Selling Your Data Without Selling Your Soul

Privacy, Property, and the Platform Economy

By Chris Berg and Sinclair Davidson

October 2019

ISSUE ANALYSIS 2019 NO. 4

COMPETITIVE ENTERPRISE INSTITUTE

CEI

Selling Your Data Without Selling Your Soul

Privacy, Property, and the Platform Economy

By Chris Berg and Sinclair Davidson

Executive Summary

Humans have always sought to defend a zone of privacy around themselves—to protect their personal information, their intimate actions and relationships, and their thoughts and ideas from the scrutiny of others. However, it is now common to hear that thanks to digital technologies, we now have little expectation of privacy over our personal information.

Meanwhile, the economic value of personal information is rapidly growing as data becomes a key input to economic activity. A major driver of this change is the rise of a new form of business organization that has come to dominate the economy—platforms that can accumulate and store data and information are likely to make that data and information more valuable.

Given the growing economic importance of data, digital privacy has come to the fore as a major public policy issue. Yet, there is considerable confusion in public debates over the meaning of privacy and why it has become a public policy concern. A poor foundational understanding of privacy is likely to result in poor policy outcomes, including excessive regulatory costs, misallocated resources, and a failure to achieve intended goals.

This paper explores how to build a right to privacy that gives individuals more control over their personal data, and with it a choice about how much of their privacy to protect. It makes the case that privacy is an economic right that has largely not emerged in modern economies.

Regulatory attempts to improve individual control over personal information, such as the European Union's General Data Protection Regulation (GDPR), have unintended consequences and are unlikely to achieve their goals. The GDPR is a quasi-global attempt to institute privacy protections over personal data through regulation. As an attempt to introduce a form of ownership over personal data, it is unwieldy and complex and unlikely to achieve its goals. The GDPR supplants the ongoing social negotiation around the appropriate ownership of personal data and presents a hurdle to future innovation.

In contrast to top-down approaches like the GDPR, the common law provides a framework for the discovery and evolution of rules around privacy. Under a common law approach, problems such as privacy are solved on a case-by-case basis, drawing on and building up a stock of precedent that has more fidelity to real-world dilemmas than do planned regulatory frameworks.

New technologies such as distributed ledger technology—blockchain—and advances in zero-knowledge proofs likewise provide an opportunity for entrepreneurs to improve privacy without top-down regulation and law.

Privacy is key to individual liberty. Individuals require control over their own private information in order to live autonomous and flourishing lives. While free individuals expose information about themselves in the course of social and economic activity, public policy should strive to ensure they do so only with their own implied or explicit consent.

The ideal public policy setting is one in which individuals have property rights over personal information and can control and monetize their own data. The common law, thanks to its case-by-case, evolutionary nature, is more likely to provide a sustainable and adaptive framework by which we can approach data privacy questions.

Legal rights to privacy are underdeveloped because governments do not want to recognize any rights to privacy against themselves.

Introduction

It is increasingly common to hear that we live in a post-privacy world—that the combination of the data economy, voluntary disclosure on social media, pervasive Internet of Things, and national security surveillance represents the end of the divide between public and private. As venture capitalist and tech entrepreneur Nova Spivack wrote in 2013:

> Privacy is dead. … We are now entering the Age of Transparency, an era of increasing openness at all levels of society. … Given that secrets will become ever more difficult and costly to protect, our expectation of privacy has to evolve. We have to accept that it's impossible and unrealistic to achieve total privacy, and furthermore there are compelling benefits to being less secretive, even on the individual level.[1]

Humans have always sought to defend a zone of privacy around themselves—to protect their personal information, their intimate actions and relationships, and their thoughts and ideas from the scrutiny of others. Yet in many respects, we seem to be no closer to resolving the challenge of protecting privacy in an increasingly connected world. In this paper we explore this challenge and propose some approaches to addressing it. We argue that there is considerable confusion in public debates over the meaning of privacy and why it has become a public policy concern. A poor foundational understanding of privacy is likely to result in poor policy outcomes, including excessive regulatory costs, misallocated resources, and a failure to achieve intended goals. In addition, a new form of business organization has come to dominate the economy—platforms that can accumulate and store data and information are likely to make that data and information more valuable.

We explore the notion of privacy as a market failure, in the neoclassical economic meaning of the term. We argue that privacy is an economic right that has largely not emerged in modern economies. There are two reasons for this. First, most private information is simply not valuable. Second, in many instances secrecy is not a desirable feature when engaging in transactions. More importantly, legal rights to privacy are under-developed because governments do not want to recognize any rights to privacy against themselves. In sum, confusion over the definition and scope of privacy, combined with government hostility toward the notion of privacy in the economic and political spheres, results in poor policy outcomes.

Ironically, the value of private information is increasingly due to the

technological changes that could undermine privacy itself. Yet, government regulation would make the problem worse. Below we examine the European Union's General Data Protection Regulation (GDPR), which came into force in 2018. The GDPR is a quasi-global attempt to institute privacy protections over personal data through regulation. As an attempt to introduce a form of ownership over personal data, it is unwieldy and complex and unlikely to achieve its goals. As we outline, the GDPR supplants the ongoing social negotiation around the appropriate ownership of personal data and presents a hurdle to future innovation.

The inadequacy of complex regulatory solutions for addressing the privacy problem is clearest when we consider the pace of relevant technological change. Mainstream interest in the protection of personal data is extremely recent—many of the services that are controversial are less than a decade old. The technological privacy challenges of 2019 are sharply different from the privacy challenges of 2009, and in ten years they will be significantly different again. Thus we conclude the paper with a consideration of distributed ledger technology—blockchain—as one possible tool under development that can reshape control of personal data.

Entrepreneurs should continue to experiment with business models that add value to personal information, and policy makers should let them. Government intervention that impedes this process of trial and error among actors in the market is likely to undermine individuals' ability to either monetize their personal information or gain from trade in their personal information.

Entrepreneurs should continue to experiment with business models that add value to personal information, and policy makers should let them.

The Increasing Ubiquity of Data

> *Your bank account, your health record, your genetic code, your personal and shopping habits and sexual interests are your own business. That information has a value. If anybody wants to pay for an intimate look inside your life, let them make you an offer and you'll think about it. That's opt in. You may decide to trade the desired information about yourself for services like an E-mail box or stock quotes or other inducement. But require them to ask you first.*
>
> *– William Safire, 1999*[2]

Data is an increasingly significant part of the modern global economy. Digital infrastructure relies on the accumulation and analysis of vast quantities of machine-readable information. Future technological changes such as automation and artificial intelligence promise significant improvements in living standards, but will require significant volumes of data for machine learning and training. The

The data that are produced, shared, and collected by firms and governments as we go about our digital lives—even indavertently—create a complex picture of our preferences, habits, and desires.

medical advances of the future will have artificial intelligence features that will require personal data to function. "Smart cities" promise better and more responsive infrastructure and service delivery through the harvesting of information from sensors embedded in everything from buildings to garbage bins.

At the same time, individual consumers and citizens currently have little control over information about themselves. This is due to the inherent non-rivalrous nature of information. Recent scandals about data breaches and the seeming misuse of personal data held by firms and governments have created a clear sense of crisis around privacy and personal data ownership. Smart city devices—such as the Wi-Fi-enabled "smart bins" installed in London for the 2012 summer Olympics—have been caught collecting personal information about passersby.[3] Social media services have allowed software developers access to personal data without users' consent.

At the beginning of the age of social media, it was common to think of privacy challenges as the sharing of embarrassing information without consent—such as posting an embarrassing photograph that could adversely impact an individual's employment options. In the 20 years since columnist William Safire wrote, in the early Internet era, that personal information is valuable and should be owned by the individual, public concern and interest in privacy has grown. While these problems are still salient— particularly concerning the sharing of sexually explicit personal images without consent—it is now recognized among the general public and policy community that the privacy challenges are more general.

The data that are produced, shared, and collected by firms and governments as we go about our digital lives—even inadvertently—create a complex picture of our preferences, habits, and desires. The deep integration of the Internet into our daily lives means that we interact with digital providers for our employment, our hobbies, our relationships with family and friends, our legal and regulatory responsibilities, and even for our sexual habits and medical challenges. For example, a simple Internet search history provides what one scholar describes as a "metaphorical X-ray photo of one's thoughts, beliefs, fears, and hopes."[4]

By comparing our digital activities with the aggregate data collected from other users, digital firms make predictions about how to personalize advertisements and product offerings. In some circumstances, these prediction engines can make complex predictions about our lives that we may not be aware of. Even brick and mortar firms can predict major, personal life events like pregnancies

solely from purchasing data.[5] These predictions are not always on point. Every Internet user is familiar with the experience of seeing advertisements for products they have already purchased online, or for life events like pregnancies that have already passed.[6] Thanks to the combination of the increased digitization of our lives and more powerful artificial intelligence and machine learning techniques, the control of information about ourselves is now more than ever vested with the firms and organisations we interact with.

Data in the Platform Economy

The latest revolution to disrupt the economy is communications technology that has driven the marginal cost of storing and transmitting information to practically zero. This has essentially eliminated the transactions costs that provide a comparative market advantage to the large hierarchical organizations that characterized the industrial revolution.[7] That, in turn, has enabled buyers and sellers to find each other with little or no need of intermediary third parties.

This latest revolution is driving two profound and related changes to the economy. First, it is creating a sharing economy in which consumers will be able to hire or rent assets rather than buy them.[8] Second, it is facilitating the emergence of a platform economy. This business structure is profoundly different from traditional business structures in which firms deployed internal hierarchy and managerial authority to either acquire or produce a good or service that was then sold to customers. Both consumers and firms engaged in search costs to discover each other and tended to trade, more or less, at arm's length. There was little need for traditional businesses to seek *detailed* information about individual consumers. Yet even if they had that information, processing it was difficult.

If trade occurs using cash, the transaction is very simple. If trade occurs on a credit basis, then firms need to collect some information about customers' creditworthiness. The costs of acquiring and storing that information are non-trivial, so credit agencies emerged to lower those transactions costs. The cost of transferring that information to third parties can prove particularly high. In time, the emergence of credit and debit cards helped to further lower discovery costs.

In this business environment, privacy concerns would be not be a high priority for many individuals. What could be of concern is that credit rating agencies have access to correct information. However, the emergence of platforms dramatically changed that situation.

Communications technology has driven the marginal cost of storing and transmitting information to practically zero.

Cross-subidies can serve beneficial functions when adopted voluntarily by private actors.

Platforms are also known as two-sided markets—they have to simultaneously satisfy two groups of individuals, buyers and sellers. While the idea of platforms is quite old, their prevalence in the economy is a recent phenomenon. Banks are the oldest platform—they intermediate between borrowers and lenders. The second oldest platform is the traditional media business model. Historically, media companies made their profits from selling advertising to businesses while providing news and entertainment to consumers. The business model required that media simultaneously satisfy two sets of customers.

The next platform business to emerge was credit cards. Credit card companies also have to satisfy two groups of customers—they have to induce consumers to use the card when making purchases and convince merchants to accept the card as payment. Credit card companies facilitate trade between buyers and sellers and dramatically reduce transaction costs for sellers when buyers wish to trade using credit. They also increase convenience for buyers by reducing the amount of cash they have to carry.

It is often the case that more value is created on one side of the market than on the other.[10] For this reason, the platform has to compensate, or cross-subsidize, one side of the market in order to induce people to participate in the platform. While they may seem inefficient upon a superficial look, cross-subsidies can serve beneficial functions when adopted voluntarily by private actors. In the case of platforms, the cross-subsidy acts as an efficient mechanism to overcome barriers to trade. Platforms generate positive externalities for the parties transacting on the platform. For example, in the case of credit cards, merchants have opted to pay (or forgo) the interchange fees—the fees exchanged between a credit card holder's bank and a merchant's bank. As Nobel Prize-winning economist Jean Tirole explains:

> Platforms often grow thanks to very low prices on one side of the market, which attract users on that side, and indirectly enables the platform to earn revenues on the other side. The structure of prices between the two sides of the market takes full advantage of the externalities between them. The basic idea is simple: the real cost imposed by a user is not the straightforward actual cost incurred in serving them. The user's presence creates a benefit for the other side of the market, which can be monetized—thus, de facto, reducing the cost of serving this user. In some cases, one side of the market might not pay anything, or might even be

subsidized, the other side paying for both.[11]

Unfortunately, as the Nobel Prize-winning economist Ronald Coase explained, the political and regulatory imperative to tackle monopolies through antitrust and competition policy has encouraged economists to identify monopolies whenever they see a business practice they do not fully understand.[12] Platforms are increasingly being targeted by politicians and antitrust regulators on the basis that they wield "market power"—traditionally understood as a claim that a firm is able to increase prices above what would prevail in a competitive market, but now encompassing claims about the use of data, violations of privacy, and purported harms to adjacent industries.[13] Antitrust regulators and politicians often interpret cross-subsidies within platforms as evidence of market power, rather than the gains from trade being shared across the market. Platforms are also often accused by traditional media—the original platforms—of destroying their business models.

The other important change is that platforms collect more data about their consumers than do traditional businesses. This data may be either a byproduct of trade or necessary to induce trade. To the extent that platforms provide matching services for buyers and sellers, it is necessary for the platform to know its customers. Under "know your customer" regulations in the financial industry, government has regulated the data and information that firms have to collect from their customers and when that information has to be revealed to government. Operating as platforms, however, banks—and the finance industry in general— already have detailed information about their customers.

Two-sided platforms match buyers and sellers to facilitate transactions. This requires them to create a trusted environment where opportunities for fraud are suppressed. This again increases the likelihood of increased transactions—and the transactions themselves generate further information. Through economic activity, buyers reveal their actual—rather than their stated—preferences. This information is collected by the platform and in turn becomes the basis for additional matching and refinement of information about the buyer.

Two types of trust problem persist in platform economies. The first type is what is known in economics as the adverse selection problem; it is not unique to platforms. Is the matching actually occurring? Are buyers being matched with the best sellers for their purposes? Is the platform systemically biased? Does the platform have a conflict of interest?

Through economic activity, buyers reveal their actual—rather than their stated—preferences.

Governments effectively nationalize a lot of data they collect.

The second trust problem relates to control and ownership of the data generated by and retained on the platform. While this issue is also not unique to platforms, its importance is likely to increase in the future because of the increasing prevalence of platforms as a business structure and the declining cost of storing and transmitting information.

The key questions are: What happens to this market data? When can it be used? Who should use it? Who should profit from its use? Jean Tirole offers what he thinks is a common sense solution:

> This raises the following fundamental question: Does the company holding customer data have the right to make money from the possession of that information? The commonsense reply … is that if the data was collected thanks to an innovation or a significant investment, then the company ought to be able to profit from retaining and using it. If, on the other hand, it was easy and cheap to collect, the data ought to belong to the individual concerned.[14]

The difficulty lies in the intermediate case. What if the data were "easy and cheap" to collect as a result of "an innovation or a significant investment"? It is useful at this point to distinguish between three categories of data.[15]

- One is **user-provided data**. Many individuals voluntarily reveal personal information online. A Facebook page, for example, may include a person's name, sex, date of birth, marital status, interests, photos, and videos.
- A second category of data is **observed data**—how individuals interact with content and with one another on the platform.
- Finally, there is **inferred data**, which is based upon an analysis of both declared data *and* observed data. The production of inferred data requires entrepreneurial insight and investment.

In the absence of clear property rights over data—however defined—the above data now appear to exist in a commons. Anyone can acquire it, with some effort and at some cost. More troublingly, governments effectively nationalize a lot of data they collect. If data were to be privatized, then the question becomes: Who should own it, the platform or the individual?

Following Tirole, it appears obvious that individuals should own their declared information, but the status of observed data is less clear. That data is jointly produced by the individual and the platform. Inferred data is not jointly produced by the individual

and the platform. The individual may have some ownership of the inputs into the production of inferred data, but the value (if any) of the inferred data is almost entirely due to entrepreneurial insight. According to Tirole's argument, the platform should be able to profit from the use of inferred data.

In a free market, the person or organization that most values the data will own and control it.[16] However, that does not exclude the possibility that the party who most values the data should not have to pay, or make some investment, to acquire it.[17]

There are currently two mutually exclusive beliefs about the property rights regime that governs data.[18] The first is that the entity that collects the data—such as a social media platform or government agency—has the right to use and control that data, potentially to turn it into something of value to it. This reflects much practice in the absence of data-specific regulation. Opposite that is the belief by some privacy advocates that property rights over data—or specifically personal data—should be vested in the individual who either provided the data or whom the data concerns. Clear ownership of personal data would allow for the sort of efficient allocation of property rights in the sense that Ronald Coase explained, where the ability to make subsequent exchanges over an asset allows the market to allocate ownership where it is most valuable.[19] However, while this latter approach has some intuitive appeal, the situation is far more complex and the arguments nuanced.

In a free market, the person or organization that most values the data will own and control it.

The Idea of Privacy

The simple question, "What is privacy?" is fraught with difficulty. Indiana University law professor Fred Cate has set out a comprehensive, yet probably incomplete, list of what privacy could be. His list includes individual autonomy, self-definition, solitude and intimacy, confidentiality, anonymity, security, freedom from intrusion, freedom from annoyance, freedom from crime, freedom from embarrassing disclosure, freedom from discrimination, profit, trust, "and countless other concepts."[20] Unsurprisingly, it is difficult to come up with appropriate public policy that addresses privacy concerns across all these areas. University of California, Berkeley law professor Paul Schwartz separates privacy into two broad categories: physical privacy, which he defines as the right to be left alone, and information privacy, the right to control and profit from your own information.[21]

The renowned American jurist Richard Posner offers a "provisional" definition of privacy as "the withholding or concealment of information, particularly personal information" from others.[22] Privacy increases as

The demand for privacy suggests that having accurate and relevant information in the public domain about oneself is valuable.

society gets wealthier. Primitive societies lack institutions for monitoring bad behavior—such as police or newspapers—and people living in close proximity to one another provides opportunities for mutual surveillance. Nobel Prize-winning economist George Stigler has suggested that privacy "refers to the possession and acquisition of knowledge about people and implicitly or explicitly also knowledge about association."[23]

To Stigler, possessing knowledge about people and associations is unremarkable. Standard neoclassical economics assumes perfect information—that all market participants have all the required information to make exchanges—which encompasses an assumption that people already hold information and knowledge about other people. As Posner has indicated, an element of concealment is necessary to secure and protect privacy in the real world. Stigler recognizes this point and clarifies that privacy "connotes the restriction of the collection or use of information about a person or corporation; the information in question 'belongs' to the individual."[24]

To a neoclassical economist, this raises the question of the consequences of restricting or concealing information. In mainstream economic theory, asymmetric information is a cause of market failure, a problem for which many neoclassical economists spend their time devising "solutions." However, in institutional economics—the field that, following Ronald Coase, studies how human societies develop institutions to reduce the transactions costs of exchange—the question is whether information about a person, commonly referred to as "private" information, should belong to that person.

Most of the economic literature deals with the public policy questions of whether consumers are better off sharing or concealing information—specifically whether consumers benefit from market segmentation and price discrimination—and the impact of privacy on consumer protection and competition policy.[25] The literature is mostly silent on the question of who should own "private" information—though the answer appears as obvious to the general population as it was to William Safire in 1999.

The demand for privacy suggests that having accurate and relevant information in the public domain about oneself is valuable. But, as Stigler recognizes, information about individuals in the public domain may be incomplete, inaccurate, improper (and thus irrelevant for market transactions), derogatory, or stale. Conversely, information could be correct and highly relevant. It may also be true, yet shameful or embarrassing.

Yet, there does not appear to be any market mechanisms to ensure that inaccurate, improper, derogatory, or outdated information is updated with accurate and relevant information. There is a missing market for privacy.

By this logic, the demand for privacy overcomes a negative externality. Privacy corrects for the problem that there may be too much "bad" information about an individual in the public domain. Adding to the challenge of sound policy making is the fact that what constitutes "bad" and "good" information is entirely subjective.

Stigler maintains that market solutions to these issues work, or could work, in the absence of government intervention. Failing that, he speculates that some knowledge is simply *not valuable*. The issue for Stigler is that privacy ultimately results in a misallocation of economic resources. In the presence of privacy, there is a reduction in informed decision making and the working of the price system and of the market economy in general.

Posner argues that privacy advocates conflate two related, but not identical ideas: seclusion, the right to be left alone, and secrecy, the right to control access or usage of information about oneself. However, unlike Stigler, Posner points to a good economic rationale for why individuals demand privacy: "they want more concealment of information about themselves that others might use to their disadvantage."[26] Posner identifies the demand for privacy in the investment that individuals make in managing their reputation. A "good" reputation increases demand from others to cooperate with the individual in both their economic and non-economic interactions with others. A "bad" reputation has the opposite effect—a reduction in demand for interaction with that individual.

If privacy is important to the curation of a good reputation, then, as the size of the market increases, the value of a good reputation increases too, and privacy rights become more valuable. Over the past few decades, advances in communications technology and falling transportation costs have dramatically increased the size of markets. More individuals interact on a global scale and can find value in having a globally managed reputation—hence the demand for greater privacy rights. The challenge to this notion is that control over knowledge can be used to mask a bad reputation. As the market increases in size, we might observe more individuals engaging in opportunistic behavior, such as email scams, due to a lack of knowledge about their behavior in a smaller market. Ironically, then, the demand for privacy increases as the size of the market increases, but so does the demand for information, as consumers seek to overcome opportunism problems that arise in a

What constitutes "bad" and "good" information is entirely subjective.

Privacy can be thought of as an externality, which occurs when someone's actions or choices impact another person.

larger market. Rating systems, such eBay scores and Uber ratings, have emerged over the past few years as a solution to this problem.

As noted, privacy can be thought of as an externality, which occurs when someone's actions or choices impact another person. Externalities can be either negative or positive. The sharing of embarrassing information, for example, would be a negative externality. Providing a positive but unsolicited reference to a potential employer would be a positive externality. The challenge here arises when third parties seek to profit from selling individuals' private information, thus turning an externality into a business transaction. In short, individuals either want to be in a position to sell their own data, share in the profits of selling their data, or prevent others from selling or sharing their data.

Externalities often arise due to the absence of a specific market—a situation known as the "missing markets" problem. In the absence of markets, we also experience the absence of market pricing.[27] In the absence of market pricing, it is difficult to distinguish stated preferences from revealed preferences. It is possible that some individuals signal an overvaluing of their privacy that leads to an excess demand for privacy. In this instance, privacy restrictions could lead to significant social costs being incurred. Building on that view, it is possible that the excess demand for privacy is due to a minority of individuals who are engaged in rent-seeking behavior that would impose their subjective preferences on the entire community.

In a 1986 paper Nobel Prize-winning economist James Buchanan discusses the notion of "private spaces" and social interdependencies. He notes that in a social environment it is almost impossible to define private spaces to exclude all conflict that may arise from an invasion of privacy.

> I prefer that my neighbors control their children's noise-making and disposal of their tricycles; I prefer that these neighbors refrain from rock music altogether, and if such "music" is to be played that the decibel level be kept low. I prefer that their backyard parties be arranged when I am out of town.[28]

By violating Buchanan's seclusion his neighbors are imposing a negative externality. Buchanan also hopes to benefit from a positive externality too.

> I also prefer that my neighbors plant and maintain shrubs that flower in May for my own as well as their enjoyment.[29]

Buchanan does not refer to his examples as externalities, but as

"meddlesome preferences."[30] He makes the point that these meddlesome preferences are mutual and reciprocal—that his own behavior can impose both negative and positive externalities upon his neighbors.

Economists well understand the notion of externality—that social costs may deviate from private costs and impose negative externalities upon others or that social benefits may deviate from private benefits and impose a positive externality. Negative externalities result in too much of a "bad" thing and positive externalities too little of a "good" thing. However, this standard analysis masks many value judgements. We might all agree in the abstract that too much pollution is a "bad" thing while we might reasonably disagree on what constitutes "too much" or disagree on the benefits and costs of reducing pollution. That it is not immediately obvious what should be done about nuisance was the important insight by Ronald Coase.[31] Prior to Coase, economists had proposed combinations of prohibition, regulation, subsidy, and taxation to overcome externality problems. While many still do, the Coasian insight was that externalities can be the subject of market negotiations, as individuals and firms compensate each other for those externalities. The fact that high transactions costs prevent these negotiations from occurring directed economists' attention to those costs. An issue well worth considering is whether such a Coasian bargain can be argued to have already occurred—Facebook and Google, for example, provide consumers with access to services at zero-price in exchange for access to their data.

There is another insight that needs to be considered. Buchanan and Claremont McKenna economics professor William Craig Stubblebine have argued that many externalities may be infra-marginal and might not persist in equilibrium. In this instance, the cost of responding to the externality may be greater than the disutility created by the externality.[32] Here too norms and institutions have evolved to resolve disputes and facilitate cooperation. In his 1986 paper, Buchanan explains that he does not exert too much effort at imposing his preferences on his neighbors. Rather, he relies on "common decency, fair play, and mutual respect."[33] Where Coasian bargaining solutions (which would involve compensation, building soundproof walls, or even moving away) are expensive, these evolved institutions (norms and cultures around appropriate stances towards ones' neighbours) are much cheaper.

It is likely that rights to privacy are mostly matters of "common decency, fair play, and mutual respect." As we argue below, "rights to privacy" have not evolved as economic rights, but

"Rights to privacy" have not evolved as economic rights, but rather have emerged as legal rights.

The supply of private information is likely to be a positive function of the need to attract trading partners and engage in reputation management.

rather have emerged as legal rights. Nonetheless, this raises the issue of missing markets in the absence of property rights. If property rights have not emerged for privacy, then markets for trading private information will not have emerged and there may be gains from trade that are not being realized. That is the challenge William Safire alluded to in 1999. Policy efforts to address it can be thought of as attempts at internalizing externalities.

Privacy as Exchange

In a recent book, one of us (Berg) outlines an approach to understanding privacy choices.[34] Rather than considering the demand for privacy, we think of privacy as exchange. Why do individuals supply information about themselves to others in the market? We also discuss the situation of providing information involuntarily to the government.

The supply of private information is likely to be a positive function of the need to attract trading partners and engage in reputation management and a negative function of the need for protection. In the first instance, individuals are social animals and, with the exception of hermits, tend to interact with other individuals on both an economic and social basis. The signal to engage with others usually involves the sharing of information about oneself. Thus, individuals have to choose to share information before it is known and in the public sphere.

Reputation management is the attempt to positively influence other individuals' assessment of one's value as a trading or social partner. Privacy is a mechanism to engage in identity management.

The protective aspect of information supply relates to Posner's insight—the demand to control information in order to prevent it from being used to one's disadvantage. It is here that the scope for opportunism arises—an individual may rightly have a poor reputation he would like to conceal. At the same time an individual may have a poor reputation for entirely incorrect reasons that she would wish to conceal or have corrected in the public domain.

The demand for private information can be broken up into two categories, private and public. The private demand for private information is a positive function of the need to evaluate trading partners to protect against fraud. Historian Yuval Noah Harari speculates that human language evolved as a means of facilitating gossip—the unauthorized sharing of private information—to facilitate mutual monitoring in small human societies.[35] This explanation is consistent with Posner's theory relating to the lack of privacy in primitive societies. Individuals face a situation

where they demand more private information than others are willing to supply. Mutual monitoring and gossip exist as evolved institutions leading to the development of sophisticated language to overcome a potential disequilibrium in the market for private information.

The public demand for private information is very different. Government demands information for taxation purposes, national security, and to administer the welfare state. It acquires information involuntarily from its citizens and any foreigners who wish to enter its territory. In 1980 Stigler made the point that all levels of government now collect information in a detailed quality and quantity unknown in human history.[36] Since then that situation has only intensified. Even then, he could point to technology as a facilitating factor of the modern surveillance state. Rightly, however, he identifies the economic and political drivers of that information collection as more important than the technology itself.

Data and Property

With some minor exceptions, privacy—control over public information regarding oneself—has not emerged as an economic property right as described by the renowned economist Harold Demsetz, in his influential 1967 article, "Toward a Theory of Property Rights." In Demsetz's view, property rights are endogenous to the market, and are recognized by the state after their emergence. Property rights emerge from the needs of economic interaction. Participants in exchange develop and expand notions of property rights where the benefits of internalizing costs outweigh the costs of that internalization. Demsetz looked at the development of indigenous family hunting territories in Canada in response to growing demand for fur from Europe during the 18th century. As the economic value of beavers increased, it became economical to introduce a property rights regime that divided up the right to hunt. The drivers of changes that allow for the creation of property rights regimes can be new technologies, changes in relative prices, or the expansion of the size of the market.[37]

Richard Posner discusses privacy exceptions, such as privileged communication, blackmail, and defamation. Privileged communication can be seen as a subsidy of—or compromise with—other important social institutions such as the presumption of innocence, the right to legal representation, and marriage. Blackmail is a crime, although Posner seems to suggest that only extortion, potentially involving violence, should be criminalized. Defamation is a tort, but is limited to reputational damage

All levels of government now collect information in a detailed quality and quantity unknown in human history.

The ability to control now public information that one would prefer to be concealed has not emerged in modern society.

related to economic relationships and not for disrupting peace of mind or inflicting emotional distress.[38]

A basic economic analysis suggests that a "right to privacy" is not an economic right that would emerge spontaneously. To the contrary, human behaviors such as gossip and mutual monitoring emerged to deny that right in primitive societies. It may be true that such a right should emerge in non-primitive societies and on some margins that is indeed the case. If we define the right to privacy as a right to seclusion, then it is certainly the case that individuals in wealthier societies have access to more quiet time and space than do individuals in poorer societies or at any other time in history. Yet, the ability to control now public information that one would prefer to be concealed has not emerged in modern society. However, that does not preclude private organizations from providing privacy as a product offering, as outlined below.

The right to control information about oneself in the public domain is best thought of as an intellectual property right that can only emerge as a legal right. Building on his work with the late University of Rochester political scientist William H. Riker, Itai Sened of Washington University in St. Louis developed a model that explains the emergence of legal-centric rights.[39] On the assumption that individuals and social agents maximize utility (however defined; governments, for example, can pursue public objectives) and that government is the only source of legitimate coercion, Sened is able to derive four conditions that would see the emergence of legal rights.[40]

- First, the right itself must have market value. In the case of privacy (the supply of private information) the market value of the right itself is contested. Subsets of the right are valuable but others are not. Alternately, the data may only be valuable in aggregate. If the entirety of the right to privacy were valuable, it would have emerged as an economic right. The right to control information about oneself is valuable to that individual, but not to others. It does not have market value; it has subjective value to one side of the market but not the other.
- Second, rights-holders need to desire the right. This is generally the case; individuals want their privacy.
- Third, the government is willing to enforce the right.
- Fourth, at least some duty bearers are willing to observe the right.

However, the fourth condition runs counter to the second condition—while many individuals as rights

holders desire the right to privacy, those same individuals as duty-bearers do not wish to observe it.

The first condition explains the difference between the private and public demand for private information. The government simply does not want to observe the right to privacy of its own citizens. While it may be true that some governments are constrained by constitutional impediments to surveilling citizens, it remains the case that these prohibitions are not absolute and can be easily circumvented. Whether these constitutional impediments are being increasingly avoided is an empirical question. In the absence of a Bill of Rights or a similar document, citizens have no enforceable right to privacy against their own government.

Turning our attention to the private demand and supply of private information, the situation becomes more complex. It is true that not all aspects of the right to privacy are valuable, because of the possibility that duty bearers may not want to respect the right. In particular, they are concerned about opportunism—that the person claiming the right to privacy may be concealing valuable information that would disadvantage the duty bearer. This raises the question: Why would the government want to enforce a right that is not valuable in the market? Enforcing rights is costly to government, but if no market value is being generated by the right, how will government either tax that value or otherwise appropriate it? This helps explain why some aspects of privacy have emerged as economic rights and others have not.

This analysis leaves us in the difficult position of suggesting that, while many people claim the desire to have greater privacy and governments give much lip service to the right of privacy, the right itself—beyond some tightly prescribed exceptions—is not particularly valuable. That is exactly the problem. Private information has public good characteristics—its use is non-rival and most private information is non-excludable. It turns out that privacy is only viable with secrecy, which is not economically valuable when dealing with other individuals on the open market, while governments do not tolerate secrecy when dealing with their own citizens.

The government simply does not want to observe the right to privacy of its own citizens.

A Regulatory Solution?

One way to solve the property rights dilemma would be to construct the idea of property rights in private information through regulation. This is the approach of the European Union's (EU) General Data Protection Regulation. The GDPR, which came into force in May 2018, is a semi-global regulatory response to the privacy dilemmas around the use of personal data. It seeks to regulate the

The GDPR is the most ambitious regulatory response to non-government privacy dilemmas in the developed world to date.

sort of uses of personal data that have generated considerable controversy—such as the non-disclosure of how data is exchanged with third parties.[41]

The GDPR is the most ambitious regulatory response to non-government privacy dilemmas in the developed world to date. It aims to regulate not only firms operating within the EU, but any firm that interacts with EU citizens. Given the global nature of the digital economy, in practice the GDPR covers nearly the entire planet. The GDPR regulates how firms of any size acquire, store, and use personal data—"any information relating to an identified or identifiable natural person," which includes but is not limited to names, identification number, location data, or "physical, physiological, genetic, mental, economic, cultural or social" identifiers. As Paul de Hert and Vagelis Papakonstantinou of the Free University of Brussels write:

> There is very little personal data processing that will remain unaffected by the combined effect of the Regulation and the Directive. Their combined scope covers all personal data processing executed by private actors as well as all similar processing undertaken by law enforcement agencies in the Member States; in fact, only processing by secret agencies for national security purposes and processing by EU law enforcement agencies is left unregulated. Apart from these exceptions, there will practically be no individual within the EU not directly affected by the reform.[42]

The GDPR is a large and complex regulatory framework structured around a consent model of data collection and use. It has some features that make it a significant regulatory shift regarding privacy protection. It provides consumers with a series of supposed "rights" regarding control of their personal data. These include:

- Right of access to their personal data held by firms;
- Right of rectification to complete or correct inaccurate personal data;
- Right to restrict data from being processed where the data is contested for accuracy or is under legal claims;
- Right to move personal data from one firm to another firm; and
- Right to object to the processing of personal data if that processing is not GDPR compliant.

The most prominent and controversial of these rights is a provision that allows EU citizens to request that companies delete their personal data "without undue delay." This right, known colloquially as the "right to be forgotten," is not unlimited. Data protection must be "considered in relation to its function in society," and some data requirements (such as those imposed by know your customer regulations) "in the general interest" mean that requests to delete may not be approved. Nor is it entirely novel. A so-called "right to be forgotten" has been in force in the European Union since 2014.[43] Since reformulated as a "right to erasure," in response to criticisms that it was being used as a limitation on freedom of speech, it is nevertheless the case that the broad geographical application of the GDPR makes this a significant regulatory requirement.[44]

The GDPR has a number of other features, some of which are shared by other data protection regimes around the world. For example, it has a mandatory data breach notification scheme, which requires firms to notify affected individuals if personal data has been stolen or accidentally released to the public, and a data rectification scheme, which gives individuals the right to correct personal data in corporate storage. In common with many other regulatory approaches, it requires businesses to delete data they have collected once that data is no longer necessary for business purposes.

The regulation requires firms to acquire explicit and informed consent for how personal data will be used. The right to erasure is intended to represent an explicit withdrawal of consent. The sanctions for non-compliance are heavy—up to €20 million ($22.14 million) or 4 per cent of annual global revenue, whichever is higher. Each EU member state has appointed a supervisory authority to manage and enforce compliance.

On the face of it, the GDPR looks like a regulatory implementation of personal data ownership, but in fact the resemblance to property as understood in the classical liberal tradition is only superficial. The EU data protection approach features a cocktail of private rights—such as the right to information about how personal data is used and to object to some automated decision making processes—and command and control mechanisms that are directly enforced by public agencies.[45] Rather than establishing general principles or desired outcomes which are then enforced by regulators and the courts, the GDPR focuses on regulating the process by which data is acquired and managed.

The distinction between personal and non-personal data is difficult to sustain.

Furthermore, the GDPR regulates only personal data, defined as all data created intentionally or in the process of pursuing other ends (what is known as "exhaust data").[46] However, the distinction between personal and non-personal data is difficult to sustain. The relative ease with which some anonymized data can be reidentified (that is, personal data can be matched to a specific individual even after clear personal markers like names are removed) makes almost any data that is the product of some human action, no matter how trivial, a form of personal data.[47] Additionally, from a classical liberal perspective, it is unclear why data about human activity when obtained and managed by groups, such as firms or nonprofit organizations, should be treated differently from that managed by individuals. In the European Union, this unclear distinction nonetheless brings about sharp divisions in the law.

Since 1996 the EU has created ownership rights in non-personal electronic data through the Database Directive, which grants a form of copyright over the structure of created data and a limited copyright-like right over data in circumstances where there has been "substantial investment in either the obtaining, verification, or presentation of the contents."[48] While intellectual property regimes like copyright have an obvious appeal when searching for a precedent for data ownership, it is not evident that principles developed for copyright protection can be adapted for data in general.

Copyright is a limited monopoly granted under the belief that creative works will be underprovided if those works can be freely duplicated without compensation to their creators. But non-personal data has economic value to its creator. It is hard to argue that data will be under-created without statutory protection. As Wolfgang Kerber of the Marburg Centre for Institutional Economics warns, to transfer the ideas underpinning intellectual property onto questions about data, would be "dangerous for innovation and competition in the digital economy, because it might lead to considerable legal uncertainty, the monopolisation of information, and impediments for the free flow of data that is so crucial for the digital economy."[49]

As the division between personal and non-personal data suggests, the rights granted by the GDPR over personal data are not property rights in the classical liberal sense and only narrowly can be considered property rights in an economic sense. Tal Z. Zarsky of the University of Haifa argues that the GDPR has a distinctly philosophical approach to the value and purpose of privacy that is particular both to its origin and to

the historical period in which it was developed.[50] Traditional or classical liberal property rights regimes allow rights holders to acquire, use, and dispose of their property as they see fit. Property can be exchanged to exploit gains from trade. This is the basis of the theory of privacy as exchange. The GDPR adopts the opposite approach. The legal rights embedded in the GDPR treat the right to personal data as inalienable—that is, unable to be exchanged. According to this approach, privacy is a fundamental human right that is vested with each individual as a virtue of being human. In the classical liberal theory of property rights, property has a social function—to allow rights holders to pursue diverse ends while avoiding disputes. By contrast, under the GDPR, privacy exists as a right to be protected on its own terms, not as a means by which other goals can be pursued.[51]

The inalienability of personal data under the GDPR will likely present a significant barrier to the use of data as an input to exchange and the subsequent development of data markets. The exchange value of information is dependent on its use as an input to economically valuable activity. The GDPR requires firms to obtain explicit consent for the use of data collected in the course of business. But as privacy is inalienable, consumers cannot give consent for data to be used at the discretion of the data collector—that is, users cannot exchange away their right to erasure of a given set of personal data, even if they do so with fully informed consent. Under the GDPR, consumers at all times retain their right to request erasure.[52]

Furthermore, the GDPR imposes the right of erasure on firms that have acquired data through secondary markets. Collecting firms that have received a right of erasure request are required to make their best efforts to ensure that other firms that have purchased or otherwise acquired the data act on the request. This likely will prove to be a prohibitive restriction on the development of secondary data markets. In the absence of a right to approve the reuse and sale of personal data, the GDPR's consent model of data use is inflexible and static. Consent has to be obtained on the basis of a "specific, explicit and legitimate" purpose, and cannot be "processed" in a way "incompatible" with that original purpose. This requirement seems to outright prohibit the analysis of data in any way for which consent was not obtained in advance.

As noted, the GDPR is the most ambitious and comprehensive legal approach to privacy yet adopted in the developed world. The consequences of the GDPR and its effect on the

The exchange value of information is dependent on its use as an input to economically valuable activity.

The GDPR represents a rigid regulatory framework that imposes artificial divisions between non-personal and personal data and limits the monetization of individual personal data.

protection of privacy and development of data markets are speculative. But as Zarsky argues, on its face, the GDPR is incompatible with the development of the economic potential of data analytics, in the form of artificial intelligence and big data.[53] As an approach to protecting individual privacy, the GDPR represents a rigid regulatory framework that imposes artificial divisions between non-personal and personal data and limits the monetization of individual personal data. Rather than offering EU citizens property rights over their data, it provides limited regulatory rights under carefully proscribed circumstances and then imposes limitations on how they can exchange information about themselves.

The Ongoing Social Negotiation of Privacy

The experience of the GDPR helps demonstrate why regulatory approaches toward property rights over data are unlikely to be effective. The GDPR is a document with a specific historical context. Proposed in 2012, finalized in 2016, and coming into force in 2018, it reflects the prevailing technologies and concerns of the time in which it was developed. The years since have seen dramatic changes in technology, data use, and the social and political consequences of information disclosure, as the Cambridge Analytica scandal dramatically showed. Rigid regulatory frameworks risk either locking in anachronistic approaches to privacy protections or failing to tackle new and unanticipated problems. As technologies change, so do the norms and attitudes around those technologies. These changes are hard to predict in advance. As Colin Bennett of the University of Victoria and Robin Bayley of Linden Consulting argue:

> The appropriate balance cannot be struck by legislating in advance those types of personal data that might never be captured or processed. Rather, the balance is struck around the principle of relevance to an explicit and legitimate purpose. The personal data required within any one organizational context are governed by a set of social norms about what might be an appropriate intrusion.[54]

Internet pioneer Vint Cerf summarizes that:

> [R]egulation is tricky. And I don't know, if somebody asked me, would you write a regulation for this, I would not know what to say. I don't think I have enough understanding of all of the cases that might arise in order to say something useful about this, which is why I believe we are going to end up having to experience problems before we

> understand the nature of the problems and maybe even the nature of the solutions. But I also want to argue that, while regulation might be helpful, that an awful lot of the problems that we experience with regard to privacy is a result of our own behavior. Which is not so much an illegality or something, or a violation in a typical regulatory sense, it is really just the fact that we didn't think about the potential hazard.[55]

Classical liberalism offers a framework through which we might better come to a social agreement about how to protect privacy in law. The technological and social environment for privacy protection is an evolving and adaptive one, and the institutional framework for privacy protection needs to be similarly evolving and adaptive. The adequate framework for privacy protection is that of a discovery problem. It is unclear *ex ante* what the most desirable institutional environment is, given the rapid adoption of new technologies by consumers and firms alike.

It is underappreciated that many firms have been responsive to the demand for greater privacy and user control over personal data, even if we might be still unsatisfied with the current outcome. Apple, for example, now offers an identity management service that competes with those of Google and Facebook. Facebook has responded to widespread public dissatisfication with its privacy policies—particularly concerning the sharing of data with third parties—by successive changes to its approach. Google's Data Liberation Front is a project that facilitates users moving data in and out of Google products.[56] Privacy management choices have ballooned over the last decade on every major digital platform.

For circumstances where market discipline does not adequately keep corporate misbehavior in check, it is not necessarily the case that regulation is the best alternative. Friedrich Hayek and Bruno Leoni valorized the common law as an evolutionary and adaptive approach to managing social conflicts. Under a common law approach, problems such as privacy are solved on a case-by-case basis, drawing on and building up a stock of precedent that has more fidelity to real-world dilemmas than do planned regulatory frameworks. Regulatory approaches such as the GDPR seek to identify and resolve all social disputes at the legislation stage. Between 2012 and 2016, privacy activists, lobbyists, consumers, researchers, and other data users funneled their institutional preferences into a single legislative contest. The framers of the GDPR had to mediate between these competing demands and finalize a document that

Under a common law approach, problems such as privacy are solved on a case-by-case basis, drawing on and building up a stock of precedent that has more fidelity to real-world dilemmas than do planned regulatory frameworks.

Rather than search for silver bullet solutions, policy makers should seek to open a space in which the appropriate legal bounds of privacy protection are discovered through learning and experimentation.

sought to satisfy in some way each interest group—along with the perceived preferences of the majority of EU citizens who did not participate in the process but will be nonetheless affected by the regulation. By contrast, case-by-case approaches mediate specific cases brought directly by involved parties, one at a time, over time.

The common law approach is not cost-free. Bringing individual cases is expensive—particularly when parties have disparate financial resources to bring to bear—and judges are not always objective. Individual consumers are not always aware that their privacy has been violated, since data can be sold, misused, or released without consumers' knowledge. Furthermore, *ex post* approaches can be unsatisfactory, as it is not always possible to restore the experience of privacy; information once released into the public domain is permanently in the public domain. Nevertheless, these objections are only compelling when considered relative to alternative institutional forms. Regulatory approaches such as the GDPR impose heavy costs themselves. An intermediate institutional form, litigation pursued by public agencies, is more promising, but the subjectivity of the experience of privacy and its violation suggests that, rather than search for silver bullet solutions, policy makers should seek to open a space in which the appropriate legal bounds of privacy protection are discovered through learning and experimentation.

It might be argued that in the near term this is a case for inactivity that would leave a clearly unsatisfactory status quo in place. But there is room for much positive activity within this muddle-through approach. One way to reduce privacy costs is to increase social knowledge about mitigating the possible harms of privacy violations. Adam Thierer of the Mercatus Center at George Mason University has offered what he calls the 3-E approach: *education*, *empowerment*, and *enforcement*. Education refers to the need for greater understanding and awareness of the way information, once exchanged, can be used. As Thierer writes, "education and media literacy must be the first line of defense in ongoing efforts to better protect personal privacy in the information age."[57] Employees need to understand that in most circumstances their employers can read their emails or messages on work-provided services and information technology departments can see what sites they browse on work computers. Much unwanted privacy loss occurs because of low levels of digital literacy, as Internet users are not familiar with the potential risks of sharing information about themselves and the tools they can use to mitigate those risks.

Empowerment is the development and deployment of those tools. There is a wide array of services, software features, and technologies to significantly enhance privacy protection online. For example, privacy activists encourage the use of ad blockers and private browsing modes when using the Internet, private browsers like TOR, encrypted messaging services, and two-factor authentication for emails (or even physical authenticator keys) in order to keep personal information secure. Consumers and citizens should use messaging and chat services that offer end-to-end encryption and turn on encryption and security features on services and devices that do not enable them by default. Passwords should be long and complex and password managers, which help users manage large unique passwords, adopted.

Like security, privacy protection can never be absolute. Not all risks are relevant to all individuals. Institutional costs are subjective. What matters is how individuals and society perceive the costs of regulation, nationalization, and the common law.[58] This is especially true for privacy, which is subjectively experienced and grounded in perceptions of being observed or being alone.

Nonetheless, many of the privacy violations in the 21st century require collective rather than individual responses. Thierer refers to enforcement as the use of existing legal frameworks that protect consumers against deceptive practices and misleading contracts. These general frameworks can, and are, being used to protect specific rights such as privacy. In that context, moral philosopher Judith Jarvis Thomson's argument that the right to privacy is hard to distinguish from rights such as property and personhood offers a fruitful guide to the protection of privacy. She argued that laws protecting property rights and personhood, such as those that prevent trespass or unlawful seizure, should be used, and if necessary, adapted, to protect privacy.[59]

Friedrich Hayek was critical of the confidence of government planners who believed they could produce superior welfare outcomes by overriding market prices and incentives. The rapid pace of recent technological change makes Hayek's insight especially important today. The last two decades have seen the rapid digitization of all aspects of the economy and society, a rapid move of our personal and social lives first onto computers and now personal handheld devices. The economy is now driven by a dramatic increase in the collection and use of data. To attempt to predict where the balance between personal data privacy and personal data use should and will lie in even the next five years is folly.

Like security, privacy protection can never be absolute. Not all risks are relevant to all individuals.

Blockchain offers a shared database of property relationships that does not require a central authority to manage.

Future Technological Change

Under what circumstances do property rights evolve? Harold Demsetz provides a straightforward answer: When the benefits of internalizing costs outweigh the costs.

> New techniques, new ways of doing the same things, and doing new things—all invoke harmful and beneficial effects to which society has not been accustomed. It is my thesis in this part of the paper that the emergence of new property rights takes place in response to the desires of the interacting persons for adjustment to new benefit-cost possibilities.[60]

The significance of personal data for consumer-producer interaction in the platform economy is remarkably new. Google's advertising service dates back to 2000, its Gmail service dates to 2004, and Facebook was only opened for public access in 2006. The use of these technologies at scale began even more recently. Parallel to this is the development of e-government services, such as digital health records, which provide new risks and opportunities for the use of data.

One especially promising technology is blockchain, the distributed ledger technology underpinning cryptocurrencies such as Bitcoin and Ethereum. It is an institutional technology for the governance of property rights that complements and competes with the existing suite of institutional governance technologies currently available such as markets, governments, firms, clubs, and the commons.[61]

Blockchain offers a shared database of property relationships that does not require a central authority to manage. Rather, blockchain vests its users with cryptographically secure control over digital assets, such as cryptocurrency tokens. Transactions using those privately held assets are made on a publicly accessible ledger that records each transaction using a distributed consensus mechanism. In the case of first generation blockchains like Bitcoin, this consensus mechanism involves a subset of users validating transactions by competing to perform a computationally difficult task (the proof of work mechanism). Later generations have developed alternative consensus mechanisms, and so-called private or permissioned blockchains offer greater variance in design.

For our purposes, the key characteristic of blockchain is its provision of a shared infrastructure for the protection and exchange of owned data. Blockchains potentially allow a new mechanism not only for the sharing of data, but also for its ownership and exchange. The latter, in turn, allows for new transactions that were technically or economically unfeasible

in environments of centralized data management.

There is a great deal of innovative effort going into developing such applications. For example, decentralized blockchain data exchange platforms such as Ocean, Datum, and Datawallet promise to give users control over their personal data and trade with digital services for limited access on their terms. To the extent that such models can be adopted at scale, they offer an alternative to the centralized planned model common in large scale data collection and analysis.[62] For example, the RMIT Blockchain Innovation Hub has explored the utility of blockchain in the context of one of the trickiest and most sensitive data management tasks in the modern economy—personal health data.[63]

These initiatives are variously speculative, of course. They also represent just a tiny fraction of the innovation and investment currently being directed toward resolving the problems associated with data control and exchange in the platform economy. Alternatively, it might become necessary to supplement these innovations with law, in the way that the examples of evolved property rights identified by Demsetz eventually came to be enforced by state action. But such legal approaches are *evolved* legal approaches, not regulatory impositions that attempt to supplant or preempt market demand for privacy.

Ultimately, what these distributed ledger technologies offer to our understanding of the debate over privacy is a recognition that this is an evolving and entrepreneurial sector. Privacy should not be seen as a static equilibrium, as if the massive changes that have occurred in the last decade are now locked in, and as if the balance of economic power obtained by the large platforms is permanent. We ought to expect as dramatic technologically induced changes in the next decade as the last. In new social technologies—such the home, the telegraph, and the telephone—privacy protection lags behind early development.[63] Those protections are not a historical certainty—they need to be developed—but there are many signs of innovation and entrepreneurship working to meet that challenge.

Privacy is key to individual liberty.

Conclusion

The privacy dilemma is this: There is an enormous amount of economic value that can be unlocked with the use and analysis of personal data, but the use of that data can expose information about individuals without their consent. Privacy is key to individual liberty. Individuals require control over their own private information in order to live autonomous and flourishing lives. While free

individuals expose information about themselves in the course of social and economic activity, public policy should strive to ensure they do so only with their own implied or explicit consent.

The ideal public policy setting is one in which consumers can control and monetize their own data. The ideal regime would be one in which individuals have property rights over personal information. Governments have begun to try to provide such rights. The European Union's General Data Protection Regulation purports to give users control over their data held by firms and other organizations. However, the "right" it offers is an extremely limited one and effectively prevents individuals from being able to monetize their own data. Consumers are unable to contractually "sell" their information to firms, as the GDPR establishes a permanent right to have their data erased (albeit under limited circumstances).

The relationship between data markets and privacy ought to be governed by the common law. Regulatory approaches such as the GDPR are insufficiently adaptive to rapid changes in technology and demand, risk locking in outdated conceptions of privacy risks and opportunities, and are static rather than evolutionary—and thus unlikely to bring public policy closer to the ideal property rights regime. The common law, thanks to its case-by-case, evolutionary nature, is more likely to provide a sustainable and adaptive framework by which we can approach data privacy questions.

The data privacy dilemma is a reflection of the current state of technology. Until recently there has been no alternative to centralized data management, a status quo that carries significant risks regarding data access and control. New technologies, such as blockchain technology, potentially offer a mechanism to change the data ownership dynamic. Ensuring that we can benefit from these changes will require the flexibility and adaptability of the common law—rather than a regulatory—approach to public policy.

NOTES

1 Nova Spivack, "The Post-Privacy World," *Wired*, July 2013, https://www.wired.com/insights/2013/07/the-post-privacy-world/.
2 William Safire, "Nosy Parker Lives," *New York Times*, September 12, 1999, https://archive.nytimes.com/www.nytimes.com/library/opinion/safire/092399safi.html.
3 James Vincent, "(Update) London's Bins Are Tracking Your Smarthpone," *The Independent*, August 9, 2013, https://www.independent.co.uk/life-style/gadgets-and-tech/news/updated-londons-bins-are-tracking-your-smartphone-8754924.html.
4 Omer Tene, "What Google Knows: Privacy and Internet Search Engines," *Utah Law Review*, No 4 (2008), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1021490.
5 Charles Duhigg, "How Companies Learn Your Secrets," *New York Times*, February 16, 2012, https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.
6 Amy Pittman, "The Internet Thinks I'm Still Pregnant," *New York Times*, September 2, 2016, https://www.nytimes.com/2016/09/04/fashion/modern-love-pregnancy-miscarriage-app-technology.html.
7 For an extended discussion of the electronic markets hypothesis, see Thomas Malone, "Modeling Coordination in Organizations and Markets," *Management Science*, Vol. 33, No. 10 (October 1987), pp. 1317-1332, https://pubsonline.informs.org/doi/abs/10.1287/mnsc.33.10.1317; and Thomas Malone and John Rockart, "Computers, Networks and the Corporation," *Scientific American*, Vol. 265, No. 3 (September 1991), pp. 128-136, https://www.scientificamerican.com/article/computers-networks-and-the-corporat/.
8 For an in-depth discussion of the lowering of transaction costs in the sharing economy, see Michel C. Munger, *Tomorrow 3.0: Transaction Costs and the Sharing Economy* (New York: Cambridge University Press, 2018).
9 For an in-depth discussion see Chris Berg, Sinclair Davidson, and David Potts, "Outsourcing Vertical Integration: Distributed Ledgers and the V-Form Organisation," Social Science Research Network (SSRN), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3300506.
10 For a fuller explanation of the economics of two-sided markets, see Marc Rysman, "The Economics of Two-Sided Markets," *Journal of Economic Perspectives*, Vol. 23, No. 3 (2009), pp. 125-143, https://www.aeaweb.org/articles?id=10.1257/jep.23.3.125.
11 Jean Tirole, *Economics for the Common Good* (Princeton, N. J.: Princeton University Press, 2017).
12 Ronald Coase, "Industrial Organization: A Proposal for Research," in Victor Fuchs, ed., *Policy Issues and Research Opportunities in Industrial Organization*, National Bureau of Economic Research, 1972.
13 For an example of this see Australian Competition and Consumer Authority, Digital Platforms Inquiry Preliminary Report, Australian Government, Final Report, July 26, 2019, https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report.
14 Ibid.
15 We thank William Rinehart for suggesting this characterization.
16 Deirdre McCloskey, "The So-Called Coase Theorem," *Eastern Economic Journal*, Vol. 24, No. 3 (Summer, 1998), pp. 367–371, https://www.jstor.org/stable/40325879?seq=1#page_scan_tab_contents.
17 For more on this point, see Oliver Hart, "Incomplete Contracts and Control, Nobel Prize Lecture, December 8, 2016, https://www.nobelprize.org/uploads/2018/06/hart-lecture.pdf.
18 A useful discussion about these concepts of data is contained in "Data ownership,rights and controls: Reaching a common understanding," Discussions at a British Academy, Royal Society and techUK seminar, October 3, 2018, https://royalsociety.org/-/media/policy/projects/data-governance/data-ownership-rights-and-controls-October-2018.pdf.
19 Ronald H. Coase, "The Nature of the Firm," *Economica*, Vol. 4, Issue 16 (November 1937), https://onlinelibrary.wiley.com/doi/full/10.1111/j.1468-0335.1937.tb00002.x. Ronald H. Coase, "The Problem of Social Cost," *Journal of Law and Economics*, Vol. 3 (October 1960), pp.1-44, http://www2.econ.iastate.edu/classes/tsc220/hallam/Coase.pdf.
20 Fred H. Cate, "Principles for Protecting Privacy," *Cato Journal*, Vol. 22, No. 1, pp. 33–57, https://www.questia.com/library/journal/1G1-90250727/principles-for-protecting-privacy.
21 Paul M. Schwartz, "Property, Privacy, and Personal Data," *Harvard Law Review*, Vol. 117 (2004), pp. 2056–2128, https://scholarship.law.berkeley.edu/facpubs/2150/.
22 Richard A. Posner, *The Economics of Justice* (Cambridge, Mass.: Harvard University Press, 1981), p. 231.
23 George Stigler, "An Introduction to Privacy in Economics and Politics," *Journal of Legal Studies*, Vol. 9, No. 4 (December 1980), pp. 623-644, https://www.jstor.org/stable/724174?seq=1#page_scan_tab_contents.
24 Ibid.
25 For expertly summarized reviews of the literature, see Laura Brandimarte and Alessandro Acquisti, "The Economics of Privacy," in *The Oxford Handbook of the Digital Economy*, Martin Peitz and Joel Waldfogel, eds. (New York: Oxford University Press, 2012), https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780195397840.001.0001/oxfordhb-9780195397840-e-20, and Alessandro Acquisti, Curtis Taylor, and Liad Wagman, "The Economics of Privacy," *Journal of Economic Literature*, Vol. 54, No. 2 (June 2016), pp. 442-492, https://www.aeaweb.org/articles?id=10.1257/jel.54.2.442.
26 Richard A. Posner, "Privacy, Secrecy, and Reputation," *Buffalo Law Review*, Vol. 28 (1979), p. 5, https://pdfs.semanticscholar.org/cef9/4836cf200ad6cc99f73956f34d124d02e790.pdf.

27 This was the insight that gave rise to the socialist calculation debate in the 1920s and 1930s. For more on that, see Don Lavoie, *Rivalry and Central Planning, 1 edition* (Arlington, Virgina: Mercatus Center at George Mason Univerity, 2015) and Don Lavoie, *National Economic Planning: What is Left*, (Arlington, Virginia: Mercatus Center, 2015).
28 James M. Buchanan, "Politics and Meddlesome Preferences," in *Smoking and Society: Toward a More Balanced Assessment*, Robert D. Tollison, ed. (Lexington, Massachusetts: D. C. Heath, 1985), pp. 335–342.
29 Ibid.
30 Ibid.
31 Ronald Coase, "The Problem of Social Cost," *Journal of Law and Economics*, Vol. 3 (October 1960), pp. 1-44, http://www2.econ.iastate.edu/classes/tsc220/hallam/Coase.pdf.
32 James M. Buchanan and William Craig Stubblebine, "Externality," *Economica*, Vol. 29, No. 116 (November 1962), pp. 371-384, https://www.jstor.org/stable/2551386?seq=1#page_scan_tab_contents.
33 James M. Buchanan, "Politics and Meddlesome Preferences."
34 Chris Berg, *The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change* (Basingstoke, U.K.: Palgrave Macmillan, 2018).
35 Yuval Noah Harari, *Sapiens: A Brief History of Humankind* (New York: HarperCollins, 2015).
36 Stigler, "An Introduction to Privacy in Economics and Politics."
37 Harold Demsetz, "Toward a Theory of Property Rights," *American Economic Review*, Vol. 57, No. 2, Papers and Proceedings of the Seventy-Ninth Annual Meeting of the American Economic Association (May 1967), pp. 347-359, https://econ.ucsb.edu/~tedb/Courses/Ec100C/Readings/Demsetz_Property_Rights.pdf.
38 Posner, *The Economics of Justice*.
39 William H. Riker and Itai Sened, "A Political Theory of the Origin of Property Rights: Airport Slots," *American Journal of Political Science*, Vol. 35, No. 4 (November 1991), pp. 951-969, https://www.jstor.org/stable/2111501?seq=1#page_scan_tab_contents.
40 Itai Sened, *The Political Institution of Private Property* (New York: Cambridge University Press, 1997).
41 This and the following section are substantially derived from Chapter 9 in Berg, *The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change*.
42 Paul de Hert and Vagelis Papakonstantinou, "The new General Data Protection Regulation: Still a sound system for the protection of individuals?" *Computer Law & Security Review*, Vol. 32, Issue 1 (April 2016), p. 180, https://www.sciencedirect.com/science/article/pii/S0267364916300346.
43 European Court of Justice, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos [es], Mario Costeja González*, May 13, 2014, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.
44 For an example of a freedom of speech critique of the right to be forgotten, see Jerry Brito, "What Europe's 'Right to Be Forgotten' Has in Common with SOPA," *Time*, January 30, 2012, http://techland.time.com/2012/01/30/what-europes-right-to-be-forgotten-has-in-common-with-sopa/ .
45 Karen Yeung, "Making Sense of the European Data Protection Law Tradition," *Algorithmic Regulation*, London School of Economics and Political Science, Discussion Paper No. 85 (September 2017), pp. 34-45, https://www.kcl.ac.uk/law/research/centres/telos/assets/DP85-Algorithmic-Regulation-Sep-2017.pdf.
46 Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (New York: Houghton Mifflin Harcourt, 2014).
47 Florent Thouvenin, Rolf H. Weber, and Alfred Früh, "Data Ownership: Taking Stock and Mapping the Issues," Chapter 4 in *Frontiers in Data Science*, Matthias Dehmer and Frank Emmert-Streib, eds. (Boca Raton, Fla.: CRC Press, 2017), https://www.taylorfrancis.com/books/e/9781315156408/chapters/10.1201/9781315156408-4.
48 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0009:EN:HTML.
49 Wolfgang Kerber, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, Joint Discussion Paper Series in Economics No. 37-2016, Philipps-University Marburg, School of Business and Economics, Marburg, Germany, 2016, https://www.econstor.eu/bitstream/10419/155649/1/870294326.pdf.
50 Tal Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data," *Seton Hall Law Review*, Vol. 47, Issue 4, Article 2 (2017), pp. 995-1020, https://scholarship.shu.edu/shlr/vol47/iss4/2/.
51 Nestor Duch-Brown, Bertin Martens, and Frank Mueller-Langer, "The economics of ownership, access and trade in digital data," JRC Digital Economy Working Paper 2017-01, European Commission, 2017, https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf.
52 For downstream consequences of this feature, see Darcy W. E. Allen, Alastair Berg, Chris Berg, Brendan Markey-Towler, and Jason Potts, "Some economic consequences of the GDPR," *Economics Bulletin*, Vol. 39, Issue 2 (April 2019), pp. 785-797, https://ideas.repec.org/a/ebl/ecbull/eb-18-00834.html.
53 Zarsky.

54 Colin Bennett and Robin Bayley, RM, 2016. "Privacy Protection in the Era of 'Big Data': Regulatory Challenges and Social Assessments," in *Exploring the Boundaries of Big Data*, Bart van der Sloot, Dennis Broeders, and Erik Schrijvers, eds. (Amsterdam: Amsterdam University Press, 2016), pp. 205-227, https://www.colinbennett.ca/wp-content/uploads/2016/05/privacy-protection-in-the-era-of-big-data.pdf.

55 Vint Cerf, "Keynote Address," Federal Trade Commission Internet of Things Workshop," Federal Trade Commission, Washington, D.C., November 19, 2013, pp. 118-152, https://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf.

56 J.R. Raphael, "Meet Google's 'Data Liberation Front,'" *PC World*, September 14, 2009, https://www.pcworld.com/article/171966/Meet_Googles_Data_Liberation_Front.html.

57 Adam Thierer, "The Pursuit of Privacy in a World Where Information Control is Failing," *Harvard Journal of Law and Public Policy,* Vol. 36, No. 2 (March 2013), pp. 410-455, https://www.harvard-jlpp.com/wp-content/uploads/sites/21/2013/04/36_2_409_Thierer.pdf.

58 Darcy W. E. Allen and Chris Berg, "Subjective Political Economy," *New Perspectives on Political Economy*, Vol. 13, No. 1-2 (2017), pp. 19-40, https://www.cevroinstitut.cz/data/nppe-13.pdf.

59 Judith Jarvis Thomson, "The Right to Privacy," *Philosophy and Public Affairs*, Vol. 4, No. 4 (Summer, 1975), pp. 295-314, file:///C:/Users/ivan.osorio/Downloads/thomsonPrivacy1975.pdf.

60 Demsetz, "Toward a Theory of Property Rights."

61 For more on blockchain, see Chris Berg, Sinclair Davidson, and Jason Potts, *Understanding the Blockchain Economy: An Introduction to Institutional Cryptoeconomics* (Northampton, Mass.: Edward Elgar Publishing, 2019) and Berg, Davidson, and Potts, "Byzantine political economy, SSRN, March 2019, https://ssrn.com/abstract=3344110.

62 For a description of the opportunities arising from the "crypto city," a framework that introduces distributed data ownership and exchange as an alternative to the planned and centralized smart city model, see Jason Potts, Ellie Rennie, and Jake Goldenfein, Potts, J, Rennie, E and Goldenfein, "Blockchains and the crypto city," *Information Technology*, Vol. 59, No. 6, pp. 285-293, https://www.degruyter.com/view/j/itit.ahead-of-print/itit-2017-0006/itit-2017-0006.xml.

63 Darcy Allen, Chris Berg, Anastasia Pochesneva and Jason Potts, "Blockchain and the New Economics of Healthcare," May 30, 2019, SSRN, https://ssrn.com/abstract=3396218, or http://dx.doi.org/10.2139/ssrn.3396218.

64 For an in-depth discussion of this phenomenon, see Berg, *The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change*.

About the Authors

Chris Berg is a Senior Research Fellow at RMIT Blockchain Innovation Hub. He is one of Australia's most prominent voices for free markets and individual liberty, and a leading authority on overregulation, technological change, economic freedom, and civil liberties. Dr. Berg is the author of nine books, including *The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change* (Palgrave Macmillan) and the forthcoming *Understanding the Blockchain Economy: An Introduction to Institutional Cryptoeconomics* (with Sinclair Davidson and Jason Potts, Edward Elgar). He is an Adjunct Fellow with the Institute of Public Affairs, is on the academic board of the Australian Taxpayers' Alliance and the Samuel Griffiths Society, and is a Research Associate at the University College London Centre for Blockchain Technologies. He is also a founding board member of the Worldwide Blockchain Innovation Hub and the International Society for the Study of Decentralised Governance. His website is chrisberg.org and is on Twitter at @chrisberg.

Sinclair Davidson is Professor of Institutional Economics at the RMIT Blockchain Innovation Hub at RMIT University, an Adjunct Fellow at the Institute of Public Affairs, an Academic Fellow at the Australian Taxpayers' Alliance, an Adjunct Economics Fellow at the Consumer Choice Center, and a Research Associate at the University College London Centre for Blockchain Technologies. He is a member of the Centre for Independent Studies Council of Academic Advisers. Sinclair has published in academic journals such as the *European Journal of Political Economy*, *Journal of Economic Behavior and Organization*, *Economic Affairs*, and *Cato Journal*. He is a regular contributor to public debate. His opinion pieces have been published in *The Age*, *The Australian*, *Australian Financial Review*, *The Conversation*, *Daily Telegraph*, *Sydney Morning Herald*, and *The Wall Street Journal Asia*. He blogs at Catallaxy Files and Tweets at @SincDavidson and @Cryptoeconomico.

COMPETITIVE ENTERPRISE INSTITUTE

The Competitive Enterprise Institute promotes the institutions of liberty and works to remove government-created barriers to economic freedom, innovation, and prosperity through timely analysis, effective advocacy, inclusive coalition-building, and strategic litigation.

COMPETITIVE ENTERPRISE INSTITUTE

1310 L Street NW, 7th Floor

Washington, DC 20005

202-331-1010

cei.org