred to as "unplanned co-authorship [sic]."[376] In this context, under both Canadian and US law, what matters for the finding of joint authorship is only that the putative co-authors submit contributions that entitle each of them to be classed as authors.[377]

Most US cases follow the so-called "Goldstein standard," which affirms that each author should make an independently copyrightable contribution to be eligible for joint authorship in work.[378] However, a minority of cases have adopted what has come to be called "Nimmer's view of authorship," which requires a putative co-author merely to demonstrate that they made a "non-*de minimis* contribution" to the joint work, even though that contribution may not be independently copyrightable.[379] Goldstein's interpretation of "authorship" relies on the argument that because work requires copyrightability to be a work "of authorship," so too must a creator of a joint work contribute something copyrightable to be considered as an author.[380] Thus, the definition of joint authorship is inevitably linked to the individualism that animates the modern concept of an author.

However, there is support for the proposition that each author of a joint work need not contribute copyrightable work. First, the construing joint authorship as requiring each putative author to contribute independently copyrightable works "form(s) part of a narrow

375. *See* Balganesh, *supra* note 370, at 1689.

376. *Id.*

377. *See* 17 U.S.C. § 101 ("A 'joint work' is a work prepared by two or more *authors* with the intention that their contributions be merged into inseparable or interdependent parts of a unitary whole.") (emphasis added); Copyright Act, R.S.C. 1985, c C-42, s 2 (Can.) ("[W]ork of joint authorship means a work produced by the collaboration of two or more *authors* in which the contribution of one author is not distinct from the contribution of the other author or authors[.]") (emphasis added).

378. PAUL GOLDSTEIN & P. BERNT HUGENHOLTZ, INTERNATIONAL COPYRIGHT 248 (2d ed. 2010) ("[F]or a work to qualify as a joint or collaborative work and a contributor to qualify as a coauthor, each contributor must have brough creative expression to the work.").

379. *E.g.*, Words & Data, Inc. v. GTE Commc'ns Servs., Inc., 765 F. Supp. 570, 575 (W.D. Mo. 1991) (quoting MELVILLE B. NIMMER & DAVID NIMMER, 1 NIMMER ON COPYRIGHT § 6.07 (2021)) ("It would seem, however, that each such contribution must, in any event, be more than *de minimis*. That is, more than a word or line must be added by one who claims to be a joint author."); Gaiman v. McFarlane, 360 F.3d 644, 658–59 (7th Cir 2004); *see also* H.R. Rep. No. 94-1476, at 120 (1976) ("The touchstone [of coownership of joint works] is the intention, at the time the writing is done, that the parts be absorbed or combined into an integrated unit, although the parts themselves may be either 'inseparable' . . . or 'interdependent' . . . .").

380. *See* Norbert F. Kugele, *How Much Does It Take: Copyrightability as a Minimum Standard for Determining Joint Authorship*, 1991 U. ILL. L. REV. 809, 819–20 (1991).

view of joint works taken by courts under the [1976] Copyright Act."[381] Each joint author's requirement to make an independently copyrightable contribution does not have deeper judicial roots, as it is not found in any cases decided under the Copyright Act 1909.[382] Instead, the courts have imposed the requirement, beginning with the standard set by the Second Circuit in *Childress v. Taylor*.[383]

Besides, there is no statutory language to support the view that originality equals authorship, either in joint works or works in general. Section 101 of the 1976 Copyright Act defines a joint work simply as "a work prepared by two or more authors" without reference to the nature of the required contribution.[384] In contrast, section 102(a) sets forth the standards for copyrightable subject matter, with the wording: "[c]opyright subsists in accordance with this title, in *original* works of authorship. . . ."[385] Although the phrase "*original* works of authorship" appears in several portions of the statute, this phrase is notably absent in the "joint works" section.[386] While a bill to insert the word "original" into the definition of joint works—which would thus require each joint author make an original contribution—it was never reported out of committee.[387] It has also been argued that the requirement of originality cannot apply to all uses of the term "author" in the 1976 Copyright Act since an employer, as an author of a work created for hire, need not have supplied any of the originality itself.[388]

As a result, non-original expressions could be authored within the meaning of the 1976 Copyright Act, although such expressions do not attract copyright protection as works under the Copyright statute.[389] In his article on the definition of an author for copyright purposes, with respect to the US Constitution's reference to "authors," Versteeg observes that "[t]he present law [Copyright Act] does not

381. Laura G. Lape, *A Narrow View of Creative Cooperation: The Current State of Joint Work Doctrine*, 61 ALB. L. REV. 43, 84 (1997).

382. *See, e.g.*, Edward B. Marks Music Corp. v. Jerry Vogel Music Co., 140 F.2d 266, 267 (2d Cir. 1944), *modified*, 140 F.2d 268 (2d Cir. 1944); Shapiro, Bernstein & Co. v. Jerry Vogel Music Co., 221 F.2d 569, 570 (2d Cir. 1955); G. Ricordi & Co. v. Columbia Graphophone Co., 258 F. 72, 75 (S.D.N.Y. 1919).

383. Childress v. Taylor, 945 F.2d 500, 507 (2d Cir. 1991). For an analysis of the statutory basis for the standard in *Childress*, see Michael B. Landau, *Joint Works Under United States Copyright Law: Judicial Legislation Through Statutory Misinterpretation*, 54 IDEA 157, 213–18 (2014).

384. 17 U.S.C. § 101.

385. *Id.* at § 102(a).

386. *Id.* at §§ 101, 201(a), 302(b).

387. S. 1253, 101st Cong. (1989).

388. Lape, s*upra* note 382, at 68; *see* Landau, *supra* note 384, at 216.

389. *See* 17 U.S.C. § 102(a).

protect as much subject matter as the constitutional grant [to authors] *could* permit."[390] The contributions of non-original expressions by an author—even though they do not entitle her to be a joint author under copyright because of the prevailing judicial approach—ought nonetheless result in some level of recognition under a *sui generis* statute.

As revealed in the above discussion, user data that has become part of aggregated data, and hence has become copyrightable processed data, could meet the standard of "original expression" as a copyrightable criterion.[391] However, it is unlikely that raw user data, except perhaps for activity data, such as farm operation data, meets the standard set under *Feist* and *CCH Canada*.[392] These categories of data do not meet the copyright's statutory standards of originality as evincing a "modicum of creativity" or "the exercise of skills and judgment" under either US or Canadian standards, respectively, in order to have a standalone right.[393] Nevertheless, user data generated in the form of machine and device data, activity data, or technical data can be analogized to what Professor Ginsburg characterizes as "low authorship works" or "sweat works," which she asserts should be protected.[394] Criticizing the lack of protection for "works at once high in commercial value but low in personal authorship" under the prevailing approach that requires "originality," Ginsburg proposes protection for information works "[where] the worth of the work lies in the information, rather than in the form imposed [by copyright]" through a legislated compulsory licensing regime affording the first compiler compensation.[395]

The argument in this Article is not that user data should be covered by copyright, either independently or as part of a joint work. However, this discussion demonstrates that a *sui generis* legislative framework for user data of diverse categories could be modeled under copyright law, given the normative basis in privative claims and recognition of the contribution of non-copyrightable works of authors under joint authorship doctrine. Therefore, in a data-governance framework that defines the relationship between technology users and

390. Russ Versteeg, *Defining "Author" for Purposes of Copyright*, 45 AM. U.L. REV. 1323, 1324 (1996).

391. *See* discussion *supra* Section VI.B.i.

392. *See* CCH Canadian Ltd. v. L. Soc'y of Upper Can., [2004] 1 S.C.R. 339, 341 (Can.); Feist Publ'ns, Inc., v. Rural Tel. Serv. Co., Inc., 499 U.S. 340, 345 (1991).

393. *See CCH Canadian*, [2004] 1 S.C.R. at 352 (Can.); *Feist*, 499 U.S. at 346.

394. Jane C. Ginsburg, *Creation and Commercial Value: Copyright Protection of Works of Information*, 90 COLUM. L. REV. 1865, 1927–29 (1990).

395. *Id.* at 1866, 1869, 1916.

data originators on the one hand and data collectors and processors on the other, copyright law could provide a model for recognizing users' contributions as sources of data. Thus, the next question that presents itself is: What is the nature and scope of the rights that should be recognized in a legislative intervention on behalf of data originators?

VII. NATURE AND CONTENT OF RIGHTS IN POTENTIAL LEGISLATIVE INTERVENTION TO SUPPORT DATA ORIGINATORS

The proposed *sui generis* framework would be best modeled on copyright law because the nature of rights to be included is best structured as a private law claim. Being that such a framework has normative roots in copyright does not suggest that data originators acquire ownership rights similar to an actual joint owner. Instead, just like copyright operates by granting creators a private cause of action for certain kinds of unauthorized use of their works,[396] data originators should be given specific rights that could be enforced through private rights of action, imitating those granted by copyright.

The proposed framework recognizes that once user data has been shared with data collectors and aggregated with a mix of different data categories, its potential is best maximized by treating it as a resource from which insights can be derived and shared. User data, such as agricultural data, are a non-rivalrous good that multiple parties can consume without diminishing the initial value enjoyed by other users of that data.[397] As such, user data are generally worth more to everyone (including those who generated them) when shared than when analyzed in silos.[398] While deciding whether or not to share data remains with the data originator, legal principles make "ownership" of user data challenging to define.[399] Such ownership framework mainly reinforces and strengthens data collectors' and data processors' claims for monopoly over data. Hence, the content of the originators' claims to user data is best defined as a right to access and maintain control.

With such rights, data originators can utilize data in their production and marketing decisions regarding their agricultural

396. *See* Shyamkrishna Balganesh, *The Obligatory Structure of Copyright Law: Unbundling the Wrong of Copying*, 125 HARV. L. REV. 1664, 1667–69 (2012) (discussing how copyright law borrows a normative, bipolar entitlement structure from elsewhere in private law).

397. Noah J. Miller, Terry W. Griffin, Paul Goeringer, Ashley Ellixson & Alekshan Shanoyan, *Estimating Value, Damages, and Remedies When Farm Data are Misappropriated*, CHOICES, Jan. 31, 2019, at 2.

398. *See id.* at 3.

399. *See* Charles I. Jones & Christopher Tonetti, *Nonrivalry and the Economics of Data*, 110 AM. ECON. REV. 2819, 2822 (2020).

activity. Also, the right to control data would enable data originators to ensure that the data they willingly share with TPs, data platforms, and data intermediaries are not shared with third parties without the originators' consent. Furthermore, if the data are transferred without their consent, originators would have a cause of action irrespective of what the data-sharing contract may provide.

The lack of a mechanism to ensure such access and control over data brings issues of trust and uncertainty regarding data and the outcome of related analysis in the age of big data.[400] The expansive rights granted to data aggregators under users' contractual relationships should be limited to protect technology users, as the weaker contracting parties, through mandatory rules of law. Such mandatory rules have long been standard in all jurisdictions to protect groups of individuals who are recognized as the weaker parties in their contracting relationships with others (e.g., employees and tenants).[401] The above discussion shows the need to guarantee the data originator's claim for access to and control over user data through a legal framework, containing rules of mandatory law that do not leave room for contractual deviation from the rules laid down within it. Such a guarantee should recognize originators' rights (entitlement) to user data. Given the normative roots for such a legal framework in copyright law, as discussed above, it is recommended that such a legal framework be adopted at the federal level in both the United States and Canada.

In defining the content of rights, the relationship of data originators to user data can be characterized both as authorial—namely, as contributors to what is held under copyright—and as users in implementing data to effectively engage in the digital economy, such as through digital agriculture. Thus, at a minimum, a potential *sui generis* legislative framework modeled on copyright for user data ought to recognize two rights that flow from these two characterizations in this respective order: the right to control disclosure and the right of access.

A. Right to Control Disclosure

The first and most crucial right that ought to be recognized for proper governance of user data and which flows directly from recognizing data originators as contributors to data under proprietary control is the right to control disclosure. As noted earlier, the right of disclosure is embedded in the common-law right of first publication of

400. *See* Gullo et al., *supra* note 45.

401. *Cf.* Anthony T. Kronman, *Contract Law and Distributive Justice*, 89 YALE L.J. 472, 491–93 (1980) (advancing the principle of "paretianism," which seeks to balance libertarian and egalitarian impulses in contracting).

unpublished works, subsumed under the exclusive right of public distribution under the US Copyright Act of 1976.[402] Given the criteria of this Act, which exclude non-original expressions from the scope of protection, a suitable *sui generis* regime for user data ought to codify the right in the form of control over the disclosure of data generated by originators.[403] To fully understand the scope of rights that technology users, such as farmers, can acquire by recognizing rights that simulate the right of disclosure, it is necessary to illuminate how the right of disclosure works in those civil law jurisdictions that recognize it in their copyright legislation.

The right of disclosure is a bundle of rights within the ambit of moral rights, broadly recognized in civil law jurisdictions (along with attribution, integrity, and withdrawal rights).[404] Moral rights are characterized as inherent rights of the author, meaning that they belong to those who actually created the work in question and not those who own copyright upon assignment.[405] The right of disclosure enables the holders to control the publication of their works, empowering them with the ultimate decision over whether a work is complete and should be made public.[406] The similar right of first publication, represented in the Copyright Act of 1976 through the right of public distribution, "failed to account for the alienability of the rights," thereby morphing "into an unrecognizable and unjustifiable right that may be asserted regardless of the identity of the person asserting it."[407] However, the right of disclosure is an inalienable right that "recognizes the author as the ultimate judge of when and under what conditions a work can be disseminated."[408] Therein lies the unique significance of the right of disclosure: the author can impose conditions on how a work is disseminated, and such a right cannot be transferred through contractual arrangements.

---

402. *See* Keller, *supra* note 232, at 26.

403. *See* Ginsburg, *supra* note 363, at 381.

404. *See* Cyrill P. Rigamonti, *Deconstructing Moral Rights*, 47 HARV. INT'L L.J. 353, 359 (2006); *cf.* Adolf Dietz, *The Moral Right of the Author: Moral Rights and the Civil Law Countries*, 19 COLUM.-VLA J.L. & ARTS 199, 213–17 (1995) (comparing different approaches to moral rights among western European countries).

405. ARTHUR R. MILLER & MICHAEL H. DAVIS, INTELLECTUAL PROPERTY: PATENTS, TRADEMARKS, AND COPYRIGHT IN A NUTSHELL 448 (5th ed. 2012) ("[T]he person claiming the moral right typically no longer own the work itself or the copyright. The claim is thus based on a different, inherent right that is part of authorship itself.").

406. See Kathryn A. Kelly, *Moral Rights and the First Amendment: Putting Honor Before Free Speech?*, 11 U. MIA. ENT. & SPORTS L. REV. 211, 216 (1994).

407. Keller, *supra* note 232, at 36.

408. Lior Zemer, *Moral Rights: Limited Edition*, 91 B.U.L. REV. 1519, 1524 n.26 (2011).

In modeling data governance for user data through the right of disclosure, data originators ought to retain the right to decide what data are disclosed to third parties and how, after sharing contractual data with a TP, data intermediary, or data platform. Given the possibility of aggregated user data being tied back to an individual or their farm, for example, such right of disclosure is essential to address data originators' fears and concerns in data sharing. Recognizing the right of disclosure would also help prevent the potential abuse of power that is enabled by data-sharing practices, such as those that have arisen in class actions in the US poultry industry.[409] The right of disclosure resembles the right to control personal data in privacy regimes.[410] However, it fills the void created in such regimes because user data cannot qualify as "personal data," even when "relating to" a particular individual or to the means of their economic dependence, such as the farm.[411]

B. Right of Access as a Counterbalance to Access-Right

Access-right is a new right that has emerged in digital copyright jurisprudence and scholarship over the last two decades.[412] "Access-right" is described as the copyright owners' "right to control the manner in which members of the public apprehend the work. . . [through] a right against the gaining of unauthorized access."[413] Although this right was explicitly introduced by the DMCA in 1998 and became an integral part of copyright in the wake of the availability of mass-copying devices,[414] Professor Ginsburg states that it was "implicit in the reproduction and distribution rights under copyright" law in earlier times but has evolved to extend to new forms of exploitation in the digital age.[415]

---

409. *See supra* notes 109–14 and accompanying text.

410. *See* discussion *supra* Section VI.A.

411. *See supra* notes 193–95 and accompanying text.

412. *See, e.g.*, Stephen B. Popernik, *The Creation of an "Access Right" in the Ninth Circuit's Digital Copyright Jurisprudence*, 78 BROOK. L. REV. 697, 719–22 (2013); Laura N. Gasaway, *The New Access Right and Its Impact on Libraries and Library Users*, 10 U. GA. J. INTELL. PROP. L. 269, 269 (2003). *See generally* ZOHAR EFRONI, ACCESS-RIGHT: THE FUTURE OF DIGITAL COPYRIGHT LAW (2011) (presenting in detail a positive and normative analysis of access-right).

413. Thomas Heide, *Copyright in the EU and U.S.: What "Access-Right"?*, 48 J. COPYRIGHT SOC'Y U.S.A. 363, 364–65 (2001).

414. *See id.* at 363.

415. Jane C. Ginsburg, *From Having Copies to Experiencing Works: The Development of an Access Right in U.S. Copyright Law*, *in* US INTELLECTUAL PROPERTY LAW AND POLICY 49 n.27 (Hugh C. Hansen ed., 2006).

The content of access-right, distinguishable from "copy"-right,[416] has been confirmed in a series of cases as a new cause of action to protect works from unauthorized circumvention of virtual locks and keys (collectively referred to as TPMs).[417] This right has empowered technology companies to contractually customize a set of entitlements to access or use their software in whatever ways the companies think best.[418] Furthermore, such a mechanism is protected with a copyright-based cause of action, which avoids analyzing whether copyright infringement has occurred.[419] As demonstrated in the above discussion, such exercise of an access-right by ATPs, like John Deere, has led to the growing "right to repair" movement in the United States and Canada, which entitles farmers to access machine-diagnostic data.[420]

As a self-standing cause of action, access-right is sometimes construed as not requiring the existence of underlying copyright.[421] Moreover, exceptions to copyright (such as fair use) do not guarantee access to a work to carry out a permitted act under copyright law.[422] In this respect, access-right is juxtaposed with the right to access, which

---

416. *Id.* at 42.

417. *See, e.g.*, MDY Indus. v. Blizzard Ent., Inc., 629 F.3d 928, 943–52 (9th Cir. 2010); Apple, Inc. v. Psystar Corp., 658 F.3d 1150, 1162 (9th Cir. 2011). The statutory basis for the protection of TPMs in the United States is the Digital Millennium Copyright Act, which provides that "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title." 17 U.S.C. § 1201(a)(1)(A). In Canada, the equivalent provision provides that "[n]o person shall . . . circumvent a technological protection measure within the [definition of a technological protection measure]." Copyright Act, R.S.C. 1985, c C-42, s 41.1(1) (Can.).

418. Dan L. Burk, *Legal and Technical Standards in Digital Rights Management Technology*, 74 FORDHAM L. REV. 537, 546 (2005).

419. *See* Popernik, *supra* note 414, at 698–700.

420. *See supra* notes 316–25 and accompanying text.

421. *See, e.g.*, Noah J. Wald, *Don't Circumvent My Dongle! Misinterpretation of the Digital Millennium Copyright Act Threatens Digital Security Technology*, 33 T. JEFFERSON L. REV. 325, 351–53 (2011) (criticizing the court's conflation of the two issues in MGP UPS Sys., Inc., v. GE Consumer & Indus., Inc., 622 F.3d 361 (5th Cir. 2010)). Though some US courts have held that a TPM must protect a copy-right in line with the World Copyright Treaty, which calls for protection of measures that are used "in connection with the exercise of [authors'] rights under this Treaty or the Berne Convention," the DMCA prohibits circumvention of a TPM that "effectively controls access to a work protected under this title." WIPO Copyright Treaty art. 11, *opened for signature* Dec. 20, 1996, S. TREATY DOC. NO. 105-17, 2186 U.N.T.S. 121 (entered into force Mar. 6, 2002); 17 U.S.C. § 1201(a)(1)(A). The difference in language is held to imply that the prohibition under the DMCA does not relate to the infringement of an underlying copyright. *See* Wald, *supra*, at 338–39. *But see* Chamberlain Group, Inc. v. Skylink Techs., Inc., 292 F. Supp. 2d 1023, 1038 (N.D. Ill. 2003) (holding that the DMCA applies to TPMs protected under copyright law).

422. *See* David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 734–77 (2000) (drawing out the unintended consequences of the DMCA's "trafficking ban"); Carys J. Craig, *Digital Locks and the Fate of Fair Dealing in Canada: In Pursuit of "Prescriptive Parallelism"*, 13 J. WORLD INTELL. PROP. 503, 510–12 (2010) (noting the clash between TPMs and Canada's doctrine of "fair dealing").

is the end user's "right to gain access."[423] Being originators and users of data, particularly machine and technical data controlled through TPMs, data originators ought to be recognized as bearers of a new right of access to such data.[424] The various "right to repair" initiatives that are intended to allow technology users access to diagnostic and repair data ought to be expanded to enable them to access other datasets of which they are the originators.[425]

The basis for this recognition arises from the conceptualization of copyright as an access-right, the grant of which entails the obligation to secure access.[426] In such a conceptualization, the data originator's right to access data is required, first, to counterbalance the access-right, thereby fulfilling "[the] proper balance between protection and access."[427] This addresses the goal of copyright law—affirmed by Canada's Supreme Court—of promoting the "progress of science and useful arts," as accepted in the United States.[428] Given that copyright exceptions are often overridden through contracts—for example, exemptions granted by the Library of Congress to circumvent TPMs for repair[429]—a legal framework is required that will entitle technology users to access data through mandatory rules. Such rules should be structured in a way that overrides any contractual clause to the contrary. Second, users' right to access machine and technical data, which are often locked under proprietary software and controlled through TPMs, is justified because technology users are the very source of such data. Given that technical and machine data are raw data and therefore do not attract copyright in most circumstances, there is no justification for TPs to exclusively "own" these data through an access-right and enjoy exclusive benefits.

---

423. See Marcella Favale, *The Right of Access in Digital Copyright: Right of the Owner or Right of the User*, 15 J. WORLD INTELL. PROP. 1, 1–2, 20 n.62 (2012).

424. For a similar argument, see Ian R. Kerr et al., *supra* note 314, at 47–49, 78 (arguing that TPMs should be "counter-balanced by a newly introduced access-to-a-work right").

425. *See supra* notes 322–25 and accompanying text.

426. For a conceptualization of copyright as an access right, see Christophe Geiger, *Copyright as an Access Right: Securing Cultural Participation Through the Protection of Creators' Interests*, *in* WHAT IF WE COULD REIMAGINE COPYRIGHT? 73, 79–80 (Rebecca Giblin & Kimberlee Weatherall eds., 2017).

427. Soc'y of Composers, Authors & Music Publishers v. Bell Can., [2012] 2 S.C.R. 326, para. 11 (Can.).

428. For a brief discussion on how the Progress Clause confers cultural benefits to society (and not solely rights to creators), see Geiger, *supra* note 427, at 83, and Margaret Chon, *Postmodern "Progress": Reconsidering the Copyright and Patent Power*, 43 DEPAUL L. REV. 97, 135 (1993) (arguing that "access to knowledge might be a fundamental civil right").

429. *See* LUCIE M.C.R. GUIBAULT, COPYRIGHT LIMITATIONS AND CONTRACTS: AN ANALYSIS OF THE CONTRACTUAL OVERRIDABILITY OF LIMITATIONS ON COPYRIGHT 243 (2002).

VIII. CONCLUSION AND FUTURE INQUIRY

There is significant enthusiasm surrounding the big data phenomenon given its potential to realize gains by applying precision technologies that combine advanced technologies (for example, IoT) with AI-based data analytics. However, there is some concern that these gains might not be fairly distributed across users, TPs, data intermediaries, and data platforms. The prevailing legal regime enables actors in the upper echelon of the user data ecosystem to retain exclusive and de facto control over access to various forms of user data.[430] A *sui generis* law inspired by copyright addresses the distributional concerns associated with the different applications of big data, such as in agriculture, by empowering technology users to appropriate a fair share of the gains of digital technologies through access to and control over data.

This Article has explored the various legal regimes relevant to accessing and controlling user data in an evolving digital landscape. It has demonstrated the inadequacy of current law and existing mechanisms for ensuring technology users' access to and control over data. It has also identified trends in which TPs, data intermediaries, and data platforms exercise ownership and control of user data to the prejudice of data originators, such as farmers. Without legislation that clarifies ownership and control through the equitable governance of user data, these trends risk widening the inequality gap and may result in the loss of technology users' autonomy.

The potential of the big data phenomenon could be realized through a data-governance mechanism that encourages users to share data with technology providers through a relationship of trust and transparency. This mechanism recognizes the need for originators to have clarity regarding access to and control of their data while simultaneously enabling data integration to provide actionable and usable knowledge across the user data ecosystem. While the exchange of data for such uses, as actionable on-farm and off-farm decisions, is facilitated through proper data sharing, data originators such as farmers need assurances as to who will have access to the data and how it will be used. This consequently guarantees that the benefits of access to and use of data are shared. This Article has argued that an ownership framework for data access and control under copyright consolidates the power of data collectors, processors, and aggregators. The prevailing mechanism of data access and control through contracts also has the same effect.

---

430. *See, e.g.*, discussion *supra* Section V.A.

Given that contractual entitlements to data are often reinforced and maintained through legal and technical forms of control under copyright, this Article proposes that the appropriate protection of farmers' access to and control over data can be accomplished through *sui generis* legislation modeled on copyright law. Copyright law provides an appropriate normative basis for recognizing data originators' privacy interest regarding user data in its recognition of authors' claims to their work, where this work has a confidential and private nature and is revelatory of the author's identity.

This Article substantiates the need for access and control over user data, to a large extent, based on an example of agricultural data. Given the multidimensional and pervasive application of big data technologies across diverse sectors, an outstanding issue remains to be explored. That issue is whether the initiatives and mechanisms for ensuring access to and control over technology users' data (i) adopt a sector-specific approach that focuses on context-specific areas to which datafication brings unique challenges, or (ii) treat the users' data as part of the interconnected domain of the economy.

In recent discourse, the question of access to and control over data is seen as part of a broader inquiry into the new political economy trend, described in such expressions as the "data-driven economy,"[431] "informational capitalism,"[432] and "surveillance capitalism."[433] In these settings, data constitutes the essential capital asset of the global economy. However, agricultural data comprises a unique data category that warrants consideration of a type different from, for example, social media users' data about which recent data-governance proposals have proliferated.[434] Unlike most other data categories, agricultural data is actively utilized in farmers' day-to-day activities, such as in the planning of farm tasks, farm monitoring, events management, automation of farm services, and forecasting of agricultural production.[435] Farmers require access to data in their role as decision-

431. *See* Tilman Becker, Edward Curry, Anja Jentzsch & Walter Palmetshofer, *New Horizons for a Data-Driven Economy: Roadmaps and Action Plans for Technology, Businesses, Policy, and Society*, *in* NEW HORIZONS FOR A DATA-DRIVEN ECONOMY: A ROADMAP FOR USAGE AND EXPLOITATION OF BIG DATA IN EUROPE 277, 278 (José María Cavanillas, Edward Curry & Wolfgang Wahlster eds., 2016).

432. COHEN, *supra* note 155, at 89.

433. *See, e.g.*, SHOSHANA ZUBOFF: THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 52–54 (2019) (assessing the wide-ranging impact of the technological revolution on human liberties).

434. *See, e.g.*, Balkin, *supra* note 130, at 15–16; Haupt, *supra* note 136, at 40; *infra* text accompanying notes 436–39.

435. *See supra* Part III and text accompanying notes 77–80. In some cases, social media data may be used by social media stars who make their living off their posts. *See* Emily D. Hund,

makers on their farms.[436] In addition to using data in the operation, management, and structure of farms, farmers utilize agricultural data to participate in the agricultural value chain, including in the marketing of their products.[437] Moreover, the harm that disclosure of agricultural data to third parties can cause farmers goes beyond interests that privacy torts traditionally compensate—such as those related to autonomy and dignity—by including economic harms. In the US Poultry industry case mentioned above, for example, Agri Stat's disclosure of agricultural data to third parties resulted in lower wages for farmers and increased prices.[438]

Thus, agricultural data has unique significance as an economic good. In this context, insofar as agricultural data is closely interlinked with a farmer's land, such as agronomic data collected using AI sensors, it would seem reasonable that the property interest in the land extends to the data. Even in such scenarios, the data would be a subject of property interest independent of the land. However, proposals to recognize data as property in this manner have faced criticism because of the limits of property rules in accommodating data ownership.[439] In this connection between data and property, it is necessary to inquire whether the instrumentalization of copyright in the manner proposed in this Article forms part of the so-called "new" materialist movement

---

The Influencer Industry: Constructing and Commodifying Authenticity on Social Media 60 (2019) (Ph.D. dissertation, University of Pennsylvania) (ScholarlyCommons). Such stars frequently utilize this data to make decisions about their posts. *Id*. at 62–63. To this extent, the analysis about access to agricultural data may apply to social media and platform data. *Cf.* Balkin, *supra* note 129, at 12 (identifying informational asymmetries between social media platforms and consumers).

436. *See* KEITH COBLE, TERRY GRIFFIN, MARY AHEARN, SHANNON FERRELL, JONATHAN MCFADDEN, STEVE SONKA & JOHN FULTON, COUNCIL ON FOOD, AGRIC. & RES. ECON., ADVANCING U.S. AGRICULTURAL COMPETITIVENESS WITH BIG DATA AND AGRICULTURAL ECONOMIC MARKET INFORMATION, ANALYSIS, AND RESEARCH 7 (2016), https://www.mssoy.org/uploads/files/big-data-cfare-nov-2016.pdf [https://perma.cc/8LFU-KH3H].

437. *See* Wolfert et al., *supra* note 271, at 74.

438. *See supra* notes 109–16 and accompanying text; Leah Douglas & Christopher Leonard, *Is the US Chicken Industry Cheating Its Farmers?*, GUARDIAN (Aug. 2, 2019, 12:21 PM), https://www.theguardian.com/environment/2019/aug/03/is-the-us-chicken-industry-cheating-its-farmers [https://perma.cc/M4XY-W9WC].

439. *See* Jorge L. Contreras, *The False Promise of Health Data Ownership*, 94 N.Y.U. L. REV. 624, 660–61 (2019) (criticizing property ownership of data in the context of health care as creating prohibitive costs and administrative complexities); Peter K. Yu, *Data Producer's Right and the Protection of Machine-Generated Data*, 93 TUL. L. REV. 859, 926 (2018) (critiquing the EU's proposed "data producer's right" for generating complications in the law and policy arena); HUGENHOLTZ, *supra* note 307, at 2 (arguing that the introduction of the data producer's right would "contravene fundamental freedoms" established by the European Convention on Human Rights); Ignacio Cofone, *Beyond Data Ownership,* 43 CARDOZO L. REV. 501, 539–40 (2021); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1301 (2000).

in intellectual property.[440] This movement seeks to highlight "the qualities and characteristics originating from non-human actors [*sic*] such that, 'the scope of original expression beyond that which originates with a human contributor, might result in an expanded incidence of authorship.'"[441] If so, the analysis in this Article in the context of agricultural data has implications for other areas, for example, areas in which datafication of the agricultural land might be seen as an equivalent to the "dematerialization" of genetic resources through digital sequence information technologies.[442] In short, the multifaceted nature of big data's applications draws convergences and interconnections between different norms and regimes concerning access to and control over data, which ought to be further explored to properly reconcile conflicting interests of individuals, social groups, companies, and countries.

440. Dan L. Burk, *Copyright and the New Materialism*, *in* INTELLECTUAL PROPERTY AND ACCESS TO IM/MATERIAL GOODS 61 (Jessica C. Lai & Antoinette Maget Dominicé eds., 2016).

441. *Id.*

442. *Cf.* Julie E. Cohen, *Property and the Construction of the Information Economy: A Neo-Polanyian Ontology*, *in* ROUTLEDGE HANDBOOK OF DIGITAL MEDIA AND COMMUNICATION 338 (Leah A. Lievrouw & Brian D. Loader eds., 2021) (observing that profit extraction in the information economy requires the reconstruction of land as "dematerialized" and "informationalized" data). In this context, "dematerialization" refers to the separation of data associated with a genetic resource from its physical substrate, usually in the form of digital sequence information (DSI). *See* Mark Lycett, *'Datafication': Making Sense of (Big) Data in a Complex World*, 22 EUR. J. INFO. SYS. 381, 382 (2013); *see also* Executive Secretary of the Convention on Biological Diversity (CBD), *Digital Sequence Information on Genetic Resources: Concept, Scope and Current Use*, at 2, U.N. Doc. CBD/DSI/AHTEG/2020/1/3 (Mar. 20, 2020) (illustrating further the scope of DSI).