Statement of Jeffrey Ritter

Founding Chair of the American Bar Association Committee on Cyberspace Law; External Lecturer at University of Oxford, Department of Computer Science (on research sabbatical)

United States Senate
Committee on Banking, Housing, and Urban Affairs
October 24, 2019
Hearing on "Data Ownership: Exploring Implications for Data Privacy Rights and Data Valuation"

Good morning Chairman Crapo, Ranking Member Brown, and members of the Committee. Thank you for the opportunity to join you, speaking in my role as an active contributor for over 30 years to law reforms enabling US and global electronic commerce. The time is long overdue for comprehensive privacy reform legislation. For now, we just seem to have been relegated to playing 'catch-up' with the EU and other nations that have embraced their rules; we are trying merely to weave together our piecemeal laws into some type of whole cloth.

Privacy law reform here will surely fail if we do not incorporate something new—a legal answer to the most fundamental question: who owns digital information? For the totality of digital information, this is an enormous chasm in the evolution of the rule of law for the Digital Age. For personally identifiable information, the question is particularly relevant. Yes, it is identifiable, but who owns it?

In many steps to advance electronic commerce, the United States has led the world, notably enabling electronic contracts and electronic signatures to be legally valid without paper. Indeed, in humankind's history, no rule of law was more rapidly incorporated into the laws of the world than the rules we helped innovate to enable digital commerce to become real. But, in privacy, we are behind.

To re-establish this nation's leadership, privacy reform must express clear, explicit rules that establish who owns any specific digital file or record. Only then can we be successful in crafting the additional rules for

acquiring, using, transferring, selling, and controlling personal data, and imposing the sanctions for violating those rules.

Think about it. Every commercial system built on the rule of law—real estate, banking, consumer and industrial products, mining—begins with a commitment to define and protect the rights of the owner of the property. Yet, across all privacy law, while a data subject has many controls on the use of identifiable information, and we often speak in conversation about ownership, the legal right of ownership has not been established.

As summarized in a recent article submitted as part of my written testimony, Germany, Japan, and the OECD are all calling for formal legal rules on data ownership, including from Chancellor Merkel herself. Japan has already published model guidelines for structuring data sharing and licensing agreements based on ownership principles. Failing to address data ownership in our privacy reforms will surely further isolate the United States from the global momentum and allow the rules for data as property to be written by others.

The solutions on how to craft this legal concept are already part of Federal law, within the laws governing electronic transferable records[1] and, at the global level, in recently finalized UN model laws[2] authored with substantial US input and influence. There, the rights of ownership are exercised by establishing and maintaining "control" over the digital file. Realistically, the first owner of personal data will be the business entity with which a data subject is engaged—a bank, a broker, a hospital, a university. Their systems create the control over the personal data. But recognizing data ownership should do nothing to remove or

---

1 15 U.S. Code §7021. Transferable Records. The statute enables a person "in control" of a qualifying electronic transferable record to act as a *holder* under the Uniform Commercial Code, able to exercise the rights and defenses of a holder in due course or purchaser (i.e., acting as the owner of that record).

[2] UNCITRAL Model Law on Electronic Transferable Records (2017), available at https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records.

diminish a data subject's rights and controls—indeed, if ownership is clear, accountability for violating those controls can be more readily enforced. As more fully explained in my written testimony, writing these rules should not disrupt any of our existing Federal laws for protecting personal information, including those governing our financial systems.

As to valuation, there is an essential truth: The accurate valuation of any asset in commerce begins with a calculation of the certainty of ownership. Any calculation of the economic value of personal information will be inherently inaccurate if ownership and the related rights are not certain. The new California privacy law has attempted to address valuation but its silence on ownership fatally handicaps that effort.

Privacy law reform to merely play catch-up with the EU will not be enough. To seize the opportunity, the US must address and define ownership rights in personal information. This will move the US ahead in providing a more stable, predictable legal environment in which the value of personal information can be more fairly calculated, the rights of data subjects more readily enforced, and commercial innovation built around personal information can thrive.

I will defer to my submitted written testimony for my responses on other topics the Committee invited me to address. Thank you.

***

Supporting Additional Testimony

In support of my oral testimony today, the following is offered to expand upon several of the topics introduced and to provide further substantive material for the Committee.

Background Perspective

Since 1988, I have been actively engaged in identifying legal barriers to electronic commercial practices, eliminating those barriers, and crafting the rules that would enable the legal validity and expansion of those practices. Most notable was my work as the founding chair of the American Bar Association, Section of Business Law, Committee on Cyberspace Law and my active service, on behalf of the United States, in the United Nations' varied programs that produced a foundation for global digital trade.

At the UN, I served as a co-rapporteur on legal questions for the UN Economic Commission for Europe Working Party on the Facilitation of International Trade Procedures.[3] In that role, I led efforts that ultimately involved more than 80 nations and non-governmental nations in formulating legal solutions to advance electronic commerce. I also participated extensively in the activities of the United Nations Commission on International Trade Law (UNCITRAL)[4] and the United Nations Conference on Trade and Development (UNCTAD)[5], and, in 1997, had the opportunity to contribute to "A Framework for Global Electronic Commerce" strategic plan of the United States.[6]

"Electronic information—data—is emerging worldwide as a fundamentally new species of property. Data is being created, manipulated, stolen, bought, sold, leased, stored and transported in transactions for which our existing laws . . . no longer provide easy accommodation." This statement was published in July 1993 as part of the Mission Statement for The DataLaw Report, for which I served as co-founder and editor-in-chief (copy attached as Annex A). The first issue's lead article addressed privacy rights of employees in the workplace. Even earlier, beginning in 1989, through my UN work, I actively interacted with EU representatives on privacy issues, for which they lobbied to align international work products with the EU's privacy laws.

In the last decade, I have continued to engage on these topics, crafting at Johns Hopkins University, Whiting School of Engineering a graduate course on "Privacy Engineering", as well as teaching at the University of Oxford, Department of Computer Science a course titled "Building Information Governance." My most recent book, Achieving Digital Trust: The New Rules for Business at the Speed of Light, was used as the text for that course and has been adopted at other universities. A full c.v. has been previously submitted to the Committee staff.

Regulating Data as Property: A New Construct for Moving Forward

In late 2018, the Duke Law & Technology Review published an article I co-authored with a research assistant, Anna Mayer, "Regulating Data as Property: A New Construct for Moving Forward" (copy attached as Annex B)[7]. While the analysis focuses on personal information and privacy law, the overall scope is broader and introduces a new classification scheme to better enable incorporating ownership rights into the larger legal structures already in existence (see A New Concept for Classifying Digital Information below).

The article presents in substantial detail the following elements referenced in my oral statement:

- The policy statements of Germany, Japan (through METI), and the OECD on data ownership as a key priority for enabling innovation in commerce.

[3] The work products of that group are now incorporated into the work of the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT). See https://www.unece.org/cefact.html.
[4] Key work products of UNCITRAL that were produced or initiated during the tenure of my work included the UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures, each of which are available at https://uncitral.un.org/en/texts/ecommerce.
[5] In addition to authoring for UNCTAD a special report on the legal facilitation of electronic commerce for developing nations, I had the privilege of helping secure and host in Columbus, Ohio a meeting of the United Nations which produced the Columbus Ministerial Declaration on Trade Efficiency, available at http://sunsite.icm.edu.pl/untpdc/tei/columbus.html.
[6] Available at https://clintonwhitehouse4.archives.gov/WH/New/Commerce/.
[7] 16 Duke Law & Technology Review 220-277 (2018), available at https://scholarship.law.duke.edu/vol16/iss1/7.

- A summary of international privacy law, to the extent available to us in the English language (or translations), notably the conclusion that no formal law addresses ownership of personally identifiable information.
- The relevant provisions of the Uniform Commercial Code and Federal law, as well as the United Nation work product, that serve as a model for how to structure the definition of ownership and adapt concepts of "control" toward creating the legal formalities for defining the ownership of data.

Our analysis also examined several additional points of possible interest to the Committee:

- Recognition that, as a matter of consensus in the scientific community, information (including digitally recorded information) is best considered as a physical asset, rather than treatment as an "intangible" thing.
- An analysis of how US Copyright law and the EU Database Directive have failed to deal with digital information ownership rights, and their inadequacy in doing so.
- A survey of the advocacy relating to the automotive industry (outside the United States) calling for clear, certain rules for data ownership.

A New Concept for Classifying Digital Information

The current portfolio of laws protecting information is awkwardly suited to enabling better expressions of ownership rights in digital information. For too long, we have tried to "fit" the realities and trends of digital commerce into legal structures that were written before computers and the Digital Age were considered. Notably, both in the US and the EU, adjustments to copyright law have been ineffective and inconsistent. The article offers a new classification scheme:

- Factual Data, which can be either
    - Personal Information (or Personally Identifiable Information), or
    - Industrial Data (everything else that is factual)
- Fictional Data.

This scheme enables the following immediate benefits to advancing data ownership principles:

- By separating Factual Data from Fictional Data, copyright laws (which were intended to protect Fictional Data) can be revised, providing more robust and focused protection for both classes.
- Personal Information can itself be given appropriate rulesets which enable both ownership and data subject rights and controls.
- Industrial Data can also be given dedicated, appropriate rulesets that address ownership, and also better advance the data sharing, data analytics, distributed systems, and other innovations which exist and will continue to evolve.

Who is the First Owner of Personal Information?

As mentioned in my oral statement, a data subject is ***not*** likely to be the first owner of personal information identifiable to that individual. Yes, the data is personal, possibly intensely personal, but the primary reason a record of that information is being created is to enable effective transactions between the individual and another entity—a retail store, a hospital providing medical care, a financial institution servicing an account, a broker managing investments, an airline transporting passengers or shipments.

Any of those entities are investing enormous amounts in their systems to gather, store, analyze and use the data to deliver the primary services. Legitimately, as the data creators, they have always felt they "owned" the data, and the emergence of privacy concerns was not driven by their entitled sense of ownership but by another far more substantive force.

What commerce, industry, and governments as a whole did not appreciate, as those systems were being developed, were the powerful, dynamic manners in which any data, once gathered, could find secondary uses and secondary, downstream markets, when aggregated, analyzed, parsed, and combined with other data sources. As networking, data standards, high-speed communications, and computational power have evolved, new ways were created in which data, once shared, could transform a company's revenue, productivity, and quality of services.

These capabilities are what shifted the momentum of concern regarding privacy—once data began to be a functional commodity to be shared, the privacy of the data subject became vulnerable. Yet, while the last 30 years have seen evolutions in the rights of a data subject to control those sharings and uses, the issue of ownership has never been formalized into any legal structure.

It is my view that the original point of recordation of information—whether on a phone, a device, or a server—is the starting point where ownership can be asserted, through the exercise of "control" as more expansively explained in the article (Annex B). For personal information, this is also where the negotiation between a data subject and the owner regarding how the personal data can be used (and the rules and controls required) is best placed.

Here is an example:

> A new automobile in 2019 is basically a data collection tool also operating to provide transportation. Within the machine, there are dozens of sensors that not only monitor geographic location, speed, and operator behavior, but also continually measure and report on performance of the functional components. Unless the driver has uniquely 'logged in' with a unique ID (such as a biometric sensor panel), the vehicle knows nothing about the identity of the actual driver (i.e., it is Industrial Data). Yet all of that data is intensely valuable to the manufacturer, component suppliers, public authorities managing traffic flow patterns, and many others.

But who owns the data as the vehicle drives off a dealer's lot? The component suppliers? The software developer whose software is installed in those components? The manufacturer? The captive leasing company that has leased the vehicle to a new driver? Perhaps the driver has elected to retain the data all to themselves! Indeed, going forward, in an Internet of Things (IoT)world, virtually every product is two things: a service provider and a data collection and communication device. *Nearly ubiquitous surveillance is advancing; who owns the data streams?*

It is easy to imagine that the dealer may offer the driver two prices: one price is for a vehicle with no data-sharing services; the second, at a lower price (taking account of the downstream economic value of the data), allows the data sharing. A third, at an even lower price, may be tied to matching the Industrial Data to related Personal Data (such as the identity of individual drivers) and, in that instance, negotiating the controls on secondary, downstream transfers and uses of the personal data.

Today, however, many consumer IoT devices offer no such negotiation and the existing privacy laws do nothing to produce meaningful descriptions of the transactions (and revenues) the device manufacturer

realizes under the "consent" given by the purchaser. But the manufacturer, in nearly every instance, is acting as the de facto owner of the collected data.

Why not provide legal certainty to that situation? Doing so makes the negotiation of the rights and controls far easier to accomplish. The economic valuation of the data can be more easily incorporated into the negotiation—perhaps even as a separate item for which different data subjects may be induced to pay greater or less value for the device itself.

Data Ownership and Existing Federal Laws (Privacy in Financial Systems)

Data ownership must be addressed at a global level, allowing concise, known rules for determining who owns a specific data asset to be understood and applied irrespective of the geographic location of the participants. We have achieved that certainty for physical goods[8]; doing so for digital information is imperative. Ideally, the law reforms required would address both Industrial Data and Personal Data, as well as include adjustments to copyright laws where the distinctions between Fictional Data and Factual Data have been muddled by previous enactments (such as the Digital Millennium Copyright Act).

But a useful and constructive step in the right direction is to establish a doctrine of ownership for personal information. As part of the privacy reform this nation is contemplating, it is critical that we abandon industry-specific sectoral solutions (like Gramm-Leach-Bliley Act, Fair Credit Reporting Act, and the Health Insurance Portability and Accountability Act) and embrace an omnibus model similar to the EU's GDPR and related rules and regulations. In doing so, substantial alignments must be made, but adding data ownership rules into that alignment process should do little to disrupt the reforms of existing rules in order to be responsive to the greater expressions of rights and controls sought be data subjects.

Data Ownership and California Privacy Law

While privacy advocates may applaud the new rules in California[9], defaulting to the enactment of privacy law reforms by individual states is in fundamental conflict with the trends and practices of international, global commerce, as well as the integrity and fluidity of interstate commerce in the United States. Privacy is a topic on which uniformity is incredibly important; that demand is one reason why the GDPR rules from the European Union have been so readily adopted more broadly across global trade. It is simply the nature of computing to seek uniform, standardized rules.[10]

As briefly noted in my oral statement, the California law does take an affirmative step toward improving the economic valuation of data, and moving calculations of value into the transactions between a data subject and data collector.[11] But the law is silent on ownership. Having not been involved in the drafting or negotiation of the CCPA, I have no insight into that outcome. It is an opportunity missed, though I strongly believe a uniform Federal solution is to be preferred.

---

[8] *See* The United Nations Convention on Contracts for the International Sale of Goods, available at https://www.uncitral.org/pdf/english/texts/sales/cisg/V1056997-CISG-e-book.pdf.

[9] California Consumer Privacy Act of 2018, Cal. Civ. Code Section 1798.100-1798.199) ('CCPA').

[10] In turn, these influence our business practices. For example, the invitation from the Committee for my testimony instructed that this testimony be submitted in a single format-Microsoft Word.

[11] See Cal. Civ. Code Section 1798.125(b) and Article 6 of the Proposed Regulations, available at https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf.

Data Ownership and Data Valuation

The accurate valuation of any asset in commerce begins with a calculation of the certainty of ownership. When there is uncertainty as to ownership, any negotiated value will be lower. Yet, for personal data, the absence of any defined mechanism for establishing ownership inherently reduces valuation, and makes any calculation of value difficult to execute with any accuracy.

There can be little disagreement that the vast collections of digital personal data already built during the last 40 years have been collected with no explicit awareness of ownership nor valuation, at least at the point of collection. In the downstream, secondary marketplace in which personal data is the asset of the transactions, various valuation mechanisms have developed. However, none of them are particularly effective because, since ownership cannot be legally verified, all transaction participants carry some risks.

Those risks have several adverse impacts on the transactions. First, the valuations are going to be less, discounted by some economic expression of the value of those risks. Second, the transaction costs, particularly legal fees (and time) incurred to negotiate how the risks will be allocated, degrade the net present value of the transactions to the participants—even if the controlling party has strong confidence that the proposed use of the personal data in the transaction has been approved by the privacy consents of the related data subjects.

I have no particular competence to offer an opinion on the valuation methods to be used with personal data. But I do know that certainty of ownership will contribute to improved certainty in valuations, as well as eliminate risks, accelerate transaction velocity, and provide a substantive foundation for continued innovation in the use of personal information in the marketplace.

Personally, while I want to know what data is collected about me, I have few objections to a world in which our systems and devices do so. The results are more personalized, focused interactions: A hospital can more immediately, and accurately, deliver medical care; a financial institution can tailor cross-marketing more effectively and better protect my financial assets; and advertising, whether as online banners or in direct marketing, is more focused to my interests and needs.

Personal data has become a new kind of asset for which, as a data subject, I want to have controls on its use and be more fairly compensated for the value that data provides to the collecting entity with which I am engaging. Understanding who owns that data will make those transactions more functional and useful across our economy and our global systems.

Data Ownership and Digital Trust

Writ large, privacy law serves to secure the trust of data subjects with the collection and use of their personally identifiable information. As discussed at length in my most recent book, Achieving Digital Trust, trust is not an emotion, but the result of complex calculations in which we identify the rules we expect to govern particular transactions and evaluate the quality with which those rules are executed. When suitable rules do not exist, or existing rules are not executed, our determinations to trust are impaired or, in the worst case, impossible to calculate.

For privacy, the rules and regulations expressed in formal public law are the first step; however, effective execution of those rules requires policies, procedures, terms of use, and contractual agreements to be

authored, implemented, and capable of enforcement, whether by the transaction participants, self-regulatory organizations, or public authorities.

In addition, all of those rules must be mapped into software code and applications, capable of being executed automatically and also capable of keeping logs of their due execution to provide adequate proof of compliance with all of the rules. Collectively, there are a lot of rules, and each rule is an opportunity for risk when that rule is ignored, not properly implemented, or not supported by proper records of the due execution of those rules.

The inventory of the rules for privacy, on a global level, is complex. Billions of dollars are spent trying to build systems and processes that are in compliance.[12] The situation is the more difficult when an organization's operations or customer assets cross multiple boundaries and thereby invoke different rules applicable to defined subsets of information. This is another functional reason why companies rightfully should seek a Federal solution versus state-by-state privacy reforms.

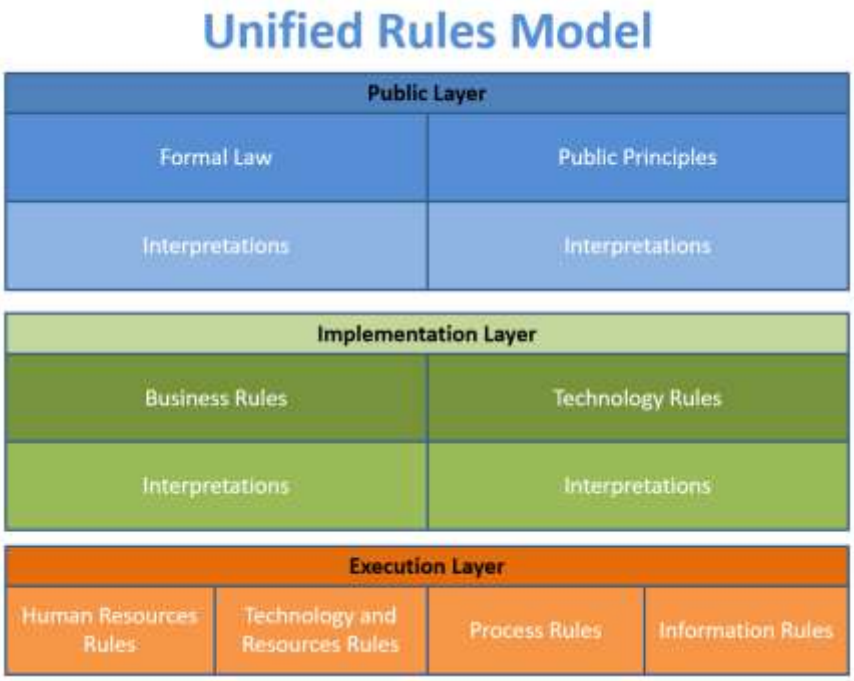
"Privacy by design" is an important concept. In its essence, it advocates creating a full inventory of the applicable rules *before* responsive systems and processes are constructed, thereby dramatically improving the probability all of those rules are being satisfied. The result is intended to be greater trust, calculated because of the knowledge that a specific system has been well-designed to the rules.

The metaphor to a residential home or commercial building is easy to imagine—who could build any such structure without first accounting for, and providing evidence of compliance to the relevant building authority prior to occupancy for, all of the building code rules?

I believe the key principles of rules-based design should not be limited merely to systems managing or interacting with personal data; the principles should be expanded to all systems. I similarly advocate that data ownership should be clear with respect to all types of data. But the overall task of organizing and assembling those rules into a unified, coherent inventory will be challenging. Moreover, different governance models (i.e., common law, civil law, authoritarian law) strike different balances among the various rule types, particularly with regard to how much flexibility private sector actors have in authoring the non-public rules (policies, procedures, terms of use, privacy notices, etc.) that still must be present for trusted services to be delivered.

To provide structure to these tasks, one tool that may be helpful as the Committee analyzes how to proceed, is the Unified Rules Model—a visual tool for classifying and organizing the rules required to engineer improved compliance and governance of any system, application, or device.

[12] A new report prepared for the California state attorney general by an independent economic research firm projects initial compliance costs with the new CCPA may be as much as $55 billion. https://www.cpomagazine.com/data-protection/new-report-suggests-initial-compliance-costs-for-ccpa-could-reach-55-billion/.



The detailed classifications and uses of the Unified Rules Model are described in detail in Achieving Digital Trust (a hard copy of which has been provided as Annex C to Committee staff in support of this written testimony).

****

Please feel free to contact me with any further questions relating to my testimony at jeffrey@jeffreyritter.com, jeffreyritter54@gmail.com, or 202.285.7385.

The DataLaw Report

Analyzing the changing global legal environment for electronic information

Vol. 1, No. 1 July 1993

Employers' Access To Employee E-Mail

E-Mail Privacy Versus Corporate Privilege

More and more companies are implementing electronic mail systems to improve and expedite internal and external communications. E-mail is beginning to rival the telephone as a means of conducting business: organizations implementing E-mail find that it "flattens the management hierarchy, improves project tracking, and speeds time to market for new products or services." A. Reinhardt, *Smarter E-Mail is Coming*, BYTE vol. 18, no. 3, p. 90 (March 1993). One estimate is that the number of LAN E-mail users in the United States rose 60 percent last year, will climb another 60 percent this year to 15.1 million users, and will be up to 38 million in 1995. Meanwhile, the number of messages transmitted within Fortune 2000 firms in North America will surge from 6.1 billion in 1993 to 14.3 billion in 1995. Id., citing research by the Yankee Group (Boston, Mass.), and the Electronic Mail Association (Arlington, Va.).

The increased use of electronic mail in commercial practice has led to increased concerns about the privacy rights of the users of such systems, and the rights of employers to gain access to E-mail transmissions. Several recent controversies have highlighted the dilemmas facing employers and employees when electronic messaging technologies are used.

In 1992 a software vendor, Borland International, Inc., found E-mail evidence that a former employee, Eugene Wang, had transmitted confidential business information to a rival company, Symantec Corp., via

(Continued on page 7)

IN THIS ISSUE:

Published by CLARK BOARDMAN CALLAGHAN • 155 Pfingsten Road • Deerfield, Illinois 60015

The Negligent Operation of Electronic Networks

Judicial Standards of Accountability

The movement of information has always been an essential aspect of commerce. Information must be communicated in the course of every commercial transaction. With the advancement of technology, the ability to send and receive information electronically has created the opportunity for companies to increase their portfolio of activities to include the business of sending and receiving information, both for themselves and as a service provider to third parties. Initially with electronic mail, and now with electronic data interchange (EDI), the business of sending, receiving, storing and processing information in the course of conducting business has become a separate and viable enterprise, introducing into commerce a new class of commercial player—the value-added network or VAN.

The Role of Value-Added Networks

There is no question that networks have become indispensable to the current and foreseeable expansion of electronic commerce. Much as we have developed an integrated, multi-modal, global network for the physical transport of goods, so have the individual networks become the essential components of an integrated framework for the advancement of electronic commerce. Even with the exist-

(Continued on page 11)

The DataLaw Report Mission Statement

The DataLaw Report exists to provide a means for reporting upon and analyzing the changing global legal environment for electronic information. Electronic information—data—is emerging worldwide as a fundamentally new species of property. Data is being created, manipulated, stolen, bought, sold, leased, stored and transported in transactions for which our existing laws, set forth in the diverse legal systems of an emerging global economy, no longer provide easy accommodation. Electronic information has become something deserving of its own rules, and it is now apparent that the law will be responsive.

By giving focus to both new and divergent areas of law, **The DataLaw Report** will become an essential tool for enabling companies, their attorneys and other information professionals to learn and master the new rules of the game.

Korea Requires Electronic Commerce

New Law Requires EDI for International Trade Documents

There remains little question that implementing EDI yields competitive advantage for those first to recognize its potential for efficiency, accuracy and speed. Korea has become the first nation to promote the automation of the exchange of commercial and administrative documents through national legislation, the Act on Promotion of Trade Business Automation (Law No. 4479, Dec. 31, 1991). The legislation is a revealing work, demonstrating unequivocally the prospects for further national policy-making by other countries and regions.

The Ministry of Trade and Industry (MTI) promoted the Act in order to accelerate the establishment of a paperless trading system. According to documents in English provided to the United Nations by the Korea EDIFACT Center, the goal is to establish the ability of trading companies and trade-related administrative bodies to electronically exchange information normally moved by traditional paper documents. The scope of the Act is impressive; MTI includes on its agenda trade administration, customs, banking, insurance and transport activities. It is hoped that pursuit of automation in these areas will improve the competitiveness of local trading companies in the international

(Continued on page 14)

REGULATING DATA AS PROPERTY: A NEW CONSTRUCT FOR MOVING FORWARD

JEFFREY RITTER AND ANNA MAYER [†]

ABSTRACT

The global community urgently needs precise, clear rules that define ownership of data and express the attendant rights to license, transfer, use, modify, and destroy digital information assets. In response, this article proposes a new approach for regulating data as an entirely new class of property.

Recently, European and Asian public officials and industries have called for data ownership principles to be developed, above and beyond current privacy and data protection laws. In addition, official policy guidances and legal proposals have been published that offer to accelerate realization of a property rights structure for digital information. But how can ownership of digital information be achieved? How can those rights be transferred and enforced?

Those calls for data ownership emphasize the impact of ownership on the automotive industry and the vast quantities of operational data which smart automobiles and self-driving vehicles will produce. We looked at how, if at all, the issue was being considered in consumer-facing statements addressing the data being collected by their vehicles.

To formulate our proposal, we also considered continued advances in scientific research, quantum mechanics, and quantum computing which confirm that information in any digital or electronic medium is, and always has been, physical, tangible matter. Yet, to date, data regulation has sought to adapt legal constructs for "intangible" intellectual property or to express a series of permissions and constraints tied to specific classifications of data (such as personally identifiable information).

[†] Jeffrey Ritter, J.D. is a Visiting Fellow at Kellogg College, University of Oxford, where he is researching and writing on the first principles of quantum law. He is an External Lecturer at Oxford, teaching in the Department of Computer Science, and also teaches Privacy Engineering at Johns Hopkins University, Whiting School of Engineering. Anna Mayer is a graduate student at the Institute of Political Science, University of Vienna, M.A. expected 2018. Anna Mayer is researching the concept of e-residency at the Ragnar Nurkse Institute of Governance and Innovation, Technical University Tallinn. A preliminary draft of this article was presented at MyData2017 in Tallinn, Estonia on August 30, 2017 and the additional input and comments from Triin Siil are greatly appreciated.

We examined legal reforms that were recently approved by the United Nations Commission on International Trade Law to enable transactions involving electronic transferable records, as well as prior reforms adopted in the United States Uniform Commercial Code and Federal law to enable similar transactions involving digital records that were, historically, physical assets (such as promissory notes or chattel paper).

Finally, we surveyed prior academic scholarship in the U.S. and Europe to determine if the physical attributes of digital data had been previously considered in the vigorous debates on how to regulate personal information or the extent, if at all, that the solutions developed for transferable records had been considered for larger classes of digital assets.

Based on the preceding, we propose that regulation of digital information assets, and clear concepts of ownership, can be built on existing legal constructs that have enabled electronic commercial practices. We propose a property rules construct that clearly defines a right to own digital information arises upon creation (whether by keystroke or machine), and suggest when and how that right attaches to specific data though the exercise of technological controls.

This construct will enable faster, better adaptations of new rules for the ever-evolving portfolio of data assets being created around the world. This approach will also create more predictable, scalable, and extensible mechanisms for regulating data and is consistent with, and may improve the exercise and enforcement of, rights regarding personal information. We conclude by highlighting existing technologies and their potential to support this construct and begin an inventory of the steps necessary to further proceed with this process.

INTRODUCTION

The rapid and accelerating development of data analytics, automated manufacturing, probability-based management practices, machine-based commodities trading, and other innovations is generating an entirely new global awareness of the economic value and functional utility of digital information. All of these industrial creations confirm that data has now become a new kind of property—an asset that is created, manufactured, processed, stored, transferred, licensed, sold, and stolen. Yet, on a global basis, there is no legal regulatory framework or model that

provides guidance on how transactions using data as an asset are to be constructed.[1] That void in the rule of law can no longer be overlooked.

Reforms in copyright law to address digital creative works and the continuing evolution of regulations for personal information are important. But these adaptations to the realities of our digital world are not sufficient; indeed, there is little question that the largest volumes of digital information that already exist, and continue to be created, have two distinctive features which make copyright and privacy law adaptations inadequate. First, these enormous data sets have nothing to do with the creative artistic assets that copyright laws serve to protect. The data are industrial in nature, generated by vast networks of sensors that observe and record the smallest units of entire global supply chains. Second, they have nothing to do with personally identifiable information. The data are functional to how machines, networks, systems, devices, and information interact with one another and perform against their defined objectives. Something more is needed, urgently.

In recent months, both in Europe and in Asia, public officials and industry organizations have been declaring a need for the ownership of data to be explicit and confirmed by legal instruments.[2] Once ownership is well-defined, then the attendant rights can be more precisely expressed—rights to access, license, transfer, modify, combine, edit, and delete data naturally flow from the control that ownership vests.[3] In addition, both existing and new types of transactions can be more formally expressed (e.g., licenses, sales, transfers, processing services, storage services, analytics, and more).

There is no question that these types of transactions are occurring already. The Worldwide Semiannual Big Data and Analytics Spending

---

[1] Electronic commercial practices have frequently faced legal hurdles as each new generation of technology places stress on the state of the rule of law that then exists. Model agreements and model laws, when developed and published, offer solutions on how those hurdles can be overcome. *See, e.g.*, MODEL FORM OF ELECTRONIC DATA INTERCHANGE TRADING PARTNER AGREEMENT AND COMMENTARY (Am. Bar Assoc., 1989); *Model Contracts for the Transfer of Personal Data to Third Countries*, EUR. COMM'N, http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm (last visited Nov. 7, 2017); *Sample Business Associate Agreement Provisions*, U.S. DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html (last visited Nov. 7, 2017) (providing samples for health information privacy); INTERMODAL INTERCHANGE EXEC. COMM., UNIFORM INTERMODAL INTERCHANGE AND FACILITIES ACCESS AGREEMENT (2018), *available at* http://uiia.org/assets/documents/newuiia-Home.pdf (providing samples for, among other items, electronic and non-electronic receipts for equipment interchange).

[2] *See infra* Part II.

[3] *See infra* Part V.

Guide from International Data Corporation estimates that big data and business analytics alone will create US$203 billion in annual revenues by 2020, with revenue growth from information-based products (data monetization) doubled by the end of 2017 for one third of the Fortune 500 companies.[4] But who owns the assets that are the focus of these deals?

This article offers a bold proposition: An explicit, legal mechanism to establish, claim and transfer property rights in data must be adopted. Doing so rapidly is essential to enable digital commerce to evolve while continuing to assure the enforcement of privacy and data protection rules and existing intellectual property law constructs.

The critical insight on which this proposition rests is the scientific consensus that digital information is not intangible, but is physical, tangible matter. Governance of data, including personal information, will best be achieved by leveraging existing legal systems that govern the ownership, use, and transactions of the other physical assets which are the assets of economies, commerce and wealth.

Sales transactions, licensing deals, joint ventures, downstream distributions and syndications of rights to access and use data, valuation for accounting and tax purposes—all of these are possible, and some are already occurring. But defining ownership to attach to physical data will provide the proper foundation on which the globalization and continued growth of digital markets can proceed. To fail to do so, and to continue to focus only on the regulation of personal information without addressing the critical need to define and enable ownership of *all* data, renders a major disservice to the potential of the Digital Age in which we now live to be achieved.

This paper proceeds as follows. First, to facilitate our analysis, Part I introduces and defines certain terms useful to analyzing data ownership. These terms present important elements for how to discuss the totality of digital information, beyond the boundaries of personal information that current public regulations emphasize. Part II reviews current policy statements supporting the call for data ownership, as well as proposed legal reforms and innovations in business practices involving the automotive industry in Europe and Asia. A summary of the current state of the law for industrial data also is presented, to highlight that clear principles of ownership for all types of data have not yet been adopted. In Part III, existing academic literature on the suitability of property rights systems for data is surveyed and two additional essential conclusions are presented.

---

[4] Gil Press, *6 Predictions for the $203 Billion Big Data Analytics Market*, FORBES (Jan. 20, 2017, 9:27 AM), https://www.forbes.com/sites/gilpress/2017/01/20/6-predictions-for-the-203-billion-big-data-analytics-market/#498daf472083.

Part IV introduces the scientific literature regarding the physical quality of information, which supports the essential conclusion that data is physical, tangible matter, no different in its essential attributes than any other physical property (for which humankind has developed robust, mature, and functional property right systems, such as those governing real property, commodities, or manufactured goods).

The paper concludes in Part V with our proposal on how to proceed forward to install a property rights legal foundation for data that can work globally and be scalable across the diversities of existing and future systems, nations, and data classifications. The proposal builds on the physical nature of digital information and leverages the model law that has recently been adopted at the United Nations for transferring control of electronic records with legal value, as well as predicate constructs adopted in the U.S. Uniform Commercial Code and Federal law. Additional next steps for moving the proposal forward into contractual and regulatory legal systems are suggested.

I. DEFINED TERMS

For the purposes of this article, the following terms will be used. These terms have been developed in order to facilitate the discussion presented. The definitions are not scientifically precise; rather, they are intended to focus the analysis and, hopefully, enable ongoing dialogue about the utility and application of a property rights legal foundation for data.

> *Data* means any information recorded by electronic or digital means and is retrievable, whether perceivable to a human or machine.[5]
>
> *Industrial data* means any data that is created, processed, stored, or used in commerce, including business-to-business transactions, and excludes any personal information. Manufacturing, production, transport, mining, shipping, aeronautical traffic, financial services, securities markets—these are representative examples of the sources and uses of industrial data.
>
> *Personal information* (or personally identifiable information, or "PII") means any information that may be identified with a data subject or individual person, whether or not formally defined as such by any applicable statute, regulation or other legal requirement. For our purposes, personal information includes, but is not limited to,

[5] *See infra* Part IV. This definition is an adaptation of the definition of "record" introduced into the Uniform Commercial Code to provide a technology-neutral word that would include both paper-based and digital information records. The adaptation adds including information that is perceivable by a machine, but which may not be sensible to humans.

"personally identifiable information" as such term--and similar terms--are defined in various statutes and public laws.[6]

Factual Data means any data that serves to describe as fact a condition, circumstance, event, transaction, attribute, or process, whether or not determined to be factually accurate. A very large amount of factual data is recorded in logs, describing events or transactions that have occurred within information systems (including extensions of those systems as distributed systems operating across Internet-based networks).

Fictional Data means any data that is intended to describe fictional conditions, circumstances, events, transactions, attributes, or processes. Examples include creative works such as poetry, novels, films, audio recordings, etc., that are the primary focus of global copyright laws. Fictional data also includes data that is offered as factual but demonstrated to not be factual in truth by a defined calculation process using probability mathematics.

---

[6] What information may be defined as personally identifiable information varies across international, national, and state laws. For example, the General Data Protection Regulation (GDPR) adopted by the European Parliament, which becomes effective in May, 2018, defines "personal data" to mean ". . . any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679. By contrast, the U.S. has no formal statutory definition; the Office of Management and Budget states in a memorandum directed to Federal agencies that

PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES: PREPARING FOR AND RESPONDING TO A BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (2017), https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf, at 8.

These terms serve several purposes. First, the list itself highlights that personal information is merely a subset of the data being created by humankind, our systems, and our machines. We contend that further regulation of personal information that fails to align to, and share a common foundation with, industrial data (which is factual data) and fictional data will exacerbate rather than improve the effectiveness of regulating how industry manages personal information and accommodates the rights and controls of data subjects.

Second, these terms do not embrace the existing structures of copyright laws which, responding to digital media and digital information, have been amended, construed by courts, and, ultimately, supplemented in some nations by explicit laws expressing the rights of those who create databases (and distinguishing those from copyright owners).[7]

Finally, the definitions present an explicit distinction between industrial data and personal information. Anonymization, pseudonymization, tokenization, filtering, masking, and similar techniques continue to evolve as "work-arounds" that limit the effectiveness of the rights of data subjects.[8] But once anonymization has served its purpose, the resulting data is truly functioning as industrial data. The distinctions in definitions will enable industrial data to be owned, transferred, and legally protected by distinct legal and commercial rules while also more fully achieving the goals of privacy and data protection laws to truly vest in data subjects meaningful control of their identifiable personal information.

II. CURRENT CALLS FOR DATA OWNERSHIP

This article was provoked by discussions in public media and conferences about the conflicts among legal systems regarding *ownership* of data and the impact of those conflicts in light of the GDPR.[9] One commentator noted, "Ownership of data, both personal and machine-

---

[7] As proposed *infra* Part V, the continued tension of trying to adapt copyright and trade secret laws to protect industrial data may be addressed by limiting copyright laws to fictional data (such as creative works—books, films, music, etc.) and revising trade secrets law and the new proposed structure to focus on factual data.

[8] *See, e.g.*, Clyde Williamson, *Pseudonymization vs. Anonymization and How They Help with GDPR*, PROTEGRITY BLOG (Jan. 5, 2017), http://www.protegrity.com/pseudonymization-vs-anonymization-help-gdpr/ (explaining the differences between anonymized and pseudonymized data and their relevance to compliance with the GDPR); *see also* BALAJI RAGHUNATHAN, THE COMPLETE BOOK OF DATA ANONYMIZATION: FROM PLANNING TO IMPLEMENTATION (2013) (offering an integrated view of how anonymization processes work).

[9] *See, e.g.*, Zenobia Hedge, *Privacy and Data Ownership as a European Business Advantage*, IOTNOW (Dec. 21, 2016), https://www.iot-now.com/2016/12/21/56731-privacy-and-data-ownership-as-a-european-business-advantage/.

generated, is at the core of the data-driven economy."[10] That statement is deceptive in its simplicity; if ownership itself is not recognized and enforceable under the rule of law, then the vitality, integrity, and potential of the "data-driven economy" is at risk.

From legal, contractual, and economic perspectives, numerous questions arise. As a general proposition, no privacy or data protection laws expressly define which entity *owns* personal information.[11] So, the following questions appear to apply both for industrial data and personal information: How should ownership of data be defined, if at all? When does ownership attach to data? Are there pre-conditions or criteria (such as originality, level of effort, or imposition of security controls) to be satisfied before ownership will be deemed to be attached to specific data? What are the rights, privileges, controls, and constraints that data ownership vests in the owner? How may those rights, privileges, and controls be transferred or regulated by contracting tools (such as purchase agreements and licenses)? What tools, mechanisms, or processes exist (or can be imagined) that may automatically enforce the rights, privileges, and controls of data ownership across distributed, complex information systems? Do existing, conflicting legal treatments of industrial data under copyright and database laws continue to work if clear ownership itself is defined now as an explicit starting point? How do certainty of ownership and the legitimate exercise of controls on the rights of ownership affect how data is economically valued as an asset of any company, business, or operating entity?[12]

All of these are challenging questions. For this article, we surveyed how, if at all, these questions are being answered amidst the current calls for data ownership to be established. As one scholar described the situation, we are facing "a series of as yet 'unknown unknowns' . . . a framework of law (as distinct from regulation) based on the clear definition of property rights is the best way to lay foundations for future economic success."[13] While we attempted to review the full portfolio of discussions of data ownership and property rights, our focus was on three nations and one international organization: Germany, Japan, Estonia, and the Organization for Economic Co-Operation and Development (OECD).

---

[10] *See* Williamson, *supra* note 8.

[11] Whether property rights are a suitable construct for personal information has been vigorously discussed in academic literature in both the EU and the United States. *See infra* Part III.

[12] "Infonomics" is a term coined by Doug Laney, Vice President and Distinguished Analyst at Gartner. *See generally, e.g.* DOUGLAS B. LANEY, INFONOMICS: HOW TO MONETIZE, MANAGE, AND MEASURE INFORMATION AS AN ASSET FOR COMPETITIVE ADVANTAGE (2017). His work on monetizing data as an economically valued asset has been at the cutting edge of advancing the dialogue on how to value data. *Id.*

[13] EBEN WILSON, DIGITAL DIRIGISME A RESPONSE TO DIGITAL BRITAIN (2018).

A. German Strategies and Innovations

Germany's political leadership has discussed data ownership explicitly; there is also substantive research toward new innovations underway and legal reform proposals.

In March 2017, ahead of CeBit,[14] the world's biggest information technology trade fair, German Chancellor Angela Merkel used a podcast to call for rules for data ownership.[15] She recognized the importance of establishing „möglichst vergleichbare Rechtslagen in allen europäischen Ländern"[16] and besides the „Datenschutzgrundverordnung [, die] ganz wichtig für Europa [ist]," the current discussion needs to focus on „eigentumsrechtliche Fragen."[17] In her remarks, Chancellor Merkel made a strong connection between the need for rules over data ownership and the innovation potential and international competitive ability of the German and European economy. Viewing the automotive industry as a driving force in the German economy („Deutschlands Zugpferd der Wirtschaft"),[18] Angela Merkel observed the need of regulation over data ownership: „[E]s ist natürlich wichtig, ob dem Autohersteller die Dinge gehören, oder ob dem Softwarehersteller die Daten gehören. Denn mit den Daten über die Nutzer wird man natürlich wieder neue Produkte und Anwendungen herstellen können. Und da, glaube ich, alles was Urheberrecht, was Eigentum an Daten anbelangt, da müssen wir noch die Rechtssetzung in Europa sehr schnell und sehr einheitlich durchführen."[19]

---

[14] CeBIT, http://www.cebit.de/en/#new-cebit (last visited Aug. 24, 2017) (describing itself as "Europe's Business Festival for Innovation and Digitization").

[15] Byomakesh Biswal, *Ahead of CeBit Visit, Merkel Calls for Rules Over Data Ownership*, COMPUT. BUS. REV. (Mar. 20, 2017), http://www.cbronline.com/news/verticals/central-government/cebit-visit-merkel-calls-rules-data-ownership/.

[16] The quote translates to: "preferably comparable legal situations in all European countries." VIDEO-PODCAST DER BUNDESKANZLERIN #10/2017 (2017), *available at* https://www.bundeskanzlerin.de/Content/DE/Podcast/2017/2017-03-18-Video-Podcast/links/download-PDF.pdf?__blob=publicationFile&v=4.

[17] [Questions of ownership]. *Id*.

[18] For a more detailed but brief analysis (in German) of the importance of the automotive industry, see *Die Deutsche Automobilindustrie—Im Ausland Weiter Auf Der Überholspur [The German Car Industry-On the Fast Lane Abroad]*, PRICEWATERHOUSECOOPERS (Sept. 25, 2015), https://www.pwc.de/de/internationalisierung/die-deutsche-automobilindustrie-im-ausland-weiter-auf-der-ueberholspur.html (confirming Merkel's description of the automotive industry as the "driving force of the German economy").

[19] [But of course, it is important [the question of ownership], whether the things [data] belong to the car producers or to the software producer. Because by using the date of the user it is possible to produce new products and applications. And at that point, I believe, we need a lawmaking for copyright law, for ownership of data, in

1. Datenausweis for Digital Sovereignty

Alexander Dobrindt, Federal Minister of Transport and Digital Infrastructure, proposed a new law in March 2017 that aligns with Angela Merkel's podcast statement. He calls for a „Datensouveränität des Einzelnen."[20] The minister's proposed data law includes five distinctive principles.

First, data should have the same legal status as material commodities, to assure data can be allocated as property towards a natural person or a legal entity. Second, the data should belong to the person to which the data pertains. If the user does not accept the usage of his or her personalised data, the processing and networking of that data needs to be anonymous and pseudonymous. The power of revocation must be accorded.[21] Third, people should have the chance to make informed decisions on the usage of their data. For this, transparent information is needed which all services and products must guarantee and a data license should include all information about the frequency of collection as well as the usage and disclosure of data. Fourth, public data is to be considered as open data. All non-personalised data which is collected by the state should be an open source to ensure a digital value creation. Finally, as an

---

Europe very soon and in a very coherent manner (when it comes to comparable national legal situations).]

Merkel, Angela: Rede von Bundeskanzlerin Merkel zur Eröffnung der CeBIT 2017 am 19. März 2017, available at https://www.bundesregierung.de/Content/DE/Rede/2017/03/2017-03-19-rede-merkel-cebit.html. By contrast, in the opening speech for CeBit on March 19, 2017 Merkel did not explicitly speak about the regulation of data ownership. But by referring to the achievements of Japan, the guest country of this year's exhibition, she says „Gemeinsam müssen – hier nehme ich das Angebot von Shinzō Abe sehr gern auf – *Standards* für die Vernetzung der Dinge entwickelt werden." ("Together we need—and here I embrace Shinzō Abe's offer—to develop standards of the Internet of Things"). Both countries have, according to Merkel, the same expectations of a social economy with the „Mensch und seine Lebensbedingungen" ("individual and his/her living conditions") in the center. In her speech she also asked: „Bin ich ein Datenlieferant, mit dessen Daten alles Mögliche gemacht wird, oder welchen Schutz und welche eigene Beeinflussungsmöglichkeit habe ich?" ("Am I a supplier of data with whose data everything can be done or what protection or possibility of influence do I have?"). CeBIT, *supra* note 14. Though she does not explicitly call for regulation over data ownership the terminus "Beeinflussungsmöglichkeit" [possibility of influence] gives a hint towards standardizations or regulations.

[20] [Data sovereignty for the individual]. *Wir Brauchen Ein Datengesetz in Deutschland! [We Need a Data Law in Germany!]*, BUNDESMINISTERIUM FÜR VERKEHR UND DIGITALE INFRASTRUKTUR, https://www.bmvi.de/SharedDocs/DE/Artikel/DG/datengesetz.html (last visited Aug. 24, 2017).

[21] There is no indication that Dobrindt was limiting this concept to human individuals, but the principle certainly is consistent with GDPR.

alternative to the open availability of data, users should get the alternative to choose other payment solutions.[22]

While German newspapers[23] mostly wrote about the *Datenausweis* as a tool for data ownership of car drivers, according to the Ministry of Transport and Digital Infrastructure, its cornerstones should be for all „Dienste und Produkte."[24]

As recently as August 2017, a new study was published by the Ministry of Transport and Digital Infrastructure that focused on the mobile phone and related data. That study also confirmed, at present, there is no "data ownership" by the person. „Die verschiedenen Anknüpfungspunkte von verschiedenen Personen stehen in einem bisher nicht auflösbaren Widerspruch."[25]

2. Industrial Data Space

The Industrial Data Space (IDS) is a research project funded by the German Federal Ministry of Education and Research, closely associated with a member organization of companies, Industrial Data Space e.V.[26] The

---

[22] *Wir Brauchen Ein Datengesetz in Deutschland!*, *supra* note 20. In addition to aligning to property rights concepts, the latter principles reflect concepts of transparency and availability consistent with privacy law principles.

[23] *See Dobrindt Schlägt Datenausweis für Vernetzte Fahrzeuge Vor [Dobrindt Suggests a Data License for Interconnected Vehicles]*, ZEIT ONLINE (Mar. 20, 2017, 4:18 PM) http://www.zeit.de/news/2017-03/20/deutschland-dobrindt-schlaegt-datenausweis-fuer-vernetzte-fahrzeuge-vor-20161803; *Verkehrsminister: Dobrindt will „Datenausweis" für Autos [Minister for Mobility wants a "Data License" for cars]*, AUTOMOBILWOCHE (Mar. 20, 2017, 5:00 PM) http://www.automobilwoche.de/article/20170320/AGENTURMELDUNGEN/303209932/verkehrsminister-dobrindt-will-datenausweis-fuer-autosee.

[24] *Wir Brauchen Ein Datengesetz in Deutschland!*, *supra* note 20. Those outside of Europe should also take note that Germany has given digital infrastructure a Cabinet-level priority, something distinctively absent in many other developed economies.

[25] "Different starting-points of different legal entities are in a not yet solved contradiction." BUNDESMINISTERIUM FÜR VERKEHR UND DIGITALE INFRASTRUKTUR, „EIGENTUMSORDNUNG" FÜR MOBILITÄTSDATEN? [SYSTEM OF OWNERSHIP FOR MOBILE DATA?], *available at* http://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile.

[26] BORIS OTTO, ET AL., INDUSTRIAL DATA SPACE: DIGITAL SOVEREIGNITY OVER DATA [sic] (2016), *available at* https://www.fraunhofer.de/content/dam/zv/en/fields-of-research/industrial-data-space/whitepaper-industrial-data-space-eng.pdf; *see also, e.g.*, INDUSTRIAL DATA SPACE ASSOC., www.industrialdataspace.org (last visited Aug. 25, 2017); *Industrial Data Space*, DELOITTE, https://www2.deloitte.com/de/de/pages/innovation/contents/industrial-data-space.html (last visited Aug. 25, 2017).

IDS is developing integrated reference models using standards and common governance models.[27] These models are intended to enable data to be linked within and among business ecosystems and "*ensure[e] digital sovereignty of data owners.*"[28] A 2016 white paper introduced several vital descriptions of the requirements of businesses against which the reference models are to be developed:

> *Data as a product*—As evidenced by the emergence of data marketplaces, data has become a product itself.[29]
>
> *Data sovereignty*—The data owner has "sovereignty," specifically the right to specify the terms and conditions of use for any data provided to others. The models contemplate the owner being able to 'attach' terms and conditions to the relevant data.[30]
>
> *Data economy*—Data is viewed as an economic asset and includes both "private data" (industrial data owned by a specific company) and "club data" (industrial data within a specific value creation chain available to selected companies).[31]
>
> *Data governance*—Companies jointly decide on data management processes as well as applicable rights and duties. IDS emphasizes that the distributed architecture they contemplate specifically needs "rules of the game" to be authored when there is no central supervisory authority.[32]

These concepts, of course, appear to align closely with the policy remarks made by German political leadership.[33] While the IDS white paper and later research do not specify how ownership and property rights originally vest with regard to specific data, their models contemplate that the derivative rights (access, use, levels of aggregation, downstream distribution, etc.) can be implemented as modules into the automated connections among users and other stakeholders such as data providers.[34]

---

[27] OTTO, *supra* note 26, at 4. Four architectures are contemplated, addressing business (including data governance, rights, and duties), security, data and services, and software.

[28] *Id*. (emphasis added).

[29] *Id*. at 10. Big data analytical services have also been creating financial exchanges for data. *See generally*, LANEY, *supra* note 12.

[30] *Id*. at 5.

[31] The connection between this vision of a value chain and the use of blockchain distributed ledger technologies must be emphasized. *See supra* Part V of this article. Data moves within business ecosystems that functionally chain together different data assets, services, and outputs derived from the data.

[32] OTTO, *supra* note 26, at 13.

[33] *See supra* text accompanying notes 15–26.

[34] *Id*. at 24; *see also* BORIS OTTO ET AL., REFERENCE ARCHITECTURE MODEL FOR THE INDUSTRIAL DATA SPACE (2017), *available at* https://www.fraun

The 2017 Reference Architecture Model illustrates that data ownership impacts every layer of the proposed architecture; however, while recognizing that possession and ownership are different concepts, particularly for digital ecosystems, there is not yet further guidance on how ownership attaches to data itself.[35]

B. Japanese Strategies and Innovations for Data Markets

Japan's government also has been conspicuous and productive in its focus on digital strategies. Recent work emphasizes the role of contracts in expressing and governing the rights of commercial parties in industrial data.

1. Contracting for Data Utilization

Japan's Ministry of Economy, Trade and Industry (METI) has produced a number of important policy documents on digitalization strategy and innovations that emphasize its appetite for clear rules on the ownership of data. Its focus is substantive and significant, including expressing the leadership by a Director General for International Cyber Economic Policy.[36]

METI, in May 2017, published Contract Guidelines on Data Utilization Rights ver. 1.0.[37] These Guidelines aim to encourage businesses to clarify data utilization rights by drafting "proper contracts." Use cases for the Guidelines focus on manufacturing company interactions with industrial data, specifically operating data generated from machine tools used in manufacturing and analytical business data from service providers.

Under Japanese law,

> "[D]ata is intangible and not subject to ownership under the Civil Code. Non-personal data may in principle be freely used . . . except for legally protected intellectual property falling under copyright, trade secret or other legal statutes."[38]

---

hofer.de/content/dam/zv/de/Forschungsfelder/industrial-data-space/Industrial-Data-Space_Reference-Architecture-Model-2017.pdf.

[35] OTTO ET AL., *supra* note 34, at 70.

[36] *See* CEBIT ET AL., HOW DIGITAL TRADE CAN SUPPORT BUSINESS TOWARDS AND OPEN AND FAIR BUSINESS ENVIRONMENT 2 (2017), *available at* http://cdnsite.eu-japan.eu/sites/default/files/imce/seminars/2017-03-20-CeBIT/20170320-cebitreport.pdf (stating that Director General for International Cyber Economy Policy at the Japanese Ministry for Economy, Trade and Industry, Kiyoshi Mori, gave the keynote speech) [hereinafter DIGITAL TRADE REPORT].

[37] *See generally Contract Guidelines on Data Utilization Rights ver. 1.0 Formulated*, METI (May 30, 2017), http://www.meti.go.jp/english/press/2017/0530_002.html [hereinafter METI GUIDELINES].

[38] METI, BACKGROUND TO THE FORMULATION OF CONTRACT GUIDELINES ON DATA UTILIZATION RIGHTS VER. 1.0 (2017), *available at* http://www.meti.go.jp/english/

As a result, contracts are recognized as a controlling source of the rules for how data may be utilized within commercial relationships. Yet recently, METI concluded that existing contracts were insufficient.

The Guidelines offered two observations: "Data ownership is often not clarified among businesses" and "Data utilization rights (data ownership) are not necessarily properly or fairly specified in contracts depending on the nature of the data.[39] In practice, data is being utilized without clarifying the particular associated rights." Overall, "a lack of clear definitions and terms for data use in contracts between business partners hinders businesses from making progress in concluding contracts."[40] The Contract Guidelines are awaiting translation into English but are now available in Japanese.[41]

An English-language summary states that model contract clauses are included in the Guidelines, emphasizing that data utilization rights should be "examined fairly and objectively" and take account of the levels of contribution toward creation, preservation, management, and how the data will be utilized.[42] The summary emphasized that "Data utilization right [sic] is not always vested in one party."[43]

In related press coverage, *Nikkei* reported that the guidelines urge companies to clarify, when buying business equipment or entering into business partnerships, who has the rights to the data and how the proceeds from big data will be shared. Automotive (including tires, in-car electronics, and self-driving vehicles), machine tools, and building maintenance are highlighted as big data intensive industries.[44] Central to the collective efforts sponsored by METI is the potential for non-monopolistic data

---

press/2017/pdf/0530_002b.pdf. For our purposes, we accepted this summary of Japanese law without independent verification.

[39] *Id*.

[40] *See* METI GUIDELINES, *supra* note 37.

[41] METI, DĒTA NO RIYŌ KENGEN NI KANSURU KEIYAKU GAIDORAIN [CONTRACT GUIDELINES ON DATA UTILIZATION RIGHTS], http://www.meti.go.jp/press/2017/05/20170530003/20170530003-1.pdf (last visited Dec. 27, 2017).

[42] METI, OUTLINE OF CONTRACT GUIDELINES ON DATA UTILIZATION RIGHTS VER. 1.0 (2017), *available at* http://www.meti.go.jp/english/press/2017/pdf/0530_002a.pdf. Full versions of the model language in English are not yet available.

[43] *Id*.

[44] *Japan to Urge Businesses to Share Big Data*, NIKKEI ASIAN REV. (Apr. 3, 2017, 3:00 AM), https://asia.nikkei.com/Politics-Economy/Policy-Politics/Japan-to-urge-businesses-to-share-big-data.

sharing among industrial collaborators to enhance innovation and overall industrial efficiency.[45]

2. Study of the Fourth Industrial Revolution

Under the auspices of METI, Japan developed its *Japan Revitalization Strategy 2016*.[46] In furtherance of that strategy, the Cross-Sectional System Study Group for the Fourth Industrial Revolution produced a report.[47] This Report emphasized the economic, functional, and strategic importance of data, specifically industrial data, to the rapid evolution of the "Fourth Industrial Revolution."[48] Two classes of data are highlighted by the Study Group: virtual data, which emphasizes data that is inferred from online behavior, and real data, such as that which sensors from industrial operations generate.[49]

The Report describes how online transaction platforms and business operators are not only collecting and using information from their own platforms but seeking out data from other platform and business operators that may enrich and enhance their own data. The Report endorses developing a data distribution market that enables data collected by one platform or business to be more easily exchanged and exploited in order to promote innovation and economic growth. Standards, improved verification, and technology developments; developing rules for "whitelisting" selected data sets (and, logically, sources) to accelerate transaction efficiency; and guidelines and sample clauses for transactional agreements—all are identified as useful building blocks.

As for industrial data, the Report considers "[c]lassification of rights between the parties involved (including possession of the deliverables of data analysis) as a precondition to [smoother data distribution]." Indeed, the Report is quite explicit on the additional building blocks for industrial data, including: "[a]ccurately understanding the current state including what data are stored and where, and which agreement applies to the provision of data is required"; "[d]evelopment of a system of intellectual property rights

---

[45] *Id*.; *see also* George Hill, *Could Japan's Approach to Data Sharing Change the World?*, INNOVATION ENTER. (Apr. 3, 2017), https://channels.theinnovationenterprise.com/articles/could-japan-s-approach-to-data-sharing-change-the-world.

[46] METI, JAPAN REVITALIZATION STRATEGY 2016 (2016), *available at* https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/hombun1_160602_en.pdf.

[47] *See generally* METI, REPORT OF THE CROSS-SECTIONAL SYSTEM STUDY GROUP FOR THE FOURTH INDUSTRIAL REVOLUTION (PROVISIONAL TRANSLATION) (2016), *available at* http://www.meti.go.jp/english/press/2016/pdf/0915_02c.pdf [hereinafter REPORT].

[48] *Id*.

[49] *Id*.

related to data and databases;" and "[u]nderstanding of the current state of contracts regarding intercorporate data transfers."

While expressed in terms of intellectual property and copyright, more detailed discussion in the Report emphasizes that the envisioned data distribution market requires clearly defined rules regarding the rights and privileges of data under the control of platform and business operators. The promotion and sharing of data is encouraged, in large part, to strengthen competitive advantage for existing and new businesses. International standards are encouraged for development, including how companies may identify and express the rights relating to certain data and conditions which may influence the exercise of those rights.[50]

In addition, while acknowledging that databases are protected in Japan by the Copyright Act and that the Unfair Competition Prevention Act also provides trade secret protection of the related creativity and confidentiality, the Report shares contributed comments that "protection outside the existing system is necessary; and not intellectual property rights *but access rights or rights of utilization may be practical for data)*."[51]

In summary, several elements of the Study Group Report are worth emphasizing. The Report recognizes the emergence of industrial data as a resource of economic, functional, and strategic value. But the Report concludes that existing legal systems are insufficient to support the emergence of a data distribution market and that new rules are required. Those rules need to focus on rights, conditions, and commercial agreements (in the words of the Report: "Appropriate rights protection is required for these [new data sharing] technologies and database[sic]."). That seems to confirm the importance of defining rights of use and access without regard to whether the data is personal data or industrial data.[52]

3. Japan Business Council in Europe and EU-Japan Centre for Industrial Cooperation

The Japan Business Council in Europe and the EU-Japan Centre for Industrial Cooperation issued a report in March 2017 emphasizing their mutual, shared progress toward "digital trade" and the development of a "predictable and seamless framework for the digital economy."[53] The report, and the substantive work described in its pages, emphasizes the

---

[50] *See infra* Part V. The proposal offered in Part V is intended to support these building blocks being achieved.

[51] REPORT, *supra* note 47, at 28 (emphasis added).

[52] *Id*. at 27. METI has continued to make progress supporting research toward data utilization and improving distribution environments; *see also Guidelines for Concluding Contracts with Credit Card Affiliated Stores Formulated*, METI (July 3, 2017), http://www.meti.go.jp/english/press/2017/0703_003.html.

[53] DIGITAL TRADE REPORT, *supra* note 36, at 1.

cross-continental work being done to move beyond current digitally-intensive business models toward further innovation.[54] Among other topics, the report described the joint EU and Japanese government commitments to include data flow issues and cooperation on the data economy in the negotiations of a comprehensive Economic Partnership Agreement/Free Trade Agreement (EPA/FTA).[55]

C. Estonian Strategies and Innovation

Estonia is Europe's most entrepreneurial hotspot,[56] with start-ups such as Skype[57] and Transferwise.[58] The most Northern Baltic state is a digital forerunner not only in Europe but worldwide when it comes to digitalization. As a "Baltic Tiger"[59] that was able to radically change its administration towards an e-governance of the 21st century, Estonia is a "digital zoo"[60] visited by national delegations from all over the world, with innovative approaches such as the establishment of data embassies[61] abroad

---

[54] This event report, emphasizing German-Japanese collaboration, should be considered alongside the analysis in the final section of this Part II on the data sharing innovations and developments among the automotive manufacturers from those two nations.

[55] *Id*.

[56] Alex Gray, *Europe's Most Entrepreneurial Country? It's Not the One You Might Expect*, WORLD ECON. FORUM (Mar. 16, 2017), https://www.weforum.org/agenda/2017/03/europes-most-entrepreneurial-country/.

[57] Isabelle de Pommereau, *Skype's Journey from Tiny Estonian Start-up to $8.5 Billion Microsoft Buy*, CHRISTIAN SCI. MONITOR (May 11, 2011), https://www.csmonitor.com/World/Europe/2011/0511/Skype-s-journey-from-tiny-Estonian-start-up-to-8.5-billion-Microsoft-buy.

[58] *See Welcome to Money Without Borders*, TRANSFERWISE, https://transferwise.com/us/about (last visited Dec. 27, 2017) (noting that the company's founder worked for Skype Estonia).

[59] *See generally* FREDERIK ERIXON, EUROPEAN CTR. FOR INT'L POLITICAL ECON, THE BALTIC TIGER: THE POLITICAL ECONOMY OF ESTONIA'S TRANSITION FROM PLAN TO MARKET (2008), *available at* http://www.ecipe.org/app/uploads/2014/12/the-baltic-tiger.pdf (describing Estonia as the "Baltic Tiger").

[60] *See* Ingmar Volkmann, *Wunderdinge aus dem Silicon Valley Europas*[Miracles from the European Silicon Valley], STUTTGARTER-ZEITUNG (Oct. 27, 2017, 5:57 PM), http://www.stuttgarter-zeitung.de/inhalt.estland-als-digitaler-vorreiter-wunderdinge-aus-dem-silicon-valley-europas.f325b055-c099-4211-af53-d725b90f1f0f.html.

[61] *See Estland: Regierungschef Ratas verlagert seine digitale Verwaltung ins Ausland [Estonia: Head of Government Ratas Relocates His Digital Administation Abroad]*, FUTUREZONE.DE TECH. NEWS (June 21, 2017, 7:50 AM), https://www.futurezone.de/netzpolitik/article210981221/Estland-Regierungschef-Ratas-verlagert-seine-digitale-Verwaltung-ins-Ausland.html; *E-Residency*, REPUBLIC OF ESTONIA, https://e-resident.gov.ee (last visited Dec. 27, 2017).

or e-residency receiving attention.[62] Estonia is illustrative of what governments of other nations might implement in the closer digital future.[63]

Yet research was not able to locate any published formal discussion of the concept of data ownership in Estonia's Civil Code or related legal materials. However, the Civil Code introduces an interesting categorization of how legal rights and transactions are to be structured based on the objects of the transaction.[64] Estonian law recognizes three different objects: goods, rights, and other benefits which can be the object of a right.[65] "Property" may also include a set of monetarily appraisable rights and obligations belonging to a person.[66]

However, a right of ownership is a real right, as expressed in the Law of Property, and can be established only in the cases provided by law.[67] While there is no guidance available on the applicability of these concepts to digital information, the possibility exists to argue the rights of control for data might be an "object" that can be the basis for a commercial transaction. Of course, that approach is, at this point, merely speculative. But the Code-

---

[62] *See, e.g., Estonia is Trying to Convert the EU to its Digital Creed*, https://www.economist.com/news/europe/21724831-country-e-residency-wonders-why-others-are-more-sceptical-estonia-trying-convert (last visited Jan. 25, 2018); *Estonia Sets the Standard for a Digital Democracy*, http://www.smartmatic.com/news/article/estonia-sets-the-standard-for-a-digital-democracy/ (last visited Jan. 25, 2018).

[63] *See, e.g., Building Blocks of Estonia*, REPUBLIC OF ESTONIA, https://e-estonia.com/solutions/ (last visited Dec. 27, 2017) (stating additional details on e-Estonia); *see also* Samburaj Das, *100%: Dubai Will Put Entire Land Registry on a Blockchain*, CRYPTOCOINSNEWS (Oct. 9, 2017, 1:01 PM), https://www.cryptocoinsnews.com/100-dubai-put-entire-land-registry-blockchain/. Dubai is another jurisdiction pursuing digital transformation of government services. *Id.*

[64] The authors note, with appreciation, the assistance of Triin Siil in providing guidance on the specific provisions of Estonian law summarized here.

[65] *See* General Part of the Civil Code Act (GPCCA) §§ 48–50 (2017) (Estonia); *see also* RIIGI TEATAJA, https://www.riigiteataja.ee/en/?leht=7&kuvaKoik=false&sorteeri=avaldamiseKp+id&kasvav=false (last visited Dec. 27, 2017) (providing English translations of the GPCCA).

[66] *See* General Part of the Civil Code Act (GPCCA), § 66 (2017) (Estonia); *see also* RIIGI TEATAJA, https://www.riigiteataja.ee/en/?leht=7&kuvaKoik=false&sorteeri=avaldamiseKp+id&kasvav=false (last visited Dec. 27, 2017) (providing English translations of the GPCCA). The concept of appraising value in monetary terms is fascinating to contemplate: How much is data worth? How is that value calculated? What measures are invoked? What qualities can influence the value calculations? These questions are beyond the scope of this article but vital to how digital markets will evolve.

[67] Law of Property Act § 68(1), § 68(3) (2017) (Estonia); *see also* RIIGI TEATAJA, https://www.riigiteataja.ee/en/eli/ee/526012017002/consolide/current (last visited Dec. 27, 2017) (providing English translations of the Law of Property Act).

based recognition of rights highlights how critical it is that there be greater certainty in what those rights are for any specific data asset. At the same time, the fact that ownership rights must be explicit also underscores the potential value with which those ownership rights are viewed explicit.

D. Organization for Economic Cooperation and Development

The OECD has been actively contributing to the strategic analysis required to advance digital markets and economies. It has consistently expressed awareness of the need for reform in the legal infrastructure for data, including in these key reports summarized below.[68]

1. Key Issues for Digital Transformation in the G20

In January 2017, the OECD issued a 150+ page report, *Key Issues for Digital Transformation in the G20*.[69] The Report was prepared by the OECD Secretariat at the request of the G20 German Presidency. It is the most detailed, thorough presentation on the reforms in regulation and legal frameworks required to enable the digital economy reviewed by the authors. Building "advanced governance frameworks" is described as "necessary to effectively address the complexity of today's interlinked issues in successful Industrie 4.0 development and deployment."[70]

One key barrier identified is the awareness that the exclusive rights and control held by an owner of physical goods have *not* been extended to data. While intellectual property rights (such as copyright, database protection laws, and trade secrets) "can be used to a limited extent," more is required to enable "different stakeholders having different rights" to be properly exercised. The scope of those rights is described to include "the ability to access, create, modify, package, derive benefit from, sell or remove data, [and] the right to assign these access privileges to others."[71] Indeed, data ownership and IPRs are identified as a barrier to investments in new data assets and the capabilities of those assets in commerce and industry.[72]

---

[68] *See* OECD, KEY ISSUES FOR DIGITAL TRANSFORMATION IN THE G20, 150–62 (2017), *available at* https://www.oecd.org/g20/key-issues-for-digital-transformation-in-the-g20.pdf (including a detailed bibliography of OECD work product on digitalization and Industrie 4.0).

[69] *See generally id*.

[70] *Id*. at 8; *see also id*. at 73–81.

[71] *Id*. at 65–66; *see also* DAVID LOSHIN, PROCEEDINGS OF THE 2002 ACM CIKM INTERNATIONAL CONFERENCE ON INFORMATION AND KNOWLEDGE MANAGEMENT, RULE-BASED DATA QUALITY 614–16 (2002), *available at* http://doi.acm.org/10.1145/584792.584894.

[72] OECD, *supra* note 68, at 66.

Nearly unique among the reports that were studied was an awareness to the potential for the data generated by autonomous machine-to-machine communications, balanced against the barriers that exist to making the necessary investments.[73]

The Report also concludes that "sound regulatory frameworks . . . that enable digitalisation are essential" to foster innovation by small to medium sized enterprises (SMEs).[74] While emphasizing the importance of developing open standards for technical aspects of Industrie 4.0, the Report recommends that countries develop mechanisms to periodically review their legal frameworks and update them to be responsive to the increasingly digitalised world.[75]

2. Trade Union Advisory Committee

In February 2017, the OECD Trade Union Advisory Committee published an analysis of key issues and recommendations regarding the continuing growth of the digital economy. Emphasizing the goal of fostering progress, the Committee recommended that digital innovation will succeed when based on rules on intellectual property rights that address, among traditional patent and copyright topics, the rights to access, process and delete data, as well as "the right to access digital platforms."[76]

The Committee also addressed data governance, noting that it is important to create better data governance regimes and legal rules. To achieve that objective, "standards on data ownership including the right to access, process, and deletion, and on the pricing of data" are recommended.[77]

E. Summary

This review of German, Japanese, and Estonian developments, as well as the OECD reports, confirms several observations.

First, there is substantial recognition that industrial data has economic and functional importance to the future of digital economies and markets. Data sharing, in order to enable efficiency and innovation, is clearly valued as an outcome to be achieved by improved concepts of data ownership and data governance.

---

[73] *Id*. at 65.
[74] *Id*. at 124.
[75] *Id*.
[76] TRADE UNION ADVISORY COMMITTEE, DIGITALISATION AND THE DIGITAL ECONOMY: TRADE UNION KEY MESSAGES 2 (2017), *available at* https://www.ituc-csi.org/IMG/pdf/1703t_tu_key_recommendations_digitalisation.pdf.
[77] *Id*.

Second, both Germany and Japan recognize the monetary value their economies can create through new innovations and data markets based on a regulation of data ownership.

Finally, while ownership is viewed as an important foundational concept on which transactions in digital information can proceed, none of the materials surveyed propose an answer to the questions presented at the outset of this Part II. However, Japan and the EU-Japan cooperative efforts seem to have progressed furthest toward formulating those answers. In addition, there is formal awareness that the existing structures of copyright and database laws are insufficient to sustain the full potential envisioned for Industrie 4.0.

While other jurisdictions and organizations were examined,[78] none of the materials offered any contradictions of the preceding observations.

F. Data Ownership in the Automotive Industry

Encouraged by the ministerial and policy analyses summarized above, our research narrowed onto the automotive industry to evaluate the degree to which the issues of data ownership and propertization have evolved. Globally, the industry, including both major Japanese and German manufacturers, is accelerating the digitalization of the automobile to support both driverless vehicles and increased tracking of travel and performance.

In 2015, the World Economic Forum published an analysis, *Who Owns Connected Car Data?*[79] Summarizing industry-focused innovations, the Report noted that the technologically self-aware vehicle creates an operating environment in which all vehicles sense each other and, in turn, generate, store, and share immense amounts of data to enable their efficient and safe operation. In asking the title question, the report observed, "The issues are deceptively thorny."[80] Yet, as summarized in a 2016 KPMG

---

[78] Additional materials that were examined include those from the European Union (including the Directorate-General for Communications Networks, Content and Technology, and the European Interoperability Framework), India, Italy, Serbia, Malta, France, Great Britain, the Netherlands, United States, and the Bank for International Settlements. Detailed references are available on request.

[79] Matthew DeBord, *Who Owns Connected Car Data?*, WORLD ECON. FORUM (Sept. 28, 2015), https://www.weforum.org/agenda/2015/09/who-owns-connected-car-data/. Similar media coverage has highlighted the competitive battles among the different stakeholders. *See, e.g.*, Keith Crain, *Who Owns Vehicle-Generated Data?*, AUTO. NEWS (May 11, 2015, 12:01 AM), http://www.autonews.com/article/20150511/OEM11/305119969/who-owns-vehicle-generated-data?; Matt Asay, *Tech Giants vs. Automotive Titans: The Battle for Your Car's Data*, TECHREPUBLIC (Dec. 7, 2015, 11:47 AM), http://www.techrepublic.com/article/tech-giants-vs-automotive-titans-the-battle-for-your-cars-data/.

[80] DeBord, *supra* note 79.

report on the connected car, "What's clear is this: Those who own the data win."[81]

The data produced, and capable of being produced, from the operation of automobiles and trucks and lorries is immense.[82] Sensors monitoring mechanical and electronic components to populate dashboard displays; event data recorders;[83] and linkages between mobile phones and automobiles to enable messaging, audio reminders, and oral conversations pale in significance to the operational industrial data that is generated by a self-driving vehicle.[84] Much of the data is industrial data, irrelevant to the operator or owner's identity, but invaluable to analytics, maintenance, performance evaluation, safety, innovations, and much more. To the extent the data can be identifiable to the operator or owner, a PII classification is appropriate.

The automobile becomes an archetypical example of the fact that nearly any device will consist of two assets: the physical equipment itself and the data generated from its operation. This is true for cars, trucks, locomotives, airplanes, drones, Internet of Things (IoT) devices, industrial

---

[81] KPMG, YOUR CONNECTED CAR IS TALKING. WHO'S LISTENING? (2016), *available at* https://assets.kpmg.com/content/dam/kpmg/br/pdf/2016/11/your-connected-car-is-talking.pdf.

[82] It is estimated that a manufacturer may need to manage 1030 theoretical product variants (headlights and outside mirrors may touch 40 or more alone). Otto, *supra* note 26, at 9.

[83] *See infra* Part II, *Data Rights Ownership in Automotive Event Data Recorders*.

[84] Studies are reporting self-driving, autonomous vehicles will generate up to four terabytes per day; others report a rate of 25 gigabytes per hour. *See, e.g.*, *Connected Cars Will Send 25 Gigabytes of Data to the Cloud Every Hour*, QUARTZ, https://qz.com/344466/connected-cars-will-send-25-gigabytes-of-data-to-the-cloud-every-hour/ (last visited January 25, 2018); Patrick Nelson, *Just One Autonomous Car Will Use 4000 GB of Data/Day*, NETWORK WORLD (Dec. 7, 2016, 7:39 AM), http://www.networkworld.com/article/3147892/internet/one-autonomous-car-will-use-4000-gb-of-dataday.html; Peter Campbell, *UK Urged to Clarify Data Rules from Connected Cars*, FIN. TIMES (July 3, 2017), https://www.ft.com/content/0ebdd2aa-5dc5-11e7-9bc8-8055f264aa8b?mhq5j=e1; Florian Leibert, *The Most Revolutionary Thing About Self-Driving Cars Isn't What You Think*, WORLD ECON. FORUM (June 14, 2017), https://www.weforum.org/agenda/2017/06/the-most-revolutionary-thing-about-self-driving-cars-isn-t-what-you-think/ (stating that "[e]ach self-driving car is becoming its own powerful data centre" and highlighting that one of the key challenges is the speed at which computing must occur within the vehicle—a one second delay, at 65 mph moving speed, could be a life-or-death consequence).

manufacturing units, and so much more.[85] Overall, any associated PII is only a small slice of the overall data any of these devices will be producing.

It may be useful to delve into a fairly standard transaction set involving the assembly and sale of an automobile to illustrate the thorniness. The automotive manufacturer assembles each vehicle from a variety of components acquired by contract from subcontractors, including devices that act as data sensors, recorders, and communication units. Subcontractors may include both device suppliers as well as software developers that license software for installation in the vehicle (as well as paired applications enabling the data to be received and used by the manufacturer). Among the manufacturer and the subcontractors, who claims ownership to the data produced during the vehicle's operation? All would have good reasons to negotiate for the rights of ownership, including controlling the use of that data for analytics, product design and other uses unrelated to specific PII.

The vehicle is then sold to a commercial dealer. Does the dealer acquire any ownership interest in the data produced during operation? Until the vehicle is sold to a consumer, the dealer is the true owner; would that status not vest the dealer with rights to access and control the related operational data no different than the end consumer might claim to possess?

In wholesale and retail consumer transactions, the purchase price may be financed, either through a consumer loan or a lease (in which a leasing company purchases the car as the true owner, and then leases the vehicle to a consumer). Does the leasing company acquire the ownership rights to the data stream during the term of the lease? At this point, the consumer identity also can become tricky—even a true owner of the vehicle may not always be the operator. How will data associated with each operator be distinguished, and what will be their respective claims to their PII, as well as the other industrial data?

Insurance companies and governmental authorities have ongoing interests in being able to access the operational data generated by the automobile. For insurance companies (as well as financing lenders and leasing companies), the data has immediate use for assuring compliance with any conditions that may be a part of the related agreements (for example, conditioning insurance coverage on operation of the vehicle within defined geographic boundaries or at speeds not exceeding 105% of the posted speed limits). In these circumstances, the identity of the operator

---

[85] The National Football League is even placing data sensor chips in footballs used in professional games. Ken Belson, *NFL Expands Use of Chips in Footballs, Promising Data Trove*, N.Y. TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/sports/nfl-expands-use-of-chips-in-footballs-promising-data-trove.html.

of the vehicle at any time, their respective rights in the operating data and their rights with respect to the related PII add additional complexity.

Other media coverage we surveyed highlights the type of questions for which the data can be useful in the event of a collision. Will parts suppliers be liable if the data indicates a related component failure? Was the use of autopilot suitable in the surrounding circumstances (such as extreme weather conditions)? Were brakes properly applied? Was the steering wheel at a suitable angle? Did the airbags properly deploy?[86]

There are also information security issues. Who is responsible for securing the systems and operational data from intrusion, exfiltration, or compromise? As well, there are further complexities of ownership when automotive systems connect to telecom systems or on-board entertainment devices such as OnStar or Sirius.[87] In our view, many of these questions can be resolved by clear, legally enforceable allocations of ownership and control among the various stakeholders.[88]

1. Data Rights in Automotive Event Data Recorders

Event data recorders installed in automobiles (EDRs) are similar to the black boxes installed in aircraft. They record data from sensors and systems within the vehicle and, when the EDRs detect an accident or collision, the related data is then stored and preserved for extraction and analysis. In 2010, significant public attention was drawn to the use of these devices and, in turn, media coverage reported on how Toyota used and disclosed the information.[89] Historically, while EDRs had been installed for

---

[86] *See* Crain, *supra* note 79. For recent liability issues relating to airbag deployment, *see, e.g.*, *Takata Airbag Recall – Everything You Need to Know*, CONSUMER REPORTS (July 14, 2017, 10:30 AM), https://www.consumerreports.org/cro/news/2016/05/everything-you-need-to-know-about-the-takata-air-bag-recall/index.htm. For information regarding unintentional accelerations, *see, e.g.*, Junko Yoshida, *Acceleration Case: Jury Finds Toyota Liable*, EE TIMES (Oct. 24, 2013, 9:00 PM), http://www.eetimes.com/document.asp?doc_id=1319897. For information regarding emission controls, *see, e.g.*, Guilvert Gates et al., *How Volkswagen's 'Defeat Devices' Worked*, N.Y. TIMES (Mar. 16, 2017), https://www.nytimes.com/interactive/2015/business/international/vw-diesel-emissions-scandal-explained.html. All the related accidents involved in-car control systems and operational data was vital to the investigation and discovery of the related product defects.

[87] *See* KPMG, *supra* note 81.

[88] The KPMG report also describes an April 2016 negotiation breakdown among Apple, BMW and Daimler regarding questions of data ownership, cloud-based software, and data protection. *Id*.

[89] *See, e.g.*, Peter Whoriskey, *Event Data Recorders Used in NHTSA Study of Toyotas Have History of Problems*, WASH. POST (Aug. 20, 2010),

several years, Toyota was reported to refuse to disclose the data or would make only partial disclosures, including in litigation involving automotive safety claims.[90] State governments, including California, have enacted responsive regulations requiring notice and disclosures to consumers of the circumstances in which data may be downloaded from a vehicle's EDR, generally inside the user's manual that is delivered with the vehicle.[91]

Admittedly, there is a privacy element to the data collected by an EDR, but when EDR data is limited to accident-based collection (such as storing the data for the 30 second period prior to an event detected by the EDR), much of that concern is diminished. Indeed, when a collision has occurred, the public laws specifically confirm how regulators, investigators, and insurance companies may require access to, and obtain, the stored data. What the regulations seem to infer is that the automotive owner or operator controls the access and use to the collected data, but we explored how different manufacturers complied with the notice and disclosure rules regarding the data access and use rights to automotive owners, consistent with the regulatory requirement that they do so. The user manuals for the following automotive manufacturers were considered: Ford,[92] Toyota, Honda,[93] Porsche,[94] and BMW.[95]

Each manufacturer, with one exception, seems to faithfully reproduce the notices and disclosures that were mandated by public laws. Some variations occurred in how the language was presented, perhaps as a

---

http://www.washingtonpost.com/wp-dyn/content/article/2010/08/19/AR2010081906562.html.

[90] *See, e.g.*, Zachary L. Wool, *Toyota Hides Important Black Box Crash Data*, BARRIOS KINGSDORF & CASTEIX, L.L.P., http://www.bkc-law.com/blog/toyota-hides-important-black-box-crash-data/ (last visited July 24, 2017).

[91] The National Conference of State Legislatures has published a summary of this legislation. *See Privacy of Data from Event Data Recorders: State Statutes*, NAT'L CONF. OF STATE LEGS., http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx (last visited Aug. 10, 2017).

[92] FORD, FORD FOCUS 2017 OWNER'S MANUAL (2017), *available at* http://www.fordservicecontent.com/Ford_Content/Catalog/owner_information/2017-Ford-Focus-Owners-Manual-version-1_om_EN-US_EN-CA_10_2016.pdf.

[93] HONDA, 2008 PILOT ONLINE REFERENCE OWNER'S MANUAL (2008), *available at* http://techinfo.honda.com/rjanisis/pubs/OM/9V0808/9V0808OM.pdf.

[94] PORSCHE, PANAMERA OWNER'S MANUAL (2009), *available at* http://www.porsche.com/all/media/pdf/Owners_Manual_Panamera_PCNA.pdf.

[95] BMW, OWNER'S MANUAL FOR VEHICLE (2007), *available at* www.bmwusa.com/pdf_6ea435bc-898e-4455-90ac-0175dc04d47c.arox.

result of differences in the locations in which the vehicles are sold.[96] But the notices were complex, difficult to understand, and likely ineffective.[97]

The exception is noteworthy. In its notice, Honda, a Japanese-based manufacturer, stated specifically:

> This vehicle is equipped with one or more devices commonly referred to as event data recorders. These devices record front seat belt use, front passenger seat occupancy, airbag deployment data, and the failure of any airbag system component. ***This data belongs to the vehicle owner*** and may not be accessed by anyone else except as legally required or with the permission of the vehicle owner.[98]

This clear declaration of the automobile owner's ownership of the data is not required, but is both conspicuous and effective. Indeed, often, by its own terms, the manual is part of the contract between the manufacturer and the purchaser of the vehicle.[99] We find this example encouraging; it illustrates that data ownership can be affirmatively vested in an end consumer, while also clearly reserving the rights of designated third parties to access and use the stored data for defined purposes.[100]

G. The State of Law Regarding Data

The existing states of formal law regarding data ownership are both diverse, and often in conflict; many works of scholarship summarize these conflicts and report on the manner in which existing laws have evolved.[101]

---

[96] As with many consumer disclosures, manufacturers appear to work to consolidate into one notice and disclosure everything required by all of the jurisdictions.

[97] While the effectiveness of these specific notices has not been researched, their semantic structure and presentation are comparable at first glance to other notices regarding Internet websites and personal health information, the effectiveness of which has been researched and reported upon. *See, e.g.*, Matthew W. Vail et al., *An Empirical Study of Consumer Perception and Comprehension of Web Site Privacy Policy*, 55 IEEE TRANSACTIONS ON ENG'G MGMT. 442, 442–54 (2008); Ninghui Li et al., *A Semantics-based Approach to Privacy Languages*, 21 INT'L J. COMP. SYS. SCI. & ENG. 339, 339–52 (2006); Annie I. Antón et al., *The Lack of Clarity in Financial Privacy Policies and the Need for Standardization*, 2 IEEE SEC. & PRIVACY, 36–45 (2004).

[98] HONDA, *supra* note 93 (emphasis added).

[99] The Ford manual says "[this manual] is an integral part of your vehicle." FORD, *supra* note 92. Of course, this language does not resolve other questions raised in the preceding text regarding the ownership rights of non-owner operators, leasing companies, etc.

[100] This approach is exactly what is proposed *infra* Part V. Asserting and confirming the property rights in data need not conflict with the controls and constraints that a data subject (or similarly positioned corporate entity) may be entitled to assert with regard to the use of the data.

[101] Several of the most significant works are presented *infra* Part III.

For our purposes, it is sufficient to conclude here that there is no clear expression of ownership rights for digital data in the legal systems we reviewed in Europe, the United States, or other countries for which we surveyed summaries (available in English or German languages). Four essentials, however, are worth summarizing.

First, U.S. law, through an important decision of the Supreme Court, limits reliance on copyright law to protect databases of factual information, unless there is sufficient creativity in the development of the databases to justify copyright protection.[102] Second, the EU Database Directive, perhaps in reflex to the U.S. Supreme Court decision, does grant to the manufacturer of a database *sui generis* rights that vest in a database without regard to the innovation or originality required under U.S. copyright law.[103] Those rights are similar to many rights vested in owners of physical, tangible properties, including the ability to prohibit extraction or use of the data without suitable agreement.[104] Third, privacy and data protection laws conspicuously omit any direct references to "ownership" of PII; instead, there is a focus on the controls and limitations a data subject may exercise and/or negotiate through consent mechanisms.[105] Finally, in Japan, data is not subject to ownership under the Civil Code and, unless copyright, trade secret, or other legal statutes directly apply, data may be freely used.[106]

---

[102] *See* Feist Publ'ns, Inc. v. Rural Telephone Serv. Co., 499 U.S. 340, 363 (1991); *see also* Assessment Techs. v. Wiredata, 350 F.3rd 640, 644 (7th Cir. 2003) ("A work that merely copies uncopyrighted material is wholly unoriginal and the making of such a work is therefore not an infringement of copyright."). For an excellent perspective on the impact of the *Feist* decision, *see generally* Craig Joyce & Tyler T. Ochoa, *Reach Out and Touch Someone: Reflections on the 25th Anniversary of* Feist Publications, Inc. v. Rural Telephone Service Co., 54 HOUS. L. REV. 257 (2016–2017).

[103] Directive 96/9/EC, of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, 1996 O.J. (L 77/20), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996L0009.

[104] *See generally Protection of Databases*, EUROPEAN COMM'N (June 7, 2016), http://ec.europa.eu/internal_market/copyright/prot-databases/index_en.htm (containing links to several useful, detailed analyses of the Directive and its subsequent implementation).

[105] *See, generally*, Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, available at http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf; Privacy Regulation 2013 under the Privacy Act 1988 (Australia), available at https://www.legislation.gov.au/Details/F2018C00011; and the Fair Credit Reporting Act, 15 U.S.C. § 168 (regulating, in part, the privacy of personal financial information).

[106] *See supra* notes 36–55 and accompanying discussion.

III. PROPERTY RIGHTS IN DATA — ACADEMIC REVIEW

In preparing this article, we sought to identify existing scholarship on proposing property rights for all data. Our purpose was not to exhaustively account for all analyses; instead, we were investigating whether the two fundamental principles on which our proposal rests (as presented in Part V *infra.*) have been previously considered. Those two principles are that a) data is physical, capable of being governed by property rights systems comparable to those in place as part of the global legal infrastructure,[107] and b) control of data, as already expressed in formal commercial statutes and international model laws, could be the basis on which property rights may be asserted and transferred.[108]

Our research did not uncover any considerations of those principles. But the concept of applying property rights to personal information has been vigorously debated and analyzed. In addition, recent work, particularly in Europe, is advocating property rights for industrial data. These are useful to highlight, if only to emphasize that the functional questions of *how* to assert, perfect, and govern property rights in digital information have not been addressed.

A. Personal Information and Data Subjects

Global legal standards for protecting personal information evolved with considerable speed. Today, across most developed economies, data subjects have rights—expressed in constitutions, directives, statutes, regulations, and judicial decisions—to regulate how their personal information, once collected, can be used, processed, or distributed.

As a general matter, the pivot point at which those rights are to be expressed is the mechanism for notice and consent. In those terms and conditions, most of the rights are described in detail, particularly when the rights differ from the statutory default rules. Certain additional rights, including the right to correct fictional data (which includes inaccurate statements of data purported to be factual data) and to remove the availability of specific personal information from databases or published resources (i.e., the right to be forgotten) also have been described in formal regulations. Of course, the EU's framework, updated by the GDPR, contrasts dramatically with the industry-specific regulatory approach in the United States.[109]

---

[107] *See infra* Part IV.

[108] *See infra* Part V.

[109] *See* Directive 96/9/EC *supra* note 103; *see generally* ALAN CHARLES RAUL, THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 268 (2014), *available at* https://www.sidley.com/-/media/files/publications/2014/11/the-privacy-data-protection-and-cybersecurity-la__/files/united-

1. American Scholarship

In the evolution of privacy laws, there were several detailed academic explorations of whether explicit property rights should be granted to data subjects with regard to their personal information, notably in U.S. literature.[110] Alan Westin proposed that personal information should be formally recognized as an object of property rights in the late 1960s.[111] The issue continues to be analyzed into the current decade and five more recent works are worth highlighting.

Professors Nimmer and Krauthaus asserted that the notion of privacy in the United States was first shaped and framed by an article by Warren and Brandeis published in 1890.[112] They concluded that, from that early point, privacy analysis in the United States abandoned any notion of being grounded in property law concepts. Instead, the expression of rights was based in tort (i.e., liability). A violation of an individual's rights entitled them to seek compensation because their ability to assert personal control had been abused, in the same manner that a corporation is presumed to have control of their trade secrets which, if abused, entitle them to seek recourse under tort law.

By contrast,

> Property rights in information focus on identifying the right of a company or individual to control disclosure, use, alternation and copying of designated information. The resulting bundle of rights and limits comprises a statement of what property exists in information . . . . A property analysis speaks in terms of transferable assets and fixed zones of legally enforceable control, rather than the type of

---

states/fileattachment/united-states.pdf (summarizing the diverse regulations and enforcement approaches in the United States).

[110] The American Bar Association Section of Science and Technology Law has established a Data Property Rights Committee. *See Section of Science & Technology Law: Data Property Rights Committee*, AM. BAR ASS'N, http://apps.americanbar.org/dch/committee.cfm?com=ST207055 (last visited Aug. 5, 2017). As part of their work, the Committee maintains an outstanding inventory of legal materials relevant to evaluating the evolution and debate regarding the exercise of property rights in data. *See* AM. BAR ASS'N, COMMITTEE SUMMARY OF ARTICLES ON THE LAW OF PERSONAL DATA (2014), *available at* https://www.americanbar.org/content/dam/aba/administrative/science_technology/2014_data_prop_rights.pdf.authcheckdam.

[111] ALAN F. WESTIN, PRIVACY AND FREEDOM (1967).

[112] Raymond T. Nimmer & Patricia A. Krauthaus, *Information as Property Databases and Commercial Property*, 1 INT'L J. L. & INFO. TECH. 3, 30 (1993–1994) (citing Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)). Those outside the United States may be surprised that privacy considerations arose so early in American jurisprudence!

> continuously flexible balancing of interests and reliance on standards of reasonable behavior common in constitutional or tort law analyses."[113]

The distinction was elaborated on by Professors Lemley and Weiser:

> Traditionally, rights such as the ownership of real property are generally protected by injunctions, while tort and contract rights are enforced by means of compensatory damages. As famously explained by Calabresi and Melamed, these different remedial options represent alternatives for enforcing a legal entitlement—a property rule provides for an injunction and a liability rule provides for nonconsensual access in return for a payment of money damages.[114]

Professor Bergelson used this distinction to advocate that property rights were a suitable legal foundation for personal information in the United States.[115] She recommends certain rights be "inalienable," incapable of being foreclosed even if other rights for specific data have been transferred. She suggests those include rights to obtain records, demand corrections, and block or erase inaccurate information.[116] In doing so, she moves into offering a structure for property rights that is distinctive from those rights grounded in tort.

This distinction influenced the evolution of our proposal. To assert that a property rights system is suitable for all data has two implications. First, the existing legal structures for personal information (including the GDPR) need to be evaluated by asking whether there are any different notions of property rights now established. Quite simply, we do not see that to be the case. Instead, while the GDPR includes useful reforms responsive to new technologies, business models, and improving accountability, the fundamental structure is still expressive of a tort law framework in which vague or ambiguous standards must be applied within a variable larger context described by relevant circumstances and actions. The same is true in the United States.[117] Second, is there any explicit property rights or tort

---

[113] Nimmer & Krauthaus, *supra* note 112, at 5–7.

[114] Mark A. Lemley & Philip J. Weiser, *Should Property or Liability Rules Govern Information?*, 85 TEX. L. REV. 783, 786 (2007) (citing Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1092 (1972)).

[115] Vera Bergelson, *It's Personal But Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379 (2005).

[116] *Id*. at 444 (citing Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) art. 12).

[117] Nimmer cites the Supreme Court's decision in *Feist Publ'ns, Inc*., which reserves protection for databases determined to have sufficient originality in their

law construct established to protect industrial data beyond the portfolio of copyright and database laws? Again, we have concluded that is not the case. Professor Nimmer concurred, concluding that copyright laws are an unstable means of protecting distributed informational works, noting that protection relies on enforcing contractual obligations and technology controls.[118]

In 2011, Lund argued that an individual should have an "enforceable property right" over their own personal information.[119] Lund describes it as a "limited" property right, sufficient to allow individuals to enforce requests for retraction or correction of inaccurate personal information (therefore fictional data in our proposed classification).[120] Implicit is the burden on the data subject to prove the factual information asserted to be true is "readily verifiable."[121] The analysis fails to address how that right might be enforced across cloud-based services that cross national boundaries or other current complexities; illustrative examples of how the right might be exercised are built upon American actors seeking recourse in American courts under American judicial rules.[122]

Even earlier, in 1993, Laudon proposed information markets for personal information were entirely viable.[123] He envisioned the markets could be the only legal avenue for transferring personal information for secondary purposes; this idea is notable because it introduces structured governance for the administration of the property rights.[124] With his focus on personal information, Laudon offered:

---

design to overcome the general rule that assembled factual data is itself not protected. Nimmer & Krauthaus, *supra* note 112, at 15. This result is in contrast, of course, to the EU Database Directive, which grants explicit rights, but still conditions those rights on the level of effort invested in constructing and maintaining the database. *See generally* Directive 96/9/EC, *supra* note 103.

[118] Raymond T. Nimmer, *Information Wars and the Challenges of Content Protection in Digital Contexts*, 13 VAND. J. ENT. & TECH. L. 825, 826 (2011).

[119] Jamie Lund, *Property Rights to Information*, 10 NW. J. TECH. & INTELL. PROP. 1, *passim* (2011).

[120] *Id.* at 9.

[121] *Id. at 16.*

[122] *See generally id*. An earlier work by Professor Schwartz also advocated for these inalienable rights; the analysis is comparable, but dated by the evolutions in technology since its publication. *See generally* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004).

[123] Kenneth C. Laudon, *Markets and Privacy* (Ctr. for Dig. Econ. Research, Working Paper No. 93-21, 1993), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1284878.

[124] *Id*. at 18. The debates and competing models between this type of centralized control proposed over 25 years ago and the decentralized administration envisioned

> No revolution in American property law is required to support national information markets. First, property law is quite flexible in recognizing value in a wide variety of tangible and intangible assets, including one's personal image. For instance, since the turn of the century courts have recognized the claims of celebrities to a property interest in their photographic image and the right of celebrities to seek compensation whenever their image is used for a commercial purpose. What is needed is the extension of a property interest to the digital data image of ordinary individuals.[125]

The surveyed American academic scholarship confirms that current U.S. law does not express a definitive right of ownership in any class of data, whether industrial data or PII. At the same time, there is nothing that appears to prevent legal reforms to establish those rights. What will be fascinating is whether the rights should be incorporated into federal law (such as copyright) or state laws (such as the laws for real property, goods, and various individual rights) with respect to the breach or unauthorized disclosure of PII. Our proposal does not restrict the mechanisms for implementation to any specific legislative body.

1. European Perspectives

Perhaps the most thorough European study on property rights in data was produced by Professor Purtova.[126] While limited to personal data, the analysis surveys the legal and pragmatic foundations of current EU laws on the scope of rights in data and how those rights might be governed. But, as stated by Purtova, "The key message this study hopes to convey is that it

---

by blockchain advocates will be fascinating; but neither model functions effectively if rights and obligations are not closely paired to, or coupled with, the information.

[125] *Id*. at 23. This concept is also capable of application to industrial data, consistent with our proposal *infra* Part V.

[126] *See generally* NADEZHDA PURTOVA, PROPERTY RIGHTS IN PERSONAL DATA: A EUROPEAN PERSPECTIVE (2011), *available at* https://pure.uvt.nl/portal/files/1312691/Purtova_property16-02-2011.pdf [hereinafter A EUROPEAN PERSPECTIVE]. For an abbreviated version of this work, *see* NADEZHDA PURTOVA, PROPERTY IN PERSONAL DATA: A EUROPEAN PERSPECTIVE ON THE INSTRUMENTALIST THEORY OF PROPERTISATION (2010), *available at* http://cadmus.eui.eu/bitstream/handle/1814/15124/10_Property_EN.pdf?sequence=1 [hereinafter A EUROPEAN PERSPECTIVE ON THE INSTRUMENTALIST THEORY OF PROPERTISATION]. In this paper, Purtova acknowledges that "so far only few European commentators have reflected on the possibility of propertisation." *Id*. at 3 (citing Corien Prins, *Property and Privacy: European Perspectives and the Commodification of our Identity*, *in* THE FUTURE OF THE PUBLIC DOMAIN, IDENTIFYING THE COMMONS IN INTERNATIONAL LAW (Lucie Guibault & P. Bernt Hugenholtz 2006)).

is impossible to give a simple 'yes' or 'no,' '1' or '0' answer to the questions on the possibilities of and need for propertisation."[127]

That conclusion is problematic for, in contrast to the more current calls in Europe for ownership principles to be adopted, there is no sense expressed by Purtova of why the notions of propertization were not embedded into the original and evolving states of EU data protection and privacy laws, nor any suggestion of how to navigate forward toward achieving that objective.

In early 2017, the Joint Research Centre of the European Commission issued a technical report on the economics of ownership, access and trade and digital data.[128] The report concludes that "the GDPR gives data subjects no full ownership rights, only certain specific rights"[129] While acknowledging the Database Directive "gives some limited property rights to data collectors," the report observes that there is a "wide area where ownership or residual rights are not legally specified, or incompletely specified."[130]

B. Property Rights in Data Other Than Personal Information

In the United States, both scholars and law reform organizations have considered whether property rights are appropriate for data other than personal information. Indeed, as summarized below, a formal model law was developed and approved for submission to the states for possible enactment. These materials were also considered.

In 2004, Professor Lipton contributed an important analysis of information property ownership, exploring the rights and obligations of owning information as property.[131] Her analysis emphasizes that information property rights must be balanced against important principles involving the preservation of information and ideas in the public domain, and balanced against competing private interests in the information and legitimate copyright and other intellectual property interests. In addition, she articulates how ownership also entails obligations, and uses metaphors and analogies from real property law as guidelines for constructing the

---

[127] A EUROPEAN PERSPECTIVE, *supra note* 126, at 12.

[128] Nestor Duch-Brown et al., *The Economics of Ownership, Access and Trade in Digital Data* (European Comm'n Joint Research Ctr. Working Paper 2017-01), *available a*t https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf.

[129] *Id*. at 17.

[130] *Id*. at 18. The report references the extensive German materials and also explores in some depth the merit of clarifying rights to create proper incentives and summarizes other academic proposals on ownership within a European context. *See generally id*. at 18–20.

[131] Jacqueline Lipton, *Information Property: Rights and Responsibilities*, 56 FL. L. REV. 135 (2004).

obligations of data ownership.[132] Both of these facets are important to consider, of course, as more complete structures of ownership rights and responsibilities evolve. But our proposal focuses on more narrow questions: When and how can data ownership be established, and how can it be transferred in legitimate transactions? On these, Professor Lipton provided no guidance.

However, the concept of data ownership is not unfamiliar to American law. Beginning in the last decade of the twentieth century, in response to the absence of any treatment in the Uniform Commercial Code for software transactions, a model uniform law, known as the Uniform Computer Information Transactions Act (UCITA), was produced and adopted in 2002.[133] UCITA was comprehensive, going much further than just addressing software. The proposed Act offered a legislative framework to be adopted into state law that would also enable "computer information transactions" and "informational rights" in computer information. In doing so, UCITA offered enormous vision.

But the Act also presented the concept that software licenses could be structured with warranties of fitness and suitability, and other user-protective standards, concepts to which the software industry was strongly opposed. The result, to date, is that UCITA was only adopted in two states—Virginia and Maryland—and nearly all modern software agreements expressly disclaim the applicability of the law.[134]

C. Conclusions

Based on the preceding, we reached two conclusions that substantiate the urgency of the need to pursue a property rights scheme for data.

Our first conclusion is that, without exception, none of the prior analyses of whether a property rights scheme should be applied to digital information explicitly considered the vast quantities of data that are not personally identifiable information—that is, industrial data.[135] That seems

---

[132] *Id*. at 174–77.

[133] UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT (UNIF. LAW COMM'N, Proposed Draft 2002), *available at* http://www.uniformlaws.org/shared/docs/computer_information_transactions/ucita_final_02.pdf.

[134] Detailed information about UCITA is available from the Uniform Law Commission. UNIFORM LAW COMMISSION, http://www.uniformlaws.org (last visited Jan. 5, 2018). One author of this paper, Jeffrey Ritter, was active in the drafting of UCITA for several years as a representative of the American Bar Association.

[135] The UCITA materials suggest that the full breadth of digital information was recognized by the drafting efforts, but the final version of the Act includes no characterizations that differentiate personal information and industrial data.

almost astounding, taking account of the volumes of data that are being produced and retained globally. Some public estimates project 2.5 quintillion bytes of data are created each day,[136] with total volumes growing at forty percent per year and the 2015 volumes projected to grow by fifty times by 2020.[137] Those expand to represent approximately forty-four zettabytes (1000^7 gigabytes) within less than three years.[138]

PII is only a small portion of the volumes of data that are created and retained each moment in each day of industrial operations. International shipping, fuel production, and business communications (such as electronic data interchange) produce enormous volumes entirely in support of business activities unrelated to individual persons. For example, business-to-business (B2B) electronic commerce transactions are projected to reach US$6.7 trillion by 2020, and each transaction produces data records entirely focused on the commercial transaction.[139]

Indeed, the apparent omission of any *industrial data* from prior deliberations on the suitability of a property rights scheme is surprising. While the regulation of PII is vital, the market confirms the wealth creation potential that can be extracted from industrial data. Indeed, the current and projected revenues from big data services are being realized without any substantive legal structure in place to define the information's ownership and attendant rights![140]

The second conclusion is that the academic deliberations, as well as the policy materials we reviewed, have not discussed in any manner the scientific consensus that digital information is, itself, physical. As examined

---

[136] *Every Day Big Data Statistics – 2.5 Quintillion Bytes Created Daily*, VCLOUD NEWS (Apr. 5, 2015), http://www.vcloudnews.com/every-day-big-data-statistics-2-5-quintillion-bytes-of-data-created-daily/.

[137] Michael de Waal-Montgomery, *World's Data Volume to Grow 40% Per Year & 50 Times By 200: Aureus*, E27 (Jan. 15, 2017), https://e27.co/worlds-data-volume-to-grow-40-per-year-50-times-by-2020-aureus-20150115-2/.

[138] Mikal Khoso, *How Much Data is Produced Every Day?*, NE. UNIV. (May 13, 2016), http://www.northeastern.edu/levelblog/2016/05/13/how-much-data-produced-every-day/; *see* Bernard Marr, *Big Data: 20 Mind-Boggling Facts Everyone Must Read*, FORBES (Sept. 30, 2015, 2:19 AM), https://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#b48f37017b1e.

[139] *B2B Ecommerce Market is Still Maturing*, EMARKETER (Aug. 8, 2016), https://www.emarketer.com/Article/B2B-Ecommerce-Market-Still-Maturing/1014311.

[140] In 2016, IDC projected that worldwide revenues for big data and business analytics will exceed $203 Billion in 2020. *Double-Digit Forecast for the Worldwide Big Data and Business Analytics Market Through 2020 Led by Banking and Manufacturing Investments*, INT'L DATA CORP. (Oct. 3, 2016), https://www.idc.com/getdoc.jsp?containerId=prUS41826116.

below in Part IV, that concept places much of the work during the last thirty years to adapt prior law to the nature of electronic commercial practices and digital commerce in a somewhat awkward position. If data is indeed physical, versus a form of intangible property, why has there been no legal construct modeled on well-developed property right systems for other types of physical assets?

No one seems to have asked or answered the question, "What is data?" There has been no inquiry as to the origin of data ("When does data begin to exist?"); no exposition on the classification schemes, data dictionaries, and other tools used to define and manage data ("What is this data in our possession?"); and, with few exceptions relating to anonymization of PII, no exploration of how data can be combined, transformed, processed, analyzed, and distilled into new combinations and output ("What can be done to data to make something new or create value in a transaction?").

These two conclusions are not meant to be critical of the prior literature; instead, they only serve to confirm that the proposals presented in Part V have not been previously considered. If there is not yet a clear, consensus-based agreement within the legal community on what data actually is—namely physical, tangible matter stored by electronic or similar means—how can a supportive, scalable, resilient legal construct be put into place that enables data-intensive transactions to prosper? To facilitate that consensus, we researched the simple question, "What is data?"

IV. THE PHYSICAL REALITY OF INFORMATION

In 1991, pursuing the potential for quantum computing, Rolf Landauer authored a landmark article titled *Information is Physical*.[141] That work was followed by several more papers in which Landauer presented a straight-forward point:

> Information is not an abstract entity but exists only through a physical representation, thus tying it to all the restrictions and possibilities of

[141] Rolf Landauer, *Information is Physical*, 44 PHYSICS TODAY 23–29 (1991). *See* John Mingers & Craig Standing, *What Is Information? Toward a Theory of Information as Objective and Veridical*, J. INFO. TECH., May 24, 2017, at 1("By objective, we mean that the information carried by signs and messages exists independently of its receivers or observers. The information carried by a sign exists even if the sign is not actually observed. By veridical, we mean that information must be true or correct in order to be information – information is truth-constituted. False information is not information, but misinformation or disinformation.").

> our real physical universe . . . information is inevitably inscribed in a physical medium.[142]

Landauer also stated convincingly

> Information is not a disembodied abstract entity; it is always tied to a physical representation . . . This ties the handling of information to all the possibilities and restrictions of our real physical world, its laws of physics and its storehouse of available parts.[143]

As summarized by Bawden and Robinson, the physical quality of information, and the idea that information is a physical constituent of the universe, are widely adopted within the scientific community.[144] The Foundational Questions Institute, a non-profit physics organization, has established a grant program to research the physics of information.[145] Considerable scientific research studies the physical attributes of information. From the earliest work of Claude Shannon in 1948 to set forth a definition of information offering a mathematical theory on information to ongoing research into information entropy, transmission velocities, data compression, and cryptography, the essential tangible state of information is a vital truth fueling continued advances in information technology.[146]

To this point in the evolution of regulating digital information, however, our review of the scholarship and legislative histories available to us suggests the physical nature of data (as defined above) has not been considered in deliberating on how to structure and apply the rule of law.[147]

---

[142] Rolf Landauer, *Information is a Physical Entity*, 263 PHYSICA A: STAT. MECHANICS AND ITS APPLICATIONS 63, 63–64 (1999).

[143] Rolf Landauer, *The Physical Nature of Information*, 217 PHYSICS LETTERS A 188, 188 (1996).

[144] *Id*., and authorities cited therein.

[145] FOUNDATIONAL QUESTIONS INST., PROPOSAL REQUESTS, PHYSICS OF INFORMATION (2013), *available at* http://fqxi.org/data/documents/2013-Request-for-Proposals.pdf.

[146] *See* Roman Krzanowski, *Shannon's "Information" Revisited* (July 2016), *available at* https://www.researchgate.net/publication/304903301_Shannon_revisited. Claude Shannon's paper, *A Mathematical Theory of Communication*, available at http://math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf, is considered as the identifiable beginning of the field of information theory. *See* AFHAB ET. AL, INFORMATION THEORY AND THE DIGITAL REVOLUTION (2001), available at http://web.mit.edu/6.933/www/Fall2001/Shannon2.pdf.

[147] Our research has focused on academic research and publications available in the English and German languages. We fully acknowledge that scholarship or discussion connecting the physical quality of information to the regulation of data may exist in other languages. We welcome any suggestions on any additional research.

In contrast, the physical nature of data is beginning to influence other domains, notably information science as the basis for library operations.[148]

For our research purposes, *data*, *industrial data*, *personal information*, *factual data*, and *fictional data* each exist in tangible form. We make no distinction among different digital media and believe any such distinction would not be useful. What is important to accept is that the asset is tangible when recorded. Here are several examples to differentiate varying circumstances:

- In writing this paper, both authors are pressing keys that send electrical signals to the software application to create and display the image of each character. At the same time, the software application is storing the input; the data is the stored record. The result is the same, whether the storage is local to the laptop on which this paper is being composed, stored on a server to which a keyboard is connected within the college, or stored at a remote location maintained by a cloud services provider (such as a software company offering the application via the Internet). The record is *data.*
- The user's identity, and the usage behavior of that user with the application, may also be recorded as performance data relating to the user herself. Of course, based on the nature of that record, and its association with the user, *personal information* may also be created and stored.
- A sensor is a measuring device. It can be engineered to measure sound, frequencies, thermal energy, actions, or waves (of light or energy) as physical behavior. The sensor functions to convert the measured event into a record, an expression in digital form of the physical behavior that has been sensed. That expression, at the time the record is created, is now physical *data*. It is an example of *industrial data*. It exists, and the information contained in that record will be transmitted elsewhere or preserved. If the original data

[148] *See, e.g.*, David Bawden & Lyn Robinson, *"Deep Down Things": In What Ways is Information Physical, and Why Does it Matter for Information Science?*, 18 INFO. RES. 3 (2013), *available at* http://www.informationr.net/ir/18-3/colis/paperC03.html#.Wk_ont-nGHs.

is subsequently deleted, destroyed, or overwritten, it no longer exists as physical matter.[149]

- In complex automated business processes (including computational calculations), each step or element of the process is producing two outputs, each of which has unique physical status. First, the substantive output itself is created (e.g., the result of inputted data being calculated by an algorithm) and a record of that output is established. Second, the successful execution of the step or element also is recorded, usually in one or more logs, to create evidential support (i.e., factual data) the step or element was completed. The log data may or may not be associated with the specific output but provides an audit trail to the step's execution.[150] Each of these records would also be considered as *industrial data*.
- While pausing between drafts of this paper, an author went to an online entertainment provider to pay for and watch the latest episode of a popular fantasy fiction series. The browser, provider's website, and the author's bank all created records of the user's actions, most of which likely would include *personal information*. But, if observed and recorded without regard to identity (e.g., page selection and show previews viewed before log-in), those records are

[149] Of course, it is possible that copies of the data exist, and each copy is, itself, a separate physical asset. The law has long struggled with the ability of computers to create copies of records. *See generally* MICHAEL R. ARKFELD, ARKFELD ON ELECTRONIC DISCOVERY AND EVIDENCE (2005); Steven Goode, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1 (2009). For a British perspective, *see* INST. OF ADVANCED LEGAL STUDIES, ELECTRONIC EVIDENCE (Stephen Mason & Daniel Seng eds., 4th ed. 2017). In actuality, the full record, including all associated metadata, when encrypted and time-stamped, is physically unique. Recent technologies, such as blockchain-based ledgers, are overcoming the presumption that copies of specific data are indistinguishable. *See generally* EUROPEAN AGENCY FOR NETWORK AND INFO. TECH., DISTRIBUTED LEDGER TECHNOLOGY AND CYBERSECURITY (2017); Zach Church, *Blockchain Explained*, MIT SLOAN (May 25, 2017), http://mitsloan.mit.edu/newsroom/articles/blockchain-explained/; Jonathan Hassel, *What is Blockchain and How Does it Work?*, CIO (Apr. 14, 2016, 3:48 AM), https://www.cio.com/article/3055847/security/what-is-blockchain-and-how-does-it-work.html.

[150] Business process management (BPM) software solutions and business process engineering languages (BPEL) are important tools used in the creation of these types of performance and event logs.

> *industrial data.* The content of the episode would be *fictional data* (especially if dragons are involved!).

In viewing information as physical matter, and accepting that view as the foundation for a new way of thinking about property rights systems for data, the following observations can also be made. First, physical information can be very small. A single byte is sufficient to exist.[151] Advances in quantum computing are confirming that qubits also are now working in small, functioning computers.[152] Recognition of physical information as property does not require, in principle, any de minimis size requirement. That opens up all sorts of possibilities to enable our machines to track the existence and use of data with granularity that is not humanly possible. This transforms enforcement and compliance into behaviors that do not rely on human observation.

Second, classification of data is *not* derived solely from its actual content; the surrounding context (including the identity and role of the various actors, systems, applications, and functions each are performing) can affect how data is classified in order to apply advanced rules specific to a classification type. Unfortunately, with the exception of PII, no other formal classification methods exist around which rules regarding ownership, control, and use can be structured. Building those classification methods will be an important part of how the legal constructs for data evolve.

Finally, objective recognition of data as tangible matter, in whatever volume or size, opens the door to asking whether a) original creativity is required as a pre-condition to exercising legally recognized rights (such as those bestowed on copyright owners under U.S. law),[153] or b) whether a database creator has made sufficient investment in the database to be vested with *sui generis* database rights, as provided by the EU Database Directive.[154] Neither of those measures, as expressed in current laws, enable reliance on objective, automated mechanisms to establish ownership and the

---

[151] *See Byte*, ENCYCLOPAEDIA BRITANNICA, https://www.britannica.com/technology/byte (last visited Aug. 23, 2017) ("[A] byte [is] the basic unit of information in computer storage and processing. A byte consists of eight adjacent binary digits (bits), each of which consists of a 0 or 1.").

[152] *See* EVGENIY KIKTENKO ET AL., QUANTUM-SECURED BLOCKCHAIN (2017), *available at* https://arxiv.org/pdf/1705.09258.pdf.

[153] *See generally* Feist Publ'n Inc. v. Rural Tel. Serv. Co., 499 US 340 (1991); Assessment Techs. v. Wiredata, 350 F.3rd 640 (7th Cir. 2003); Craig Joyce & Tyler T. Ochoa, *Reach Out and Touch Someone: Reflections on the 25th Anniversary of* Feist Publications, Inc. v. Rural Telephone Service Co., 54 HOUS. L. REV. 257 (2016–2017).

[154] *See* Directive 96/9/EC, *supra* note 104, at Articles 7, et. seq.

subsequent exercise of the rights of ownership. This makes it difficult to imagine how the laws themselves will be capable of dynamic enforcement.

V. A PROPOSAL AND NEXT STEPS

Our proposal begins by answering the question, "When does data begin to exist?" We propose that data becomes real the moment it is recorded by electronic or digital means. At that point in time, something tangible exists that is new and different from the preceding moment in time. Data creation occurs through one of two methods—either a human user inputs instructions to create a data asset (such as pressure on a keyboard creating the letters of this paper in a digital format) or a machine executes a process that records new data of various classifications. The data may be a light impulse, an audio sound, a pixel within an image, or an entire digital photograph instantaneously captured and preserved. There is no necessity that the data itself be in perceivable form through the use of human senses; it is sufficient to have evidence the data exists (in other words, data about data that confirms its existence and state).[155] In order for the data to become subject to property rights, several other questions immediately become important to resolve:

- How is the data to be classified? What data about the data and surrounding context are required to calculate and establish the classification?
- When do the rights of ownership attach to the data? Does the answer vary based on how the data may be classified?
- What controls or constraints are relevant to the data based on its classification? How may those be effectively exercised?
- What rights or uses does ownership entitle an owner to exercise?

In contrast to existing legal standards associated with copyright and databases (through which the rights of parties in the content are based on subjective measures of creativity, originality or level of effort), we propose that the answers to each of the preceding questions must be capable of being computationally calculated in objective reliance upon sensor records and transactional data stored in metadata and associated logs. This is not such a

---

[155] *See* U.C.C. § 9-102(a)(70) (AM. LAW INST. & UNIF. LAW COMM'N 2010). The notion of "perceivable form" was introduced in the United States Uniform Commercial Code definition of "record," developed during the 1990's in response to accelerating electronic commercial practices. *See, e.g.,* U.C.C. § 1-201(b)(31) and U.C.C. § 2-201(b)(31). For a perspective on the considerations and dynamics involved in introducing the new definitions, *see* Patricia Brumfield Fry, *X Marks the Spot: New Technologies Compel New Concepts in Commercial Law*, 26 Loy. L.A. L. Rev. 607 (1993). The definition of "data," introduced *supra* Part I, allows the perception of the existence of data to be made by a machine.

radical notion; many laws and regulations are constructed around metrics generated by automated technologies (e.g., speed limits, particulate levels in factory emissions, concentration limits on certain chemicals and fertilizers, etc.). Our proposal extends that concept into the operation of complex information systems in which the rules of ownership-and rights-are electronically expressed and enforced. The rules will be enforceable based on measurements of behavior and actions taken (and not taken) within the systems and processes themselves.

Through various existing and foreseeable technologies, systems can be envisioned in which a) the data owner's property rights may attach to data at very early moments in the data's lifecycle, b) data classifications can be bound to the data (along with associated factual information regarding parties entitled to exercise constraints on downstream uses of a data asset, such as personal identity), and c) controls and constraints can be automatically applied and enforced. Across the vastness of cyberspace, both in the present and into the future, no other mechanisms are rational to consider. Stated differently, compliance and rights must become functions that are derived from mathematical calculations. To achieve that outcome, this article's proposed construct serves as a platform on which to build.

A. Attaching Ownership to Data

Once data exists as physical matter, the next question is, "When do the rights of ownership attach to the data?" As noted earlier, the rule of law for personal information does not provide any clear benchmark of when ownership does or does not attach to the information itself.[156] Yet, as described in Part II, there are growing international calls for ownership rights to be clearly defined for all data, including industrial data or personal information, in large part to facilitate increased transactional volume and revenue in data as the asset of the deals, whether for licensing, aggregation into data lakes, fostering innovation, or other analytical or creative purposes.

But, in attaching ownership rights to data, other ancillary issues immediately arise and must be considered: How can evidence of the attachment of ownership rights be recorded? What does that evidence consist of (as transactional data about the event of attaching ownership)? Does the ownership attach merely to the primary data (such as an entry in a database or the recorded output of a process) or does ownership also attach to the related event and process logs and associated transactional information (i.e., the provenance record for the primary data)? Does ownership include any data that was created in order to support the

[156] *See supra* Part III A.

classification of data which, in turn, attaches certain rights, controls, and constraints (such as those of a data subject relating to their PII)?

We propose that these questions, and the foundation for calculating when and how data rights attach, can be answered by modeling and extrapolating from existing legal systems for governing transactions tangible assets, including goods, real property, and documents of legal significance, such as chattel paper. In each of these systems, the same questions have been previously considered and robust, mature legal frameworks and commercial systems have evolved. In each, once ownership is established, ownership and other derivative rights can be transferred between separate parties in one or a series of separate transactions. A quick survey of current commercial practices confirms that transactions involving data are not inherently unique or different, except for the absence of the necessary predicate of defining how ownership attaches. We can extract some important generalized principles from these complex legal systems.

Most commercial legal systems precisely define "goods," and include agricultural commodities and manufactured products in those definitions. For example, in the U.S. Uniform Commercial Code (UCC), goods must be "existing, identified, and movable at the time they are identified, in order for any interest in them to pass."[157] Goods also includes the unborn young of animals, growing crops and other identified things that can be severed from real estate; however it is the tangible born animal or harvested crop that becomes the asset around which a transaction is built.[158]

- For data, the requirement the data "exists" is entirely suitable. All data is a record of an action taken, created and preserved in physical form, descriptive of an event, an action, a calculation, or the performance of a process. Data must exist to be capable of being owned.
- For transactions in data, there must be "identification." Data identification requires both classification (what type of data is it?) and description, sufficient to enable a transaction to be specific to the relevant data. Within computer technology, that can require a careful balance—descriptive identifications cannot be insufficient nor so overly detailed as to inhibit efficient processing.

---

[157] U.C.C. § 2-105(1)–(2) (AM. LAW INST. & UNIF. LAW COMM'N 2002).

[158] *Cf. United Nations Convention on Contracts for the International Sale of Goods*, UNCITRAL (Apr. 11, 1980), http://www.uncitral.org/uncitral/en/uncitral_texts/sale_goods/1980CISG.html (providing no explicit definition of "goods," but contemplating contracts for the supply of goods to be manufactured or produced).

- By contrast, for transactions in data, legal reforms to enable electronic commercial practices in which electronic assets are the focus of the transaction have confirmed that data need not be "movable"; as discussed below, a data transaction can be fully performed through a transfer of 'control.'[159]

With real property, most developed and developing economies have created rule systems through which ownership is defined based on physical descriptions of the real estate, and the records of ownership are the related contracts describing the transfer of title between buyer and seller, such as a deed. The integrity of those contracts, and the validity and priority of ownership, are confirmed by recordings of those contracts filed in public offices that serve as custodians for those records.[160] Ownership attaches through a specific legal process of formal transfer, and the priority of competing claims of ownership is established by considering the contracts and public records.

- For existing and foreseeable data transactions, as noted above by the "identification" requirement for goods, the subject of the transaction will also require description. It is now apparent that data descriptions must also include some means to either a) identify the system(s) on which the data is located (remember, if data is physical, it is always some "where"), or b) uniquely identify and describe the data to enable its location to be irrelevant, provided the other descriptive information elements can be proven to be accurate and connected to the subject data itself. While conventional discussions suggest data files can be duplicated, when properly enveloped or associated with related metadata and provenance, and bundled by suitable encryption or other controls, any data file can, in fact, be unique and incapable of perfect duplication.[161]
- While data title registries, particularly by public authorities, do not currently exist beyond those

[159] *Infra* notes 175-186.

[160] *See generally* RESTATEMENT (THIRD) OF PROPERTY (AM. LAW INST. 2001); *see also* HARPUM ET AL., THE LAW OF REAL PROPERTY (8th ed. 2012).

[161] *See generally infra* Part V of this article. New developments in blockchain, zero-knowledge proofs, and quantum cryptography suggest the uniqueness of a data asset are entirely foreseeable; however, the supporting detail in this article is beyond the scope of this article.

> associated with copyrighted materials, patents, and trade and service marks, the idea has, in fact, been proposed.[162] In many respects, blockchain functions as a similar registry, creating a cryptographically secure record of the contents, submitting party, and time-stamps for any data asset placed onto a blockchain.[163]

For documents with legal value, such as chattel paper, banks and financial service interests began in the 1990s to consider how ownership of legal documents such as chattel paper might be established and transferred if the legal documents were, themselves, electronic records. Prior to that time and continuing into the present day, the ownership of physical chattel paper was defined by the information appearing on the face of the chattel paper itself and, if offered as collateral to secure loans, by formal filings of notices.

A series of amendments to the UCC (and, in turn, U.S. federal statutes) provided the foundation for ownership and transfer of their electronic equivalents (including the rights to enforce the promises represented by chattel paper). In summary, those amendments and statutes offer the following key concepts, each of which support our proposal to apply property right systems to digital information.

First, "Record" is defined as "information that is inscribed on a tangible medium or which is stored in an electronic medium or other medium and is retrievable in perceivable form."[164] Next, "electronic chattel paper" is defined to consist of "chattel paper evidenced by a record . . . consisting of information stored in an electronic medium."[165] Together, these defined terms enabled the digital information to be classified and, in so doing, allowed rules for establishing and maintaining control of

---

[162] *See, e.g.*, Andreas Wiebe, *Protection of Industrial Data—A New Property Right for the Digital Economy?*, 12 J. INTELL. PROP. LAW & PRAC. 62 (2016); WOLFGANG KERBER, "INDUSTRIAL DATA RIGHT" AND INNOVATION? (2016), *available at* http://www.grur.org/uploads/tx_meeting/04_Kerber_GRUR_1506 2016_02_17.pdf.

[163] *See generally supra* note 145. General explanations of blockchain are abundantly available, and many current implementations are emphasizing the integrity of the records and the resulting "distributed ledger" as equivalent to the registry functions of government offices or other central authorities.

[164] U.C.C. § 9-102(a)(70) (AM. LAW INST. & UNIF. LAW COMM'N 2010). This definition was constructed to assure the equivalence of information stored in electronic media to tangible paper documents. This definition did not prescribe any defined structure, volume, or minimum requirements for a record, which enabled many requirements for records set forth in the U.C.C. to be satisfied by electronic files, whether or not relating to the chattel paper.

[165] U.C.C. § 9-102(a)(31) (AM. LAW INST. & UNIF. LAW COMM'N 2010). This definition emphasized it was the stored electronic record of the chattel paper's existence that became the focus of the following steps.

electronic chattel paper to be crafted and applied. These rules specified that a secured party (with a security interest in the chattel paper) "has control of electronic chattel paper if a system employed for evidencing the transfer of interests in the chattel paper reliably establishes the secured party as the person to which the chattel paper was assigned."[166] In turn, those rights of a secured party can be transferred to other secured parties by transferring the rights of control over the electronic chattel paper.

The integrated process of establishing control and enabling transfers has been expanded to enable transactions in other electronic transferable records, documents, or instruments. Building on the UCC reforms, U.S. federal law was enacted in 2000 to enable electronic promissory notes for loans secured by real property to become transferable records, including those executed using electronic signatures.[167] Then, in 2017, these concepts were integrated into a Model Law on Electronic Transferable Records was formally approved by the United Nations Commission on International Trade Law (UNCITRAL).[168]

A distinctive feature of this UN Model Law is the definition of "electronic record" and its specific focus on metadata and similar information. "'Electronic record' means information generated, communicated, received or stored by electronic means, including, where appropriate, all information logically associated with or otherwise linked together so as to become part of the record, whether generated contemporaneously or not."[169] This view of an electronic record highlights that metadata and other log data (if logically associated with or otherwise linked together to become part of the record) need not be generated at the

---

[166] U.C.C. § 9-105(a) (AM. LAW INST. & UNIF. LAW COMM'N 2010). The reliability test of 9-105(a) was one for which additional guidance is provided as to the specific facts that can be demonstrated to evidence the existence of control. *See* U.C.C. § 9-105(b) (AM. LAW INST. & UNIF. LAW COMM'N 2010). These are further discussed in the text accompanying *infra* notes 175-186. Co-author Jeffrey Ritter was substantially involved in the drafting of the revisions described here, serving as an advisor for the American Bar Association to the drafting committee for these revisions during much of the reform process.

[167] The Electronic Signatures in Global and National Commerce, also known as the 'E-Sign Act', Pub. L. No. 106–229, tit. II, § 201, 114 Stat. 473 (2000).

[168] For the final text of the Model Law, *see* U.N. COMM'N INT'L TRADE, UNCITRAL MODEL LAW ON ELECTRONIC TRANSFERABLE RECORDS, U.N. Doc. V.17-0543, U.N. Sales No. E.17.V.5 (2017), *available at* http://www.uncitral.org/pdf/english/texts/electcom/MLETR_ebook.pdf [hereinafter "MODEL LAW"]; *see also UN Commission on International Trade Law Adopts the UNCITRAL Model Law on Electronic Transferable Records*, U.N. INFO. SERV. (July 17, 2017), http://www.unis.unvienna.org/unis/en/pressrels/2017/unisl251.html.

[169] MODEL LAW, *supra* note 168, at Art. 2.

same time as the primary content, but may be generated either before or after. This concept is, in our opinion, quite constructive toward a more formal property rights system and enables how data will be classified and how the rules for managing that information can be identified to be associated with a specific electronic record by automated means. In other words, the records of ownership and control can exist independent of the asset itself (which is no different than a land registry or the filing systems used to give notice of security interests).

The UNCITRAL Model Law also addresses the notion of what may be an "original," noting in their work papers that electronic transferable records are meant, by their own nature, to circulate.[170] The Model Law achieves the goal of preventing multiple claims of originality by relying on concepts of "singularity" and "control" that allow both the person entitled to enforce the note (or similar electronic asset) and the object of control to be identified in a unique, secure manner.[171]

This Model Law (as well as the U.S. enactments) articulates attributes and processes that can apply to any data; the definition of "electronic record" is not limited to the digital equivalents of transferable documents or instruments.[172] First, these laws anticipate that markets will want to achieve transferability of the digital versions of physical transferable documents; indeed Article 10 of the Model Law defines the conditions with which an electronic record satisfies legal requirements for a physical transferable document or instrument.[173] Article 17 expressly allows an electronic transferable record to replace a physical document "if a reliable method for the change of medium is used."[174] Current digital practices, and the calls for data ownership, emphasize that data has become something for which the value is increased by its transferability and utility in multiple environments, systems, and contexts. As evidenced by many big data analytics developments, data in any volume is capable of being licensed, transferred, and divided into downstream revenue opportunities in

---

[170] Note by the Secretariat, Draft Model Law on Electronic Transferable Records, A/CN.9/WG.IV/WP.139, at para. 81–82, available at http://www.uncitral.org/uncitral/en/commission/working_groups/4Electronic_Commerce.html. For additional working documents tracing the evolution of the Model Law, *see Working Group IV*, UNCITRAL, http://www.uncitral.org/uncitral/en/commission/working_groups/4Electronic_Commerce.html (last visited Jan. 6, 2018).

[171] Note by the Secretariat, *supra* note 170, at para. 82.

[172] MODEL LAW, *supra* note 168, at Art. 2.

[173] *Id*. at Art. 10. Art. 7(1) provides further reinforcement that "[a]n electronic transferable record shall not be denied legal effect, validity or enforceability on the sole ground that it is in electronic form." *Id*. at Art. 7(1).

[174] *Id*. at Art. 17.

the same manner as other legally valued electronic records, all while ownership continues to be claimed by the original custodian.

Second, the laws anticipate that transferability of unique data assets (where only one party can have enforceable rights with respect to electronic chattel paper) can be achieved by defined processes that transfer control of the digital asset versus transfer of the physical asset, for which many existing commercial laws exist.[175] A property rights system for electronic information could effectively leverage the legal structures that have already been developed for electronic records and how control is used as a mechanism for enabling market-based transactions. A single byte of data, once recorded on any electronic medium, is merely a smaller electronic asset for which ownership could be established.

B. Attaching Ownership – The Exercise of Control

We propose that the rights of ownership for specific data attach at that point in time and process at which an entity establishes *control* of the data. This concept, which largely tracks the reforms for electronic chattel paper and transferable records, requires elaboration (which follows below), but the principle both leverages and contrasts against some established legal principles in copyright and database law in two fundamental ways.

First, there is no requirement that the data be complete, sensible, or a finished product. This is consistent with copyright law: the related rights do not require a formal notice or registration and copyright attaches at the time of creation, even to works in process.[176] So, too, can rights of ownership attach to any data at the time of its creation, even if the record is itself partial or incomplete.

---

[175] For example, in the Uniform Commercial Code enacted among the states, Articles 3 (Negotiable Instruments) (defining the rights of holders and holders in due course), 4 (Bank Deposits and Collections) (defining the rights of holders of check items), 5 (Letters of Credit) (defining the rights of presenters and issuers of letters of credit), 7 (Documents of Title) (defining the rights relating to the negotiation of warehouse receipts and bills of lading) and 8 (Investment Securities) (defining the rights of those in possession of security certificates) all directly regulate the processes by which physical documents can be transferred as well as the legal consequences. U.C.C. §§ 1-101 to 9-709 (AM. LAW INST. & UNIF. LAW COMM'N 2012).

[176] *See* 17 U.S.C. § 101 (2010) (defining a work as "fixed" when it is captured in a sufficiently permanent medium that the work can be perceived, reproduced, or communicated for more than a short time). This notion is comparable to data being created and controlled; there must be some basis of permanency to the data itself. For example, data that consists of log inputs which, within a few milliseconds, are forever overwritten and destroyed would not be within the scope of the proposal.

Second, there is no expectation here that creativity or original work of authorship, or any level of effort of an undefined degree, is required. In this respect, data ownership is comparable to the EU database protection and not consistent with the U.S. view that mere statements of facts are not copyrightable.[177] What matters is the physical existence of the data and the establishment of initial control.

C. Establishing Control

Common law systems favor possession and physical control of goods or real property as factual considerations from which to begin evaluating ownership and the lawful exercise of the rights of ownership.[178] But, for electronic commerce and for data as property, the UN Model Law and U.S. legal reforms offer *control* as an equivalent indicium from which those rights may be exercised. What are those indicia? If we merely substitute a) "a person" (which may be a corporation or individual) for "secured party," and b) "data" for either "electronic chattel paper" or "electronic transferable record," the remaining statutory language might be further modified to read as follows:[179]

> A person owns data when the person establishes control of the data.
>
> A person has control of data if a system employed for recording and evidencing the transfer of interests in the data reliably establishes the person as the owner or the person to which control was assigned.

---

[177] *See id*.; *see also* Feist Publ'n Inc. v. Rural Tel. Serv. Co., 499 US 340 (1991); Assessment Techs. v. Wiredata, 350 F.3rd 640 (7th Cir. 2003); Craig Joyce & Tyler T. Ochoa, *Reach Out and Touch Someone: Reflections on the 25th Anniversary of* Feist Publications, Inc. v. Rural Telephone Service Co., 54 HOUS. L. REV. 257 (2016–2017). As discussed earlier, data ownership systems must be capable of being automatically operated, and the subjective standards that characterize copyright and database legal protection are not functional across complex information systems.

[178] *See* JOHN E. CRIBBET & CORWIN W. JOHNSON, PRINCIPLES OF THE LAW OF PROPERTY 12–13 (1962); In re Garza, 984 S.W.2d 344, 347 (Tex. App. 1998) (citing RALPH E. BOYER, SURVEY OF THE LAW OF PROPERTY 679–80 (3rd ed. 1981)).

[179] The language is modified from U.C.C. § 9-105 (AM. LAW INST. & UNIF. LAW COMM'N 2010). Similar language exists in the E-Sign Federal law and the UNCITRAL MODEL LAW with minor variations not directly relevant to the proposal at this stage. *See* MODEL LAW, *supra* note 168, at Art. 12 (emphasizing reliability, data integrity, preventing unauthorized access, security, audit, and third-party confirmation of reliability).

> A system satisfies [the definition of control], and a person is deemed to have control of a data record,[180] if related records are created and stored in such a manner that:
>
> (1) a single authoritative copy of the data exists which is unique, identifiable, and, except as provided below, unalterable;
>
> (2) the authoritative copy identifies the owner as the owner of the data;
>
> (3) the authoritative copy is communicated to and maintained by the owner or its designated custodian;
>
> (4) copies or amendments that add or change an identified transferee of the authoritative copy can be made only with the consent or prior approval of the owner;
>
> (5) each copy of the authoritative copy, and any copy of a copy, is readily identifiable as a copy that is not the authoritative copy; and
>
> (6) any amendment of the authoritative copy is readily identifiable as authorized or unauthorized.

Under this set of rules, more is needed than mere data creation in order for ownership rights to *attach* in a manner that could be legally defensible. There must be a system used that enables the owner to record the fact that their control of that data has been established and in a manner that satisfies how control is defined. The Model Law provides that a transfer of "control" for electronic transferable records is legally sufficient to meet any requirement for, or permitted transfer of, physical possession of transferable documents.[181]

For self-contained systems currently used inside a company or organization, many different commercial information governance and records management systems might be fully satisfactory. But more is needed across the complexity of today's IT environments, which have systems of systems through which data passes across multiple firewalls and system perimeters. Here are some examples:

- A company outsources its business software applications to use a cloud software-as-a-service provider. The data, when keyed in during normal user activity, is immediately stored on the service provider's servers or, perhaps, transferred to the servers of a subcontractor to the service provider. In these circumstances, the contract(s) become vital tools

[180] *See* 15 U.S.C. § 7021(c) (2000).
[181] MODEL LAW, *supra* note 168, at Art. 11.

for confirming ownership and control of the data by the licensee company.

- Many big data licensing deals involve transferring copies of selected data to third-party analytics firms. If those copies might be recorded by a system that tracks control, as contemplated above, the rights of the analysts, as well as the original corporate contributor of the data, could be more rationally differentiated and administered.
- While the source data inputted might have multiple originating owners that have transferred control of copies to the analytics firm, the output of the analytics is new data, created by the analytics firm. Now, all parties (contributors of original copies, the analytics firm, and their customers for the output) must articulate their respective rights in that output. Contracts are the governance and enforcement vehicles, but the identification and exercise of rights with respect to the output data pursuant to the agreement can be automated into the relevant control systems.

The Model Law introduces an intriguing path forward in determining how the sufficiency of systems delivering control are to be evaluated. In seven different articles, the legal standard by which to measure a specific method is one of reliability.[182] In support of those references, Article 12 articulates a general reliability standard, directing that a method shall be "as reliable as appropriate for the fulfilment of the function for which the method is being used, in the light of all relevant circumstances."[183] This standard, of course, like many common law rules, invites the potential for nearly endless debates as to whether particular methods employed for a specific transaction were "reliable." But Article 12 goes further, identifying an illustrative listing of circumstances that may be relevant.[184]

---

[182] *Id*. at Arts. 9–17.
[183] *Id*. at Art. 12(a).
[184] The list includes:
(i) Any operational rules relevant to the assessment of reliability; (ii) The assurance of data integrity; (iii) The ability to prevent unauthorized access to and use of the system; (iv) The security of hardware and software; (v) The regularity and extent of audit by an independent body; (vi) The existence of a declaration by a supervisory body, an accreditation body or a voluntary scheme regarding the reliability of the method; (vii) Any applicable industry standard.
Id.; *see also id.* at Art. 12 cmt. 122–39.

The practical effect of this listing is to create a template against which any method must be designed. In other words, any method that does not proactively incorporate operational rules for assessing reliability, assuring data integrity, preventing unauthorized access, securing hardware and software, requiring regular and extensive audits, securing accreditation, and complying with applicable industry standards is easily challenged as being insufficiently reliable. Looking forward, our proposal for how to expand the concepts of control into enabling new markets should surely build upon, and be measured against, the same template elements to improve the likelihood of early successes.

Article 12 offers another alternative. Under 12(b), a method can be reliable if "proven in fact to have fulfilled the function by itself or together with further evidence." As explained in the Explanatory Note, this provision is similar to one used for demonstrating the functional equivalence of electronic signatures to physical signatures under the Electronic Communications Convention.[185] If a method can be proven to have worked as intended, reliability need not be the basis of frivolous litigation.[186] This concept is also important, particularly if market participants commit to, and actively use, a specific method to maintain control across many different transactions; their prior conduct confirms the reliability of the systems, foreclosing further disputes.

After years of negotiation at the United Nations, the Model Law offers a governance structure that is well-suited to enable how ownership in data might be defined and ownership rights attached (and subsequently transferred). As well, those derivative rights can themselves be expressed in metadata or other information "logically associated with or otherwise linked together so as to become part of the record, whether generated contemporaneously or not."[187]

The finalization of the Model Law delivers a strong, international platform upon which our proposed model can expand. In other words, the proposal here is intended to leverage and enable agreements that connect commercial transactions working across multiple national boundaries. The foundation is already in place to do so as a result of the Model Law.

Formulating a legal structure that is scalable and extensible for data on a global basis into the foreseeable future certainly will require many

---

[185] *Id*. at Art. 12 cmt. 136–137. *See* U.N. COMM'N INT'L TRADE L., UNITED NATIONS CONVENTION ON THE USE OF ELECTRONIC COMMUNICATIONS IN INTERNATIONAL CONTRACTS, U.N. Doc. V.06-57452, U.N. Sales No. E.07.V.2 (Jan. 2007), *available at* http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf.

[186] MODEL LAW, *supra* note 168, at Art. 12.

[187] *See* MODEL LAW, *supra* note 168, at Art. 2 (defining "electronic record").

nuances and adjustments. The reliability criteria of Article 12(b) in the Model Law suggest a good inventory of the work ahead. Our proposal, however, remains grounded in the simple truths that a) data is physical matter, and b) legal reforms at the international level have already been formulated that migrate traditional legal rules based on physical records into the more electronically enabled commercial practices of the present. Leveraging those rules to advance a property rights system applicable to all data *is* possible.

D. Reconciling Existing Privacy Laws

As noted earlier, privacy laws have often been the intense focus of academic debate as to whether property rights systems were appropriate for personal information. In our analysis of the related scholarship, the view often was one of either/or—personal information must be governed by either a property rights system or a torts-based system (with the latter being viewed as the prevailing model). We believe there is a way in which the rights of data subjects can be accommodated within the larger framework of a property rights system for all data.

As noted earlier, to assert control, data must be both identified and classified. As a practical matter, those actions are now entirely automated. But once data is classified as PII, the owner can still be immediately subject to the same constraints imposed by current privacy laws on how the PII may be used and transferred. Indeed, that is no different than current legal systems, other than that the ownership of the PII by the collecting entity (i.e., controller) is now explicit, rather than inferred.

Defining ownership does not derogate from the ability of data subjects to still exercise tort-based rights and remedies if controllers or processors violate the terms of consents that are given. Concepts of clear ownership are useful, as well, to the negotiating position of a data subject; if they wish to explicitly retain ownership of the identifiable data relating to them, that can be an express topic in the negotiations which notices and consents under current law theoretically enable (as well as the possible consideration payable to the data subject for the transfer of ownership to occur).[188]

---

[188] *See, e.g.*, WORLD ECON. FORUM, UNLOCKING THE VALUE OF PERSONAL DATA: FROM COLLECTION TO USAGE (2013), *available at* http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf; Cassandra Liem & Georgios Petropoulos, *The Economic Value of Personal Data for Online Platforms, Firms, and Consumers*, LSE BUS. REV. (Jan. 19, 2016), http://blogs.lse.ac.uk/businessreview/2016/01/19/the-economic-value-of-personal-data-for-online-platforms-firms-and-consumers/ (reporting on the calculation of advertising revenues per user (ARPU) reported by major online providers such as Google and Facebook); Jeff Desjardins, *How Much is Your*

For example, from this point forward, many electronic consumer products, including automobiles, will become data collection devices.[189] For each, we envision that a property rights framework allows explicit recognition of a) the product itself (such as the car), and b) the future data streams (both of industrial data and personal information) the product will produce. The sensor networks within cars and trucks certainly can associate some data to the operator of the vehicle, which becomes personal information subject to normal law. But much of the data those networks will collect has primary industrial value—predicting maintenance repair needs, improving innovation, identifying time to failure for specific components—which is valuable to car manufacturers, component suppliers, and service networks irrespective of the identity of the human operator. How is ownership of that future data defined? In Germany, the ministry of transport and digitalization defines the ownership of data created by automobiles as follows:

> Die Verfügungsrechte an Daten sollen demjenigen zugewiesen warden, auf den die Erstellung der Daten zurückgeht. Damit gilt im Grundsatz: Die Daten und damit verbundene Rechten gehören den Menschen – bei Fahrzeugdaten etwa dem Halter,[190] der das Fahrzeug erworben hat.[191]

Personal Data Worth?, VISUAL CAPITALIST (Dec. 12, 2016, 11:30 AM), http://www.visualcapitalist.com/much-personal-data-worth/ (reporting nine key data brokers realized $426 million in annual revenues, as of 2012). Significant research that has been conducted on the economic value of PII to data subjects, both amounts payable to secure clear rights of use, as well as the downstream revenues PII generates from which data subjects are normally excluded in the marketplace. For an interesting calculator used to calculate the value of an individual's data, *see* Emily Steel et al., *How Much Is Your Personal Data Worth?*, FIN. TIMES (June 12, 2013), http://ig.ft.com/how-much-is-your-personal-data-worth/. In contrast, for industrial data, the "monetization" of data in commerce is driving entirely new innovations in how accounting practices (and others) measure and express the economic worth of information. *See* Hedge, *supra* note 9.

[189] *See* Matthew Wilson, *BMW and IBM Team Up for Cloud-Connected CarData Network*, IBM (June 16, 2017), https://www.ibm.com/blogs/cloud-computing/2017/06/bmw-ibm-cloud-cardata/; Federico Guerrini, *BMW Partners With IBM to Add Watson's Cognitive Computing Capabilities to Its Cars*, FORBES (Dec. 15, 2016, 9:44 AM), https://www.forbes.com/sites/federicoguerrini/2016/12/15/bmw-partners-with-ibm-to-add-watsons-cognitive-computing-capabilities-to-its-cars/#2e1257841a90. In June 2017, BMW and IBM announced a joint initiative to develop a cloud computing project linking different operating networks and data sources. The press release emphasizes the consent-based rights of the drivers to allow the collection and use of the data. https://www-03.ibm.com/press/us/en/pressrelease/52595.wss#release.

[190] Minister Alexander Dobrindt's approach to define the collected data as property of the car owner opens new discussions how the regulation of data ownership has to

Recall that unborn animals and growing crops are not yet classified as goods under the Uniform Commercial Code. Future data streams are similar; they do not yet exist, though their attributes, sources, and structures are predictably identifiable as byproducts of the design of the related technologies. For these future data streams, legal solutions similar to those for future goods can be deployed. A sale of future data can be structured, with the related agreements defining when control of the future data will commence and, if so negotiated, will be transferred, with details emphasizing the systems, processes, and records on which the parties shall rely.

In many respects, companies that see their operating data acquired by cloud-based service providers are situated no differently with respect to their data than data subjects are with respect to their personal information. We believe the preceding balances work just as effectively for both industrial data gathered by third parties from the operations of a company and PII gathered with respect to individual data subjects.

E. Allocating the Risks of Fictional Data

Recall that Part I of this paper introduced the terms "factual data" and "fictional data." In doing so, our focus was not on copyright protection for fictional works, including those in digital form. For those works, copyright law generally provides sufficient enforcement. Instead, we were contemplating how to address situations in which industrial data fails to pass relevant tests for assuring its authenticity as factual information.[192] As noted earlier, the U.S. Supreme Court concluded copyright law does not protect mere listings of "factual information."[193] But the analysis in that case, focused on telephone directory listings, did not require the Court to provide a measure of when data intended as factual is, in truth, fictional.

---

take into consideration how this approach fits to leased cars or the increasing number of shared cars.

[191] [The right of disposal shall be allocated to the data supplier. In principle this means: Data and the attributed rights belong to persons - in the case of vehicle data, to the registered keeper respectively owner of the car.] *See* BUNDESMINISTERIUM FÜR VERKEHR UND DIGITALE INFRASTRUKTUR, *supra* note 20.

[192] The issue occurs at any point in the information lifecycle of data. Of course, many security techniques exist to help verify the continued authenticity of information and protect the data from malicious conduct that seeks to manipulate the information itself. But the consequences of how to allocate responsibility for either the failure of security controls to be applied, or the ability to protect data across the larger commercial ecosystems in which data now circulates, remain significant commercial issues.

[193] *See* Feist, *supra* note 102.

A traditional warranty made in corporate acquisitions will require the seller to verify the integrity and authenticity of the information on which the transaction is based; similar warranties for data, structured into purchase agreements, licenses, and other commercial arrangements can be easily contemplated. But, where is the line of demarcation among the parties for how and where to transfer their responsibilities?

The *control* concept can be useful to define that line of demarcation. When control is transferred, so too can the responsibility for assuring the factual integrity of the subject data be transferred. Stated differently, the original owner, on asserting control, assumes the responsibility for sustaining the integrity of the data, and retains that responsibility until control is transferred.[194] Thus, the chain of title and control allow the chain of responsibility for data integrity to follow along in parallel.

While a full expression of how copyright laws should be reformed to support the Digital Age is beyond the scope of the paper, we suggest that copyright law could be conformed to protect fictional data as fully as possible, and enable property rights in industrial data and personal information (all of which is also factual data, including analytical output derived therefrom) to be explicit and governed by appropriate, unique controls such as proposed here.

F. Enabling Technologies

This proposal has been developed taking account of known, emerging technologies, notably blockchain distributed ledgers and zero-knowledge proofs, as well as existing cryptographic tools for securing the integrity of data.[195] We fully believe the proposal can be sustained with

---

[194] An astute lawyer might argue the original owner can only assure the integrity of the data collected by the related sensors, but disclaim responsibility for the accuracy of the sensors themselves. That secondary responsibility for the accuracy of the sensors becomes part of the negotiation for the purchase or use of the sensors.

[195] We note that Estonia, briefly surveyed in Part II, is proceeding forward with blockchain at the governmental level. *See, e.g.*, *Blockchain Technology in Estonia: What Happens at Governmental Level*, GLOBAL BANKING AND FIN. REV. (Mar. 8, 2017), https://www.globalbankingandfinance.com/blockchain-technology-in-estonia-what-happens-at-governmental-level/. Zero knowledge proofs ("ZK proofs") enable one party to mathematically prove the truth of an assertion about an asset to a second party (such as a seller describing a data asset to a buyer) without exposing the asset to the second party. Imagine buying a new automobile and being able to mathematically be convinced every statement about the attributes of the automobile are factually accurate. ZK proofs enable that outcome. ZK proofs are being actively explored in today's innovative maelstrom for data assets, including those secured on blockchain-based ledgers. *See, e.g.*, Nelson Petracek, *What Zero-*

these technologies, as well as improved as next generations of quantum-based cryptography are introduced (In-depth discussion of these technologies is beyond the scope of this paper).

Blockchain is, however, already being considered in the automotive industry. Online reports of initiatives by Toyota highlight that the technology may allow for pooling and sharing data among owners, fleet managers, manufacturers, insurance companies, and other stakeholders.[196] But, in those types of circumstances, the fundamental questions of ownership (and the related rights to control access, use, and further distribution or reuse) have not yet been resolved.

We believe the answers, when structured around identification, classification, and exercise of control, become entirely feasible to contemplate and structure into the existing web of commercial agreements among the varied stakeholders. Indeed, among the manufacturers and suppliers of components equipped with sensors, and software applications that create, process, store, or communicate data from a vehicle, the ownership and use of related industrial data will quickly become a commercially vital variable in their relationships.

CONCLUSION AND NEXT STEPS

Cognizant of international policy and industrial calls for explicit legal rights to own data, our research examined more closely the classifications of data on which those calls were focused. A classification scheme was developed and applied through new definitions that allow various distinctions to be made in evaluating how to build a construct of property rights for data.

The automotive industry was selected as a focal point of our analysis and, indeed, significant momentum was identified in that industry, in both Europe and Asia, to develop property rights principles, including in commercial agreements. Currently enacted laws and academic scholarship were surveyed to determine if two principles on which the proposed new construct is based have, in any degree, been recognized: namely the physical nature of data and the manner of attaching ownership to all

---

Knowledge Proofs Will Do for Blockchain (Dec. 16, 2017, 2:41 PM), https://venturebeat.com/2017/12/16/what-zero-knowledge-proofs-will-do-for-blockchain/.

[196] Philip E. Ross, *Toyota Joins Coalition to Bring Blockchain Networks to Smart Cars*, IEEE SPECTRUM (May 24, 2017, 2:02 PM), http://spectrum.ieee.org/cars-that-think/computing/networks/toyota-joins-coalition-to-bring-blockchain-networks-to-smart-cars; *see also Toyota Explores Blockchain Tech in Autonomous Cars*, AUTO. FLEET (May 22, 2017), http://www.automotive-fleet.com/channel/safety-accident-management/news/story/2017/05/toyota-explores-blockchain-tech-potential.aspx.

classifications of data through automated systems exercising control. Based on our research, we concluded those principles have not been recognized for data as a separate property classification. However, we also noted that economic models are advancing to monetize data as property that would benefit from greater clarity of ownership.

On the basis of the preceding, a construct is proposed to recognize ownership of data at the moment of creation and to enable ownership to attach to data through automated systems exercising control. Once ownership is attached through digital systems, the rights, privileges, controls, and constraints by which the subject data can be used may be expressed and enforced through electronic contracting mechanisms that are already in place across vast sections of the global marketplace. The suitability of that construct was considered, taking into account existing privacy laws and intellectual property protection laws, and we concluded that those laws can be reconciled with the notions of data ownership.

Since the 1980s, legal reforms to harness the potential of digital technologies have occurred with astonishing speed, particularly in comparison to the evolution across humankind of certain other established principles and governance concepts! Our collective experience during that time period confirms that legal solutions work best which deliver predictable, scalable, and extensible mechanisms for enabling new kinds of digital transactions. This article's proposal is designed to achieve those outcomes by leveraging and adapting appropriate legal structures that have already been negotiated and adopted by consensus, both in U.S. legal systems and, more recently, at the United Nations.

In other words, the consensus-based orientation of good rulemaking for electronic commercial practices has already produced useful work product that can, in turn, support the next steps needed to build additional rules and market mechanisms that will scale across nation-state, regional, and industry-specific solutions. The German and Japanese industry-specific materials referenced in this paper indicate the collaborations and potential to achieve even more are already underway. The Estonian digital government advances illustrate the applicability and potential at the nation-state level.

The next steps are not insubstantial in number or degree. Greater precision will be needed, and existing information governance and information security technologies and innovations must be considered more closely to assure that their adaptability to enable the proposal can be accomplished. But our hope is that the proposal made here will stimulate a more focused discussion on how ownership can be created, attached, and exercised to most fully advance the potential of our Digital Age.

Jeffrey Ritter
Testimony, US Senate Committee on
Banking, Housing, and Urban Affairs
October 24, 2019

Annex C

A hard copy of Achieving Digital Trust: The New Rules for Business at the Speed of Light has been delivered to the Committee staff as part of this written testimony.