SELLING PRIVACY

By

Patricia Sanchez Abril*

Take a moment to think of something that is private to you – something you might not want to share with the entire world. It may be your phone number, your salary, or your darkest secret. Now ask yourself what that information is worth. More specifically, at what price, if any, would you sell this data? If your secret is sellable, what terms would you impose on the buyer, if you could? What consequences would you be willing to risk?

There can be no doubt that privacy already has a price. [1] Everywhere we turn we see evidence of personal information propertized. Supermarket rewards clubs, frequent flyer miles, and coupons are all now-common examples of benefits conferred on consumers as *quid pro quo* for their names, addresses, buying habits, and other information. Some businesses barter discounts for consumer endorsements (good reviews, Facebook "likes," FourSquare "check-ins") that boost their reputations or internet traffic. Personal data is an unbridled commodity and its transfer is our information economy's defining business model. Data is constantly traded, bartered and even sold.[2] But personal data also represents identity, reputation, and personhood. A digital dossier is an individual's face in society – one with both economic and dignitary value. As evidence of this value, social media profiles are bequeathed in wills[3] and reputation services are profitably cleansing people's reputations.

But the "sale" of privacy is unregulated and, some argue, unjust.[4] Individuals are rendered powerless under the current system: They sell their information cheaply, for nominal or fleeting benefits, but then lose the ability to access or alter it. Individuals then become vulnerable to scrutiny through a one-way mirror by employers, corporate interests, and others, and are thereby made susceptible to a variety of insidious social ills, from pricing discrimination to irrebuttable reputational harm. The problem is one of lack of control over the personal information.[5]

Both industry and academia have addressed the lack of personal control over information. Some companies have set up privacy exchanges, brokering the sale of private information between advertisers and individuals. Although daily life constantly requires that we give away information about ourselves, the idea of *selling privacy* – that is, whether private data should be sold at all -- poses ethical questions.

Others have gone further, suggesting that not only should private data be freely tradable and alienable, but that the law should make it subject to a legally enforceable property rights regime, or *propertize* privacy. Scholars such as Richard Posner and Lawrence Lessig have considered the ramifications of using an intellectual property model to govern personal information.[6] Intellectual property law is the framework that protects information, so it was intuitive for scholars to look there first when considering how the law could best protect information privacy. Moreover, the rules of property appeal to us as a society because they have always guided our behavior when it comes to protecting what is (or we perceive to be) ours or within our control. While propertized privacy has stirred heated academic debate, most agree that gargantuan legal and logistical hurdles render the proposition unfeasible.[7]

*Associate Professor of Business Law, University of Miami School of Business Administration

Today, the asymmetry – and ubiquity -- of modern privacy transactions reignites the debate about the selling of privacy. [8] Technology now can ease some of those early logistical challenges.[9] Although the law does not acknowledge a property interest in private information, the market has already commodified private data. But burning ethical and legal questions remain regarding the desirability of selling privacy and the law's response to it. At the core of these questions is how we value privacy and balance it against freedom of speech.

This chapter explores the questions associated with selling and propertizing privacy. Should we be able to *own* ourselves, that is, control the bits and bytes of our representative personal information scattered about the Internet? If so, should we also be permitted to commoditize ourselves by *selling* our privacy? If private information is sold, to what extent should the law protect information subjects from their own transactions? Should private information be made subject to a regime of legally enforceable property rights like intellectual property?

It has become apparent that the law cannot treat private data as it does intellectual property. Privacy interests are dissimilar to property interests in intellectual creations, even though they may share some justifications and foundations. Practically-speaking, such regulation is not imaginable today in a way that respects freedom of speech. However, concepts endemic to intellectual property can play an important role in informing the evolution of privacy and allowing individuals control over their data.

Part I lays out the market for privacy in the context of the current environment. Part II charts the history of U.S. privacy law, querying whether it is equipped to address modern threats. Part III outlines the arguments for and against selling privacy. This debate reveals the law's conundrum in protecting privacy – tensions between morality and economics, dignity and control. Part IV examines how intellectual property concepts can inform the evolution of privacy and protect its associated values. Part V concludes.

I. A MARKET FOR PRIVACY?

People sell privacy, or access to themselves, all the time. Consider celebrity endorsers, who lend their names and alleged opinions to promote a product, or reality stars trading their intimacy for notoriety. Authors of autobiographies agree to chronicle the details of their lives for a publishing contract. Erotic models bare their bodies for compensation. Human subjects are often compensated for their participation in research.

In these transactions, information subjects agree to forego their privacy (as to their preferred cereal, details of their past, the minutia of their daily lives, or their private parts) for benefits. Public curiosity gives value to the transferred information, and its price is negotiated. Although some may snub those who live their lives indiscreetly or call too much attention to themselves, the morality of these privacy sales is seldom called into question.

One reason for this acceptance is that it is an exercise of free will. Contract law ensures that the subjects freely consent and realize a benefit from these transactions. It limits the enforceability of bargains made under duress, fraud, and undue influence to ensure that the assent is real.[10] Since these contracts are negotiated in the context of a business relationship, the process ensures that the parties relinquishing control do so knowingly and within an acceptable power differential.

Another reason our society accepts these privacy markets is because they are protected by the law's safety net. Besides contract, different laws ensure the deals do not exploit the subject or

the general public. Consumer protection laws govern the use of endorsements and testimonials in advertising.[11] Criminal law prohibits suggestive images of minors.[12] Tort law punishes the commercial use of a person's name or likeness without consent.[13] Employment and labor laws protect the rights of workers in the entertainment industry.[14] Detailed administrative rules protect the rights of human subjects participating in experiments.[15] And intellectual property law ensures that the endorser retains control over who holds the right to his endorsement and how it is transferred.

Digital technology has facilitated widespread data exchange. Many of these exchanges involve consent or, at the very least, an initial affirmative act of disclosure on the data subject's part. The internet's defining business model involves users giving their personal information, or access to themselves, in return for access to services, discounts, or other benefits. Facebook built an empire as a vehicle for the interpersonal exchange of its users' private information.[16] But once this data leaves its subject, it acquires a life of its own, leaving the subject susceptible to unforeseen harms.[17] Shopping preferences, age, travel patterns, credit card transactions, allergies, political and social causes, wish lists of books and films, family photographs, third party commentary, contact lists, and other previously unavailable data amalgamate to form an individual's digital persona.[18] The collection and interpretation of this data at the hands of marketers, statisticians, employers, and even busybodies carries personal and dignitary implications, especially when its analysis was unconsented to.

For the first time in human history, the private minutia of everyday life has economic value.[19] Before the era of digital information, the costs of collection, dissemination, and information mining were prohibitive. Today, "cheap processors, cheap networks and cheap sensors"[20] have transformed these products of the human mind into the treasure troves of industry. The magnitude of big data is staggering; U.S. firms spend $2 billion a year on personal data collection.[21] The nation's leading data broker has an estimated 500 million consumer profiles with an average of 1,500 data points per person, mined from 50 trillion data transactions per year.[22] The economic value is extracted not from the data, but from what it tells us. For example, credit card companies mining customer data have found that people who buy anti-scuff pads for their furniture are less likely to default on debts.[23] On a smaller level, mining the internet for evidence of a job applicant's personal history can inform hiring. This knowledge can contribute to efficiency and drive business decision-making.[24] It is no wonder that in in describing the digital world, former Google CEO Eric Schmidt refers to personal information and identity as both "commodity" and "currency."[25]

Data also carries social value. Google uses the search engine's keyword trends to produce a daily estimate the occurrence of influenza and dengue.[26] Identifying flu outbreaks promises to limit them. Predictive analytics of people's behavior patterns and locations has helped law enforcement allocate resources effectively to identify offenders and prevent criminal activity.[27] And digital data has contributed to solving social, public health, and security problems around the world. The transparency of open information has certainly uncovered many deceitful employees, spouses, and fraudsters and deterred others' bad behavior.

But personal information has a different kind of value to its subjects. Our ideas, opinions, images, and how we choose to present ourselves to certain audiences are all expressions of the human mind and constructions our identities, and by extension, our dignity and autonomy. Lawrence Lessig noted, "your hard drive is you."[28] Years later, as Schmidt put it, "we are what we tweet."[29] Relinquishing all control over our information in a permanent medium[30] makes us too vulnerable, especially when we lose the ability to consent, determine its

uses, and object to its interpretation and disclosure. Target was able to determine which of its shoppers were in the early stages of their pregnancies – a fact which many women prefer not to divulge – by tracking their purchases.[31] We expect others not to use or abuse that information, but that is not a realistic expectation after something of value has left our control.

The lack of individual control over defining information also poses serious risks, both on individual and societal levels. When personal information is released in the permanent digital record, it can result in intrusion and become subject to irrebuttable interpretation by invisible audiences. When Target sent coupons for baby items to one household, it revealed a pregnancy before it was out in the open.[32] This can become vehicle for reputational and physical harms[33] and a backdoor to illegal discrimination and harassment.[34] Imagine the price of an airplane ticket increasing *just for you* because the airlines know you are flying to your own wedding – or employers, insurance companies, and health care marketers buying information about a person's genetic propensity to disease to draw conclusions therefrom. These incidents would be doubly unjust if their assumptions turned out to be wrong. Monitoring invites insecurity and limits freedom. A society under surveillance is one that is controlled, whose forum for democratic discourse is stymied, and whose freedom to innovate socially and culturally is thwarted.

And yet, unlike the well-accepted endorsement, modeling, or reality television agreements, this new privacy market is not founded on free will or a bargained-for exchange. The Internet reduced the cost of contracting, and in doing so, weakened the notion of consent. Modern life presents a Hobson's choice: an online presence or privacy.[35] With no ability to bargain or go elsewhere, the "choice" of whether to accept contract terms is ultimately a choice regarding social participation. For most, the Internet's convenience, socialization, and communication are too essential to forego. In fact, people with little Internet presence are viewed suspiciously, like they are hiding something nefarious or anti-social.[36] Most people do not have the time, money, or inclination to seclude themselves in such a way.

Current markets for personal information are replete with failures such as disparities of power,[37] information asymmetries that preclude informed choice, and inaccurate pricing of personal information.[38] Privacy policies tend to be overly complex, can be unilaterally changed on whim, and ultimately, allow invasions of privacy under the farce of consent.[39]

Privacy exchanges have prohibitively high transaction costs, because they should ideally reflect the nuance and relativity of people's privacy preferences.[40] This is true offline and on, but much more onerous in context of power disparities. In our introductory examples, the privacy traders or their agents negotiate the terms of the disclosure – the endorsement, the appearance, or the photographs – within a continuing business relationship. But imagine a user proposing to Facebook: "You can sell my contact list with the following exceptions:" or telling Google: "You can keep a record of my searches, but not ones related to medical conditions." It would be inconceivable to value each bit of private information, then negotiate and contract over its appropriate destination and uses ex ante. Transaction costs are also high for consumers reacting defensively. Even for the most sophisticated consumers, the costs involved in identifying offending companies and protective technologies are prohibitive, not to mention purchasing self-help devices and deciphering the multitude of privacy policies and security settings that touch their data daily. [41]

In addition to an impaired exercise of free will, the current market transactions governing privacy and data collection are, by and large, unregulated by law and uncontrollable by individuals.[42] The robust safety net of laws –consumer protection, crimes, torts – that supports traditional privacy exchanges is lacking in the online world's privacy trades. Although the FTC's

Fair Information Practices (FIPS) have been influential in framing the law and policy surrounding the collection and use of personal information, they do not have the force of law. [43] The Electronic Communications Privacy Act of 1986, which protects the private transmission and storage of electronic data, provides little guidance and redress in a digital world since it was written long before the rise of the internet.[44] The dearth of relevant federal privacy legislation makes online privacy entitlements spotty and confusing at best.[45]

But perhaps most detrimental is that, by design, privacy law is only reactive. Since a system of liability rules, the holder of a privacy right receives compensation only after an involuntary transfer.[46] In other words, privacy law seeks to remedy the shamed after the shaming and does little to control the offense before it occurs. Privacy law does not give individuals a monopoly right in their private facts. As liability rules, privacy law only provides the wronged individual with an opportunity to seek remedy for invasions after the damage is done.

Since people do not have property rights in their private information, the downstream transfer of the divulged information by the celebrity, the author, the reality star, the model, and the consumer is governed by privacy law. The right of publicity, stemming from privacy law, gives the famous endorser the right to sue anyone who appropriates his commercial identity without his consent.[47] Although one may argue that the value of an autobiography is the access to certain author's own life perspective and opinions, the law gives no proprietary interest in those thoughts and dreams, only to their tangible expression.[48] Similarly, models and reality stars do not "own" the intimacy of their own bodies and homes which they allow cameras to invade. Once such information is out in the open, its subject can no longer control its use and destination.

On the other hand, intellectual property law acts as a gatekeeper. A property entitlement can only be transferred with the consent of its holder. This model allows for the subject to control the information, even after it has left his hands.

This retention of downstream control over information has spurred proposals to propertize private data. Since the late nineties, notable academics and economists have suggested personal information should be recognized by law as a form of property.[49] That is, they have put forth that the law could protect such information as it does intellectual property.[50] Personal information property owners (a.k.a. individuals) could then barter, sell, and control their information in the marketplace. In fact, many have a sense that they have a right to exclude others from access to their private data.

In the 1999 edition of his book *Code and Other Laws of Cyberspace*, Lawrence Lessig suggested that private information should be treated like intellectual property as one way of regulating cyberspace.[51] Lessig saw a privacy market facilitated by technology where individuals can control the transfer of their information beyond its first disclosure. Although his incendiary proposal was before the days of Big Data and even widespread social media, Lessig was prophetic in envisioning the privacy challenges that would eventually arise in the digital space and creative in proposing how experiments with law and technology could meet those challenges. In the years since his proposal, while much academic debate ensued, neither privacy nor intellectual property law have achieved a solution.

In the meantime, the online privacy environment has continued to erode as technology and market forces advance. The existence of a privacy market is no longer a hypothetical; it is a reality. Some companies have launched marketplaces for personal data that promise transparency for the sellers and better data for the corporate buyers.[52] One startup offers users $8 a month in

return for unrestricted access to their social media accounts and credit card transactions.[53] For a 35% fee, another company will broker the sale of a person's data to advertisers.[54] One privacy service's slogans read "It's your data. Own it." and "Small data is the new oil."[55] Eric Schmidt predicts that the commodity of privacy will give rise to multiple new industries, such as "identity managers … as common as stockbrokers and financial planners"[56] and a "black market where people can buy real or invented identities."[57] This reality now forces us to examine the role of property rules, if any, in a privacy arena overrun by nimble technologies and aggressive market forces. We begin by examining the historical intersections of privacy and property.

II. THE U.S. PRIVACY LAW AND ITS UNEASY RELATION TO PROPERTY

U.S privacy law is comprised of federal and state statutes, tort law, federal and state constitutional law, evidence law, contract law, and other sources encompassing a diverse array of interests and harms from fundamental constitutional rights to the disclosure of credit reports and personal secrets. [58] In general, privacy law can be defined as the government's ability to restrict the penetration into one's private space and the use, transfer, or disclosure of certain personal information. Privacy law is a relatively modern concoction: in roughly a century it has evolved as a result technology's continuous challenges. Through its history, it has been compared, justified, and distinguished in reference to its more well-established cousin, intellectual property.

It stands to reason that intellectual property law, firmly established by the U.S. Constitution, [59] would be a point of comparison for a burgeoning legal right. Both areas of law involve intangible human products that are closely tied to us as people – because we made them, because they represent something about us, or both.[60] Both privacy and intellectual property both suffer from a daunting breadth of subject matter covering notably diverse issues. [61] And both share a common purpose: control of information. [62]

Unlike intellectual property law, American privacy law lacks a unifying principle or guiding document.[63] Before 1890, privacy in the U.S. was a "vague social concept"[64] – hardly the foundation for a legal right. Its roots, if any, were in principles of property; privacy harms found redress under the assumption that reputation was essentially a proprietary interest.[65] Property – in the sense of space and land – also influenced privacy law in a direct way: The shift from an agrarian to an industrial, densely populated society forced a renegotiation about the limits of privacy and its regulation.[66]

1890 brought privacy law its most significant impetus, with the publication of Samuel Warren and Louis Brandeis's landmark piece advocating for a right to privacy. This highly influential 1890 Harvard Law Review article described a right to an inviolate personality[67] and set the stage for the creation of civil remedies against privacy intrusions.[68] In supporting their innovative legal right, the authors drew from the deep-rooted law of intellectual property. Although the authors ultimately rejected property as adequate protection for privacy, they argued that the notion underlying copyright protection was, in fact, the same as that which would undergird a privacy right: "an inviolate personality."[69] For example, although the common law of copyright (protecting unpublished manuscripts against the unauthorized dissemination) dressed as a property right, the authors argued that its value was "found not in the right to take the profits arising from publication, but in the peace of mind or the relief afforded by the ability to prevent any publication at all."[70]

Ironically, despite the dignity-centered essence of Warren and Brandeis's argument,[71] the concept of privacy grounded in dignity did not come to shape U.S. privacy law. Instead, the notion of privacy as control took hold over American jurisprudence and policy.[72] In conceiving

private information as the object of control, American law has implicitly focused on the holder's governance over his information.[73] Generally put, when something is tightly controlled, it is protected by privacy law; but when that object or information becomes free, it can no longer be private. Since control is the parlance of property, it is hard to imagine this conception of privacy divorced from the question of property. Privacy law evidences the push-pull of property logic in the jurisprudence of the Fourth Amendment, workplace privacy, privacy torts, and publicity rights.

Fourth Amendment law is replete with references to property – in the sense of control or dominion, as the basis for a privacy right. Margaret Radin noted the intimate intertwining of property and privacy. She wrote:

> The fourth amendment is worded not in terms of privacy but rather in terms of protecting people's "persons" and people's relationships with certain aspects of their external environment (their "houses, papers, and effects"). It has a great deal to do with property, insofar as property is about the relationship between people and things.[74]

In *Olmstead v. United States*, the Court held that wiretapping was not an invasion of privacy under the Fourth Amendment because it was not a physical trespass into the privacy of the home.[75] In his influential dissent, Justice Brandeis took pains to distinguish privacy from the spacial and physical. Justice Brandeis argued that the makers of the Constitution recognized that "only a part of the pain, pleasure and satisfactions of life are to be found in material things," and for this reason "sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations."[76] Later cases such as *Katz v. United States* incorporated Brandeis's view, separating the property logic to allow privacy interests to stand on their own.[77] The awkward relationship between people's privacy interests and the physical domains they control continues to be at the center of Fourth Amendment quandaries, especially when the privacy in question is dislodged from physical property or control.[78]

U.S. case law on workplace privacy often casts employee privacy in terms of the employer's property rights.[79] Since the workplace and its resources are the employer's property, the logic goes, the employer is generally free to dictate their permissible uses. This assumption is critical to the "reasonable expectation of privacy" analysis.[80] This restriction may arise constitutionally, legislatively, or in tort law, but in its essence it must be "reasonable" and not unduly erode the employer's property rights.[81] At the core of the law governing workplace privacy is the inquiry into whether the employee had a reasonable expectation of privacy in the intruded space.

Property's influence is also apparent in the four privacy torts. Although heavily influenced by Warren and Brandeis's law review (which rejected property as a basis for privacy), two of the four privacy torts directly speak the language of property in granting an individual the right to control his image. False light invasion of privacy applies when information that casts a defamatory (but not necessarily false) shadow is intentionally or recklessly published.[82] The tort of appropriation is the basis for publicity rights in the U.S. Publicity rights are no more than a tort dressed in intellectual property clothing. Although often cast as an intellectual property right, publicity rights are liability rules granting celebrities the right to prohibit unauthorized commercial use of their identities. By extension, celebrities can also grant exclusive rights to third parties to exploit their identities.[83]

Other notable privacy laws interlink with property. The tort of breach of confidentiality and trade secrets law both treat confidential information as a kind of property that can be transferred -- and whose unwarranted disclosure is remedied.[84] These laws protect the financial interest in information and reputation and are more akin to the utilitarian precepts underlying intellectual property law. Trade secrets give priority over knowledge to the creator of that knowledge, who has not only worked to create it, but also to hide it. But the costs of protection are high. Once leaked, the law gives no remedy for the disclosure of trade secrets and personal information.[85]

Despite its many intersections with property and property-logic, privacy remains a liability rule and its enforcement burden rests with its subject, when damage is done. Even those privacy rules that most approximate property do not provide rights that are enforceable against the world at large, but rather only against those touched by the obligation. Privacy does not give a right to exclude others or to prevent the transfer of information. As Landes and Posner have observed, "the tort of privacy has never prevented the intended recipient of a letter, or anyone else who has lawful access to a private document, from 'spilling the beans.'"[86]

As a result, many privacy laws are neither successfully deterrent nor adequately remedial. Traditionally, this was not a burning social problem because it was not privacy law but social norms, trust, and communication hurdles that prevented people from "spilling the beans." Today, the digital space has transformed or removed these privacy proxies and technology and market forces are attempting to forge others in their place. But can a market step in to secure privacy? We explore the arguments for and against a sanctioned market in privacy in the following section.

III. SHOULD PRIVACY BE SOLD? SHOULD PRIVACY BE PROPERTIZED? THE DEBATE

Private information is a unique thing. It is real, but it is subjective. It has the most intimate of personal value, but it is not always secured. To build relationships it must be shared, but then it cannot be controlled. It is an inseparable part of our personas, but it can be given away. It can be sold, but it is not property. And once it is gone, it cannot be recreated.

The following section examines the multifaceted moral, legal, and social arguments surrounding the sale of private information. The debate explores the desirable limits of the sale, commodification, and propertization of privacy. Should private information be commoditized? Since some markets have already commoditized personal information, should the law grant intellectual property-like rights in it?

A. For a Market in Personal Data

The Chicago school of economics proposed a basic claim: Everything is already commodified.[87] Colloquially-speaking, "everything has a price," although sometimes that price may exist only implicitly in the "shadows" without formal legal or open market recognition. This universal commodification, economists argue, is beneficial to society; legal rules should not prohibit the sale of certain services and goods.

Personal data is already commoditized, as evidenced by the Internet's central business model. From this point of departure, scholars have argued that recognition and regulation of a privacy market would serve to empower individuals.

1. Individuals should have the ability and freedom to negotiate their privacy.

In his 1981 book, *The Economics of Justice*, Judge Posner discussed the feasibility of a property rights system in information. He argued that reliance on a property rights system for privacy was precluded by two costs: the disproportionate cost of enforcing a property right in information (relative to the value of the information) and the high cost of tracing information to its origin.[88] Posner contended that "the purpose of a property right, or of according legal protection to secrecy as a surrogate for an explicit property right, is to create an incentive to invest in the creation of information. Where information is not a product of significant investment, the case for protection is weakened."[89]

Since 1981, the world has changed significantly. Digital technologies have reduced the costs of both enforcing and tracing information – Posner's two objections. In the face of this new reality, Lawrence Lessig suggested a property right in information, or the entitlement to privacy as a default – like a copyright or a patent.[90] Facilitated by technology, this property-like right would eliminate the need to make contracts and carry both the rights to exclude and transfer information to others. Further, propertized privacy would be enforceable against the world, not only parties in privity of contract.

Underlying these arguments is the libertarian notion of self-ownership: individuals must have the freedom ability to value their privacy and negotiate easily over it. [91] And people naturally have different privacy tolerances. [92] Some document every minute of their lives on social media; others abstain from sharing entirely. A system of propertized privacy forces those who want to take or use private data to reveal themselves, request it, and pay. Individuals regain control over the disclosure, use, and destination of their information.

A sanctioned privacy market also gives individuals the ability to establish a fair market price for their privacy, one that is in keeping with their personal privacy tolerance. Ian Ayres and Matthew Funk have proposed a "name your price" system in which consumers can set the terms under which they are willing to listen to telemarketing calls.[93] Consumers with a low tolerance for such calls would price their time and information out of the market; but consumers willing to receive these calls could do so for a stated price per minute (akin to a reverse 1-900 psychic hotline system).[94]

Online information brokers have recently adopted this idea of self-selection to bring together willing divulgers with curious marketers.[95] This model promises transparency, predictability, and empowerment for participants, while avoiding intrusions on the privacy-wary. However, some would argue, in its current state, private information is too slippery because there is no entitlement to transfer. Why would marketers pay for something they can legally gather for free?

2. Fairness dictates that individuals should share the benefit of their informational contributions.

Advocates for a privacy market also focus on fairness. Technologist Jaron Lanier argues that the current digital economy is based on a fundamental injustice: information gatherers take data under the guise that it is free and based on consent, but in fact, consumers have no real choice and supply all the raw materials for their profits.[96] These information collection practices are exploitative of individuals and detrimental to society.

Business models built on tracking, behavioral marketing, and other types of information collection profit on personal information they acquire at little or no cost. Individuals play an insignificant economic role in this market for information, yet supply all of it and bear the

downstream risks of its disclosure.[97] Relative to the economic value the collecting entities reap, the argument goes, consumers are being fleeced. Propertizing personal information would simply give consumers leverage and allow them to benefit from the existing market.[98]

Building on arguments of fairness and autonomy, Lanier envisions individuals receiving a nanopayment every time their digital information contributes to the creation of knowledge.[99] But Lanier sees technology, not just2 law, as the catalyst for propertized privacy. He argues that we should recognize a fundamental right in information provenance retention, or the historical record of a digital object's source.[100] With two-way linking of information, data carries its source anywhere it travels, thereby facilitating compensation to its author.[101] Information linked to its source could also carry with it terms and conditions on its use, thereby accommodating consent-based systems of privacy. He proposes that individuals set the value at which they are willing to disclose any data that can be measured from that person's state or behavior, including personal preferences, opinions and even speech patterns for translation software algorithms.[102]

3. A privacy market will result in better information and overall collective wellbeing.

The privacy market thinkers underline that privacy exchanges based on free will and fair market prices would benefit buyers and sellers alike and thereby improve collective well-being. For individuals, a privacy market is an exercise in freedom and control, allaying intrusion concerns while allowing the unconcerned to profit. For marketers, such a system would create efficiencies and reduce overinvestment in consumers who do not want to be reached. Information gatherers would be assured a more reliable product and avoid wasteful overinvestment in soliciting information from people unwilling to disclose it.

Because there is no scarcity of personal information in the marketplace, businesses rely on what they collect. As they say, you get what you pay for. Privacy-wary consumers might lie to safeguard their personal data or to save time. Patricia Mell has argued that a property rights regime might enable firms to make fewer wasteful investments in personal data and to develop higher quality databases, since individuals would presumably agree to release personal data to firms from whom they would be willing to receive information, and would have less incentive to lie as a way to protect their privacy.[103] Getting paid for personal information will create incentives to improve information, allow people to make mutually beneficial trades, and ultimately benefit society.

4. Treating privacy like property will make it more valued.

Advocates of a privacy market propose that market recognition of the value that individual information contributes to society will cause individuals to be more aware of it, protect it more, and value it more.[104] Property is the language our society uses when something has value; property is the system we use when we really mean to control something. Lessig has suggested that reframing the privacy debate into property terms will arouse people's passions for it.[105] This newfound value recognition may even effect social change. He notes: "if we could see one fraction of the passion defending privacy that we see defending copyright, we might make progress in protecting privacy."[106]

B. Arguments Against a Market in Private Data

An opposing chorus of scholars has predicted that establishing a property right in personal information would be catastrophic on societal and individual levels.[107] Supporters of this view argue that propertized privacy would be bad social policy, encouraging data transactions that will have negative social repercussions. Selling and propertizing personal data in a free market, they contend, is a moral, social, and political question, not merely legal and economic one. They focus on the inherent inalienability of interests associated with privacy and predictive arguments, focusing on the foreseen effects of such a data market.

1. Privacy is inalienable.

Privacy is often called "sacred," or "sacrosanct."[108] Some attribute privacy's revered position to its nature as a civil liberty.[109] Others consecrate it inalienable because of its intimate bond with who we are, our individuality, and our human dignity.[110] Those who value privacy as a civil liberty and personhood argue that a privacy market would defile a right whose "value" is beyond commoditization.[111]

Classical economics proposes the view that markets are inert and neutral. That is, that they do not affect the goods they exchange. Scholars have cautioned against this perspective, arguing that financial incentives have corrosive tendencies that demean values that are beyond price to society. [112] A privacy market, just like markets for babies, kidneys, and sex, cheapens an essentially moral value by treating it as an instrument of profit.

One of the loudest critiques of a propertized privacy system is that it creates a world which turns something that is – or should be – a basic civil liberty into a mere commodity.[113] Margaret Radin has defined a "commodity" as a social construction that is "capable of being reduced to money without changing in value, and completely interchangeable with every other commodity in terms of value."[114] In accepting a property right in privacy, the argument goes, we would likewise accept the treatment of our private information as an instrument of profit and use, no different than a husk of corn or a concert ticket.[115] As Professor Pamela Samuelson has written, "[i]f information privacy is a civil liberty, it may make no more sense to propertize personal data than to commodify voting rights."[116]

Some have argued that privacy is more than a right, but rather something defining and inseparable from the person. Radin's personhood theory proposes that certain objects are so intertwined with people that they become part of who they are and how they see themselves. [117] She argues that the tighter the bond between person and object, the more control the subject should be able to exert over it – and the less alienable it should be. Radin contends that an object is closely related to one's personhood "if its loss causes pain that cannot be relieved by the object's replacement."[118] Certain private information is such an object; a person's reputation, image, history, medical records, reading lists, and political opinions are a few. Since privacy is part of the person, it is inseparable and therefore inalfienable. It therefore should not be transferred, sold, or waived.

Ultimately, these scholars argue that monetizing privacy disrespects human beings by figuratively dismembering them and treating them as instruments of profit. This, in turn, weakens society's moral fiber.

2. Markets Promote Inequality.

Every property system creates "haves" and "have nots." The same, say critics of a

privacy market, would be true for a market in personal data. Who would be the first to "sell" their privacy? The poor. Whose information would be least valuable to marketers and other data gatherers? Those with the least buying power. Who would then bear the reputational risks and harms of having sold their privacy, thereby reducing their employability? The already underprivileged. A market in privacy could serve to perpetuate a vicious socio-economic cycle from which it is already difficult to break.

Markets can create exploited populations. A market in a contested commodity aggravates exploitation by financially coercing a person out of something that is part of his human dignity. Professor Michael Sandel offers the example of propertization of blood donation. When giving blood went from a charitable act to a compensated transaction, the pool of donors became limited to "Skid Row residents desperate for quick cash."[119] Propertization stripped the donors of their dignity and the positive feelings associated with a charitable act and exploited an already-downtrodden group.

Compare, then, what propertization would do to privacy. In the blood trade example, a poor person's blood has the same value as a rich person's. But the same is not true for personal information, where the data of the wealthy represents more buying power and influence. The burden on the poor would be exacerbated. Unlike blood, privacy does not regenerate. A privacy market would allow the rich to conceal information about themselves, while the poor would be more likely to suffer the illicit consequences of the data trade.[120]

A privacy market would further entrench a caste system of privacy. Indeed, money can already buy some privacy. In physical space, the rich have the luxury of bigger homes shielded from prying eyes and public relations firms and lawyers to secure their privacy and reputations. Online, this privacy inequality is being replicated. For a significant fee, online reputation management companies can monitor an individual's or business' reputation through search engine optimization, by creating, disseminating, and promoting positive content, and even assisting in eliminating damaging online remarks.[121] Hired gun reviewers are also available to artificially boost ratings or reviews on reputation systems like eBay or Amazon. This *sub rosa* reputation market leads to a favorable distortion in the reputation of those who can afford it.

The benefits of propertized privacy would accrue only to the rich, whose coveted personal information would be better compensated and who would become the privacy elite – society's new heroes with unblemished records and entrenched privileges to match.

3. Propertized privacy exacerbates market failures.

Instead of protecting individual privacy, many argue that a privacy market would erode it by legitimizing privacy intrusions and increasing the consumption of personal data.[122] Some scholars theorize that propertizing privacy would worsen the extant market failures.[123] Fueled by perverse incentives, increased trade in information would result in more trades, bad bargains, less bargaining power, less choice, and less dignity for its data subjects.[124]

These scholars contend that a property rights regime would give more economic and market power to data collectors.[125] Due to the value inherent in personal information, its commoditization would only induce its "ever more rapacious collection."[126] As Janet Gertz has noted, "any scheme based on property rights necessarily encourages alienability, and thus rather than discouraging the commercial exploitation of a person's identity, establishment of property rights in transaction data would likely have the effect of encouraging this exploitation by establishing the … institution's ownership to any and all data that a consumer provided to it for purposes of a commercial transaction."[127]

Professors Julie Cohen and Marc Lemley foresee a world where more people would also trade more of their data.[128] People are likely to be tempted to profit from something they already have. Again, the already-underprivileged would be the first to capitalize on this and would flood the market with information. But selling personal information is likely to create a false sense of bargaining power and control for the ever-more-vulnerable individual.

Behavioral economics suggests that most people will blindly accept whatever terms information collectors offer.[129] Paul Schwartz notes that the phenomenon of bounded rationality is likely to operate to vitiate any perceived power gained by a consumer in a propertized privacy regime, since the information collectors anchor the terms of the transaction to their benefit and the average consumer is likely to just trade her information. Schwartz contends that "consumers may discover that the surrender of personal information is nonnegotiable or prohibitively priced."[130] If property rights are part of a transaction, then consumers must decide which is higher: the cost of losing their personal information or the cost of doing business with a competing firm.

Professor Schwartz also suggests propertized personal data would sell cheaply, and the value would not accrue to the individual. He explains that privacy would have two values: a market value (the price at which an individual would be willing to trade his personal information) and a threat value (the price an individual would place on *not* disclosing his personal information).[131] So, a person might sell his email address for $5, however his threat value might be $3 to not divulge his email. If this person sold his email to one firm at $5 and then that firm sells it and many others for $2, the individual is both losing out on value and undermining his own threat value. Marc Lemley has predicted that the propertization of privacy would flood the market, thereby creating a vast supply of the "good" and artificially deflating the price of each person's information.[132] Given people's lack of bargaining power and bounded rationality, people would be sell their personal information at these ridiculously low values and lose the privacy that propertization set out to protect.

Ultimately, propertizing personal information gives individuals less, not more, control over their privacy. Personal information that is sold without restriction is out of its subject's control forever. The individual who agrees to participate in the data trade might only understand part of what he is agreeing to.[133] In fact, the individual may be exposing himself to discrimination or risks brought by future technologies and unforeseeable uses. After legitimately acquiring data, information collectors can use it to draw conclusions about a subject's preferences, weaknesses, price point sensitivity, and spending power – all useful tools for insidious profiling and price discrimination. Information gatherers with access to an individual's genetic materials could glean information about the subject that even she does not know.

To summarize, drawing from economic and psychological theories, scholars predict that a market for personal information would result in fewer consumer choices, unconscionable bargains, and more information asymmetries.

4. A market for privacy distorts information flows.

Information wants to be free. Predictive analytics promises many benefits to society – from business, to public health and the environment. Forcing data collectors to purchase freely-available personal data raises the cost of innovation and, as a result, creates inefficiencies and harms society. Moreover, the more that information is readily available, the harder it will be to hide truthful and nefarious facts, and this will result in a more informed and transparent society.

Scholars have long criticized privacy on the grounds that it unduly suppresses truthful facts that are better left to open judgment. As Judge Posner wrote,

> "It makes no sense to treat reputation as a 'right.' Reputation is what other think of us, and we have no right to control other people's thoughts. Equally, we have no right, by controlling the information that is known about us, to manipulate the opinions that other people hold of us. Yet it is just this control that is sought in the name of privacy."[134]

While disclosure of personal facts may cause harm or shame in some cases, a market for privacy would allow people to conceal or withhold discrediting information and manipulate the world around them.[135] The U.S. view of privacy reflects this view, promoting free speech rights over dignitary ones. Reputation is not proprietary. A robust First Amendment prohibits such reputation control. For example, copyright holders do not generally obtain moral rights.[136] In *Paul v. Davis*, the plaintiff's image had been distributed to area merchants on a flyer of "active shoplifters."[137] After being cleared of the charges, the plaintiff sued the police, claiming that this defamation had deprived him of "liberty" and "property" without due process of law. The Supreme Court disagreed. It held that reputation alone, without more tangible harm, was not cognizable as "property" or "liberty" within the meaning of the Due Process clause.[138]

Professor Neil Richards contends that propertizing personal information would limit the flow of data[139] and restrict free speech. Since information flow is a form of speech, he argues, its limitation – which would include restricting the dissemination of truthful information – would offend free speech rights.[140]

Seen in this light, the collection and accessibility of personal data achieves more benefit to society than detriment. We receive discounts and announcements tailored to our interests and our lifestyle. We save time and money. We learn who we can trust. With sunlight as a detergent, we achieve a more transparent culture. Eric Schmidt and Jared Cohen envision a world where "[a]ny would-be professional, particularly one in a position of trust, will have to account for his past if he is to get ahead" [141] and "[i]n democratic countries, corruption, crime, and personal scandals will be more difficult to get away with."[142]

Risk of exposure could even make people behave better. Landes and Posner make the case in the context of the copyrightability of unpublished letters: "Knowing that copyright protection in private, unpublished letters is weak and that these materials divulge his unscrupulousness, an author would potentially be induced to behave better, thus raising social welfare."[143]

5. A market for privacy changes behavior and limits freedom.

Markets can crowd out civic practices, altruism, intimacy, and freedom of expression. As Michael Sandel has written, "[s]ometimes, offering payment for certain behavior gets you less of it, not more."[144] A growing body of work in social psychology and behavioral economics supports the contention that in certain situations a market can weaken people's motivation, interest, or commitment to act in socially beneficial ways.[145] That is, once something is defined in market terms – with a corresponding price tag – its nonmarket value may diminish, leading to the loss of certain socially-beneficial practices and attitudes.[146]

It is easy to see how this would apply to a privacy market. Charles Fried describes

privacy as "moral capital" that builds intimate relationships, trust, and friendship.[147] Proponents of privacy's inalienability would argue that once this "moral capital" is reduced to something that can be acquired with money, it loses invaluable force as an agent of intimacy, friendship, and love. Private information is currency: disclosing one's little-known information creates an exclusive and intimate bond with the information's recipient. This, in turn, leads to healthy interpersonal relations and enhances overall social welfare and community ties.[148] On an individual level, intimacy promotes psychological and relational benefits like solace, kinship, and counsel.[149] If someone sells their "secrets" cheaply on an open market, why should I feel special when they share them with me? This could lead to an uncomfortable and socially detrimental disruption of social norms.

The introduction of a financial incentive to be monitored may also lead to self-censorship, what Jonathan Zittrain termed "press conference behavior."[150] This is strong normative pressure to fit in to well-accepted social molds, instead of expressing true opinions. The pressure to maintain "press conference behavior" suppresses individual development and social progress. As Edward Bloustein wrote, when a monitored individual "merges with the mass,"

> "[h]is opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man. Such a being, although sentient is fungible; he is not an individual."[151]

This dignity-stripping conformity also chills speech. As Justice Douglas observed, "monitoring, if prevalent, certainly kills free discourse and spontaneous utterances."[152] It limits intellectual and emotional freedom, which, as Professor Julie Cohen has argued, is essential for a civil society and a deliberative democracy. [153] Public scrutiny can also quash the rebelliousness, challenges to the status quo, and avant-garde thinking that sparks innovation and culture creation. [154] Eric Posner and Cass Sunstein have argued for the value of trail-blazing ideas that challenge the ensconced and force us to question the veracity of the accepted norms. [155]

Those who value privacy as a means to secure a deliberative democracy fear a regime that would propertize privacy. After all, something as important in safeguarding freedom should not be tradable – at any price.

III. HOW SHOULD THE LAW ADDRESS THE SALE OF PRIVACY? WHAT PRIVACY CAN LEARN FROM INTELLECTUAL PROPERTY

In the second edition of CODE, Lawrence Lessig responds to the many critics of his proposal to propertize privacy. One of his most forceful arguments is simple: it is already happening. Lessig offers a dose of practicality to a complex legal issue in reminding critics that, at this point, all efforts to salvage privacy must address its current reality. We already have a thriving market culture in which private information is bought and sold. We even have a secondary remedial market to clean up the first market's mess: to fix reputations through reputation management and protect privacy through tracking protection and data vaults.

The problem with the market is, most of the time, the sellers are not the information's subjects, and the market is replete with failures that disadvantage the individual, not the least of which is the loss of control of personal information. Remedial services are costly and therefore

not available to everyone – exacerbating the problem of privacy "haves" and "have nots." Given this situation, we must construct realistic solutions. But should these solutions be based in intellectual property?

As scholars on both sides of the privacy debate note, privacy is not intellectual property. While both intellectual property and privacy laws represent non-tangible interests, privacy is a liability rule protecting information after the harm is done, while intellectual property, as a property rule, aims to prevent information-related damage and unwarranted disclosure.

The Internet age, with its ease of information transfer at low cost, has challenged both privacy and intellectual property's relevance and social utility. Both areas are experiencing a renegotiation, particularly with their governing laws, which have been questioned and, in some instances, undermined by new technologies.[156] As Jonathan Zittrain has pointed out, the modern problems of privacy and copyright are essentially the same: the loss of control over information.[157] Zittrain anticipates that loss of control over personal information facilitated by peer-to-peer technologies will mimic the problems that ease of reproduction caused for copyrights. He states, "[t]he intellectual property conflicts raised by the generative Internet, where people can still copy large amounts of copyrighted music without fear of repercussion, are rehearsals for the problems of Privacy 2.0."[158]

Since intellectual property law is the well-established legal framework that protects information, it was intuitive for scholars to look there first when considering how the law could best protect information privacy. Intellectual property and privacy have a long history of comparison and entanglement. The rules of property have always guided our behavior when it comes to protecting what is (or is perceived to be) ours or within our control. The story of intellectual property law offers lessons for new ways of thinking about the regulation of information privacy.

A. Information has new economic and social value.

William Landes and Richard Posner offer an expansive definition of intellectual property as:

> "ideas, inventions, discoveries, symbols, images, expressive works (verbal, visual, musical, theatrical), or in short any potentially valuable human product (broadly, 'information') that has an existence separable from a unique physical embodiment, whether or not the product has actually been 'propertized,' that is, brought under a regime of property rights."[159]

Under this definition, private information may have much in common with the subject of copyrights, trademarks, and patents. In the era of Internet and Big Data, what is private information if "potentially valuable human products"?

For the first time in history, private information, no matter how trivial, can be cast as a human product of economic value. The collection and analysis of private information leads to socially beneficial outcomes, such as charting disease, deciphering traffic flows, and uncovering fraud. But does it follow that a utilitarian model would justify a market for privacy?

United States intellectual property law is premised in giving creators the incentive to innovate in ways that promote socially-beneficial outcomes. To a utilitarian, the ideal intellectual property system is one that promotes the production of more books, songs, sculptures and lawnmowers but does not unduly limit society's use and access to them. Giving creators monopoly rights over their products gives them incentives to innovate.

People do not need incentives to "create" private information. Much of what we deem

private is produced as part of who we are and the tracks we leave in society. Images, opinions, and other tidbits of personal information are human products whose disclosure is incentivized by nostalgia, narcissism, or simply a need to participate in the modern world. In contrast, other prized personal information – such as a cell phone and Social Security numbers or home and Internet Protocol addresses -- is not a product of their subject's mind, but rather a fact.

While people may not need incentives to create personal information, they may need them in order to *disclose* truthful, high quality information. Some scholars have noted the tendency of individuals to lie or give false information to protect their privacy. Given the capacity of information to lead to innovation, ensuring its quality is tantamount to realizing its social benefit. And this incentive may be even more critical than intellectual property's incentive to create because the sharing of personal information, unlike ideas, represents its loss to the individual: it cannot be recreated. As Lawrence Lessig has pointed out, private facts are different from ideas because they are diminishable: "the more it is spread, the less privacy remains."[160] So, in an important sense, the person who offers his private information suffers a loss.

That loss is more than dignitary. The donor of private information expends her time and assumes the risk of intrusion or downstream harms. She contributes, if even minutely, to the creation of knowledge, which may one day be used against her. Given these risks, a market for private information would serve to create transparency and ensure real consent before an individual gives up something of value.

As discussed above, in some comparable cases, the law regulates transactions for the exchange of personal information to protect the parties. Human subjects research is an example of a legally and normatively accepted transaction in which people give access to themselves for a socially beneficial purpose. The law ensures that research subjects receive the opportunity to knowingly consent to the transaction. A measured model incorporating legal limits and consent is more morally justified than the current system, in which invisible powers take privacy without asking or telling.

B. Information has increased dignitary value.

Personal information has always had dignitary value in shaping who we are, our security, our reputations, and our self-esteem. One could argue that the digital world, in making data permanent and easily obtainable, magnifies the harms associated with privacy breaches. In this way, it has increased the dignitary value that privacy once held. A reputation is more valuable than ever because it is close to indelible and accessible globally and with relative ease. Disclosure of private data carries multiple and unforeseeable security risks, and may fall into invisible hands in the future.

Traditionally, many have argued that privacy is a matter of human dignity and personhood.[161] A dignity-focused view of privacy emphasizes privacy as an instrument in the development of one's personality and inner self – inseparable from the persona and defining one's essence as a human being.[162] In her work on personhood, Margaret Radin suggests that we should think about property relative to its connection with personhood. Drawing on Hegelian philosophy, which says that the ownership relationship gives people an opportunity to become fully developed and autonomous, Radin eloquently argues that property is strongly justified when it becomes an inseparable part of our personas. [163] While Radin does not argue for the commodification or propertization of privacy, she views privacy as a personal interest based on its undeniable relation to personality and personhood.

European intellectual property law evidences a rich tradition of recognizing personhood in moral rights.[164] Moral rights allow the creator of intellectual property some control in the name of dignity and personhood, even when he does not physically own his creation. An artist is entitled to claim authorship of his work and to disclaim authorship if his work is altered in a manner "prejudicial to his honor or reputation" or incorrectly attributed to him (attribution rights). Integrity rights protect the artist from any intentional distortion, mutilation, or other alteration that injures his reputation.

Similarly, the conception of privacy as dignity and honor is at the core of European law and policy. Europeans have long considered the privacy of personal information to be a fundamental right.[165] The Charter of Fundamental Rights of the European Union simply states, "Human dignity is inviolable. It must be respected and protected."[166] In that light, Articles 7 and 8 provide, respectively, for "respect for private and family life" and "protection of personal data."[167] European courts have recognized that privacy can exist in public places[168] and that employees have a right to private communications, even on an employer's computer.[169]

The U.S., in contrast, summarily rejects the notion of an individual or an artist owning her reputation or controlling information about herself once it has left her hands.[170] Unfortunately, this conception has become too constrained for digital life. Anita Allen has argued that privacy rights are miscast as rights of individual control over information, because people are not really able to control all information about themselves.[171] Instead, privacy should be thought of in terms of balancing the interests involved, at the core of which is human dignity.

Our digital reality demands that we start thinking about information in ways that recognize it as a vehicle for personhood and dignity. One compromise for a privacy market is regulating the sale of information that is tied to personhood and dignity. Like property, some information directly implicates personhood and emotional and intellectual freedom, such as a genetic profile, social media page, a diary, political and religious preferences, and internet searches. Other private data may be more fungible and its relevance subject to expiration, such as one's former telephone number, laundry detergent preference, and shoe size.

Conceiving of private data on a personhood continuum may allow subjects limited control over the use and disclosure of information depending on its place on the personhood scale: the more closely related to personhood (and by extension freedom and dignity), the more control. And this control, rather than being based in proprietary rights like patents, is best conceived as a type of moral right for privacy – rights of attribution and integrity for personal information. Jaron Lanier's advocacy for a right of information provenance echoes the notion of a right of attribution that goes with the information, facilitated by technology. Such a right – whether in law or technology or both – would allow information consumers to establish the context, source, and origin of information, an integral part of its interpretation. In turn, this context creation would alleviate dignitary harms while respecting free speech. Similarly, law could establish limitations on the types of personal information data gatherers are permitted to collect and disclose without consent.[172]

C. Information demands regulation that is nimble to technological and global change.

As evidenced in intellectual property law, a changing environment requires rules that are nimble and easily enforceable. Rules governing a privacy market must be responsive to technology, the nuances of privacy preferences, and an internationalized arena.

Advances in technology have consistently challenged both intellectual property and privacy laws. The digital environment allows for the endless sharing of copyrighted works;

privacy's most daunting challenges stem from cheap technology and ubiquitous monitors: government, search engines, tourists sharing their photos.[173] While labels like WiFi-sniffing, RFID, and Big Data are new, Warren and Brandeis's article, which complained of the intrusion of "instantaneous photographs," reminds us that the tension between technology and privacy is an old story. However, the difference between Warren and Brandeis's troubles and ours can bring us hope. Today, technology can help solve the problems it has created.

Many legal scholars have advocated the adoption of new technologies to allow individuals limited control over their private information.[174] These legal scholars understand that the way forward for law must include an acknowledgment and collaboration with existing and future technologies. They realize that the law can provide limits, but only technology can solve the major practical conundrums that stand in the way of social problems. For example, digital rights management was a technological solution to copyright enforcement. For privacy, technologies like P3P can lower the transaction costs for contracting.[175] Provenance and two-way linking can ensure that individuals know how their information is being used. Whether or not these particular technological solutions are the right ones,[176] it becomes clear that technology plays a role in the solution as much as in the problem.

Intellectual property law has been agile in protecting new forms of valuable creations, such as patenting business methods and software and trademarking smells and colors. Like intellectual property, a burgeoning legal regime for privacy must be proactive to changes in its environment.

Finally, the story of intellectual property law teaches privacy that information does not have boundaries, so the law governing it must be adaptable and in sync. Like intellectual property, any meaningful efforts to protect privacy must take into account the need for an international legal vehicle.

The majority of modern privacy breaches occur in a world where the law does not have the force it once had. Technology assures cheap, undetectable, and viral transmission anywhere in the world, making reputation global, not local. But privacy laws are not global, making jurisdiction one of the most burdensome challenges a privacy plaintiff can face.

Intellectual property law learned the importance of supranational agreements early on: the Berne Convention governing copyright was first accepted in 1886 and the Paris Convention for the Protection of Industrial Property was signed in 1883.[177] While these treaties did little to control the substantive intellectual property laws of their member nations, their enactment demonstrated the need for international uniformity and provided an acknowledgement of the urgency for action on a global stage. There is currently no international agreement of heft governing information privacy, only unenforceable guidelines,[178] unilateral conditions,[179] and region-specific frameworks.[180]

D. Information control must be balanced with freedom of expression.

The First Amendment generally bars the government from controlling the communication of information, either by direct regulation or through the authorization of private lawsuits. Intellectual property law protects creations and inventions, but has built-in safety valves that secure freedom of expression. It calibrates the contexts and the ways people can own and use different types of intellectual works.

Safety valves such as fair use balance concerns over the morality and social desirability of granting information monopolies. Fair use limits copyright and trademark, allowing for some of the protected information's benefit to accrue to society. For example, a trademark prohibits

others from using the protected name on a similar product, thereby free-riding on or even ruining the company's good name. Regardless of the product's fame, however, any individual can comment on the product's quality, compare it to other similar products, and even make fun of it.

Like intellectual property law, privacy trades must adopt regulations to maintain the integrity of information flows in society. Lawrence Lessig has advocated for a "fair use"-like limitation on the kinds of information people can sell.[181] Information that is harmful or fraudulent, he argues, should be exempt from shielding.[182] But the information protected by privacy law is considerably different than intellectual property's for two reasons.

First, privacy seeks to silence facts, not just creations of the mind.[183] Suppressing truthful information is socially problematic and, some have argued, per se unconstitutional.[184] Allowing people to hide their illicit pasts or artificially cleanse their reputations interrupts the very information flow that allows us to make correct judgments. Further, Eugene Volokh contends restricting data flow is the "power to suppress facts,"[185] which no law can constitutionally do – not even intellectual property itself. Volokh characterizes the communication of information about reputation, but as facts, which cannot be suppressed.[186] As Neil Richards has put it, since "the creation, assembly, and communication of information are at the core of the First Amendment, data privacy rules that restrict this expressive activity improperly burden free speech and are thus largely or entirely unconstitutional."[187]

Second, while both privacy and intellectual property cover a diverse and daunting breadth of subject matter, privacy is considerably more slippery. Privacy is culturally-relative, subjective, and context-specific. Its subject matter might include everything that a certain society would want their upstanding citizens to hold close. In some societies, nudity may be well-accepted, in others, the body is deemed private. Even within societies, privacy is subjective. That is, people define and value privacy differently. Their estimations might depend on factors as diverse as religion, upbringing, feelings about their bodies, experiences, and safety concerns. In addition to being relative across cultures and subjective, what is private is also highly context-specific, depending on the information's recipient. Research indicates that people's valuation of their private information is inconsistent and highly malleable.[188]

For these two reasons, many legal scholars and economists have advocated that contract is the most effective – and legally legitimate – solution for privacy.[189] Unfortunately, as discussed above, digital contracts do not give consumers a real choice. Contract law, however, provides limits to what is an enforceable bargain: Contracts whose subject matter is against public policy are not enforceable, even if the parties freely consented. One solution for regulating a privacy market could be found in the strengthening or codifying of that common law rule to prevent unconscionable and socially-detrimental privacy transactions.

E. Inertia is the enemy of control

Intellectual property's evolution and resilience is strongly tied to constant monitoring and advocacy on the part of its owners. As any copyright, patent, or trademark holder knows, legal protection means nothing without monitoring on the part of the owner; the burden on protecting the creation is on its owner, and this involves a cost.

The same is true for privacy protection: The privacy-conscious, like the IP owner, must monitor, protect, and defend, even though the costs of doing so have risen dramatically. Conventional wisdom tells us that individuals are not as vigilant or protective of their privacy. Since privacy protection had traditionally been "outsourced" to well-functioning norms, people

may have been unaccustomed to bearing the burden of managing their private data. Perhaps for this reason, it seems that individuals often disregard the consequences of personal information flow in favor of expediency, convenience, or socialization.

Politically, the privacy movement can learn from intellectual property as well. The political environment surrounding intellectual property ensures its maintenance and expansion. Lawrence Lessig writes,

> "With copyright, the interests threatened are powerful and well organized; with privacy, the interests threatened are diffuse and disorganized. With copyright, the values on the other side of protection (the commons, or the public domain) are neither compelling nor well understood. With privacy, the values on the other side of protection (security, the war against terrorism) are compelling and well understood."[190]

Invasions of privacy often involve harms that are each too small to justify action on single individual's part. Since these harms do not implicate big business's bottom line, privacy's political lobby is less organized, less concerted, and less funded than alternate interests.

Some have argued that the apparent lack of individual and political militates against privacy regulation.[191] Others have contended that what appears to be people's willingness to give away, or sell, privacy, is evidence that it is no longer valued.[192] These inferences are too simplistic given the informational asymmetries and skewed technological backdrop against which this privacy drama plays out. Technology allows for invisible collectors, rendering the costs of tracking one's information too high. Individuals must have the ability and capacity to know how their information is used in third-party hands. Armed with this knowledge and power, individuals so disposed will be more apt to take an active role in the protection of their privacy.

IV. CONCLUSION

In 1967, Professor Alan Westin warned that a cumulative record of personal information would become a "new social control mechanism" that would "be the basis on which employment and membership in social organizations will depend."[193] Westin noted,

> The danger to privacy and to American liberties in this development was that individuals who knew that all this information was being collected and stored and lay readily available in the machines would never be able to know when it would be used 'against them' and for what purposes. This public awareness of potential use would lead to an increase in behavior 'for the record' and less freedom of action and expression. People will be concerned not only with the fact that they are going 'on the record,' but also how that record will 'look' to those in authority who examine it.[194]

In the mid-1960s, Westin's arguments were indeed prophetic – long before the Internet or widespread digital technologies, big data, and social media, which today make individuals more searchable and easily monitored than ever.

The most important thing that humans trade is information. It is how we get to know each other, how we build our identities, how we govern our societies, and how we pass on our

histories. Privacy is about individually choosing who gets the message. To maintain our peace and dignity, we must be able to control certain uses and abuses of our personal information.

But we are currently powerless to do so. We are now living a historical transition into a digital world, where those normative structures do not exist and are not easily replicated, making it difficult for individuals to protect privacy interests. A lack of bargaining power, limited consumer choice, and other market failures mute individual will. To protect privacy, both our digital and physical societies must catch up in establishing privacy-respecting norms based on fundamental human dignity and autonomy.

Proponents and critics of selling privacy offer a smorgasbord of economic, moral, legal and practical reasons for and against it. Deciphering their polyphonic, and often dissonant, chorus is critical to charting a way forward for the privacy debate, both at the scholarly level and at the political one. Most agree on two things: privacy is desirable (although some may disagree on the extent to which it is desirable) and technology threatens privacy and forces us to think about its protection in new ways.

At this point in history, making privacy an intellectual property-like right is neither feasible nor wise. Privacy is too slippery a concept to be propertized, but unless we act soon, the failures and inequalities of the existing privacy market will only become further entrenched. Although the intellectual property model does not suit privacy interests and selling privacy is troubling in many instances, intellectual property law offers many lessons to a struggling privacy law. Casting (or recasting) privacy into new molds is now a global question, as philosophies of privacy and the laws they inspire clash in a world without jurisdiction. Boundaries must be created by technology and reinforced by law to shape desirable public policy in a world where those who want privacy can have it without giving anything up, or having to pay for it.

---

[1] Alessandro Acquisti, Leslie John, & George Loewenstein, *What is Privacy Worth?*,42 J. LEGAL STUD. 249,253 (2013) ("Everyday we are faced with opportunities to pay to prevent our personal data from being disclosed.")

[2] *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARVARD L. REV. 2055 (2004) (noting compelling examples of Americans participating in the commoditization of their personal data); McKay Cunnigham, *Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law*, 44 GEORGE WASHINGTON INTERNATIONAL LAW REVIEW, 644(2012) ("Information services and goods constitute the world's largest economic sector").

[3] Some state probate statutes provide the process by which social media accounts pass. OKLA. STAT. tit. 58 §269 (2010); *see* Clay Calvert, *A Familial Privacy Right Over Death Images: Critiquing the Internet-Propelled Emergence of a Nascent Constitutional Right that Preserves Happy Memories and Emotions*, 40 HASTINGS CONST. L.Q. 475 (2013).

[4] *See infra* section III.A.

[5] Omer Tene & Jules Polonetsky, *Big Data For All: Privacy and User Control in the Age of Analytics,* 11 NW. J. TECH. & INTELL. PROP. 239, 261-262 (2012).

[6] RICHARD POSNER, THE ECONOMICS OF JUSTICE, 243; LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 160-163 (1999)[hereinafter Code]; CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 (Basic Books 2006)[hereinafter, Code 2.0].

[7] *See* Developments in the Law--The Law of Cyberspace, 112 HARV. L. REV. 1574, 1634-49 (1999); Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 63-65 (1999); Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 26-41 (1996); Kenneth C. Laudon, *Markets and Privacy.* 39 ASS'N COMPUTING MACHINERY: COMM. OF THE ACM 92(1996); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2383 (1996); Edward J. Janger, *Enforcing Privacy Rights: Agency Enforcement and Private Rights of Action: Privacy Property, Information Costs, and the Anticommons,* 54 HASTINGS L.J. 899 (2003).

[8] Paul M. Schwatz and Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information* 86 N.Y.U. L. Rev. 1814, 1854 (2011).

[9] JARON LANIER, WHO OWNS THE FUTURE? (Simon & Schuster, 2013).

[10] *See generally*, ARTHUR L. CORBIN, CORBIN ON CONTRACTS at §6 (1992).
[11] Federal Trade Commission 16 C.F.R. §225 *Guides Concerning the Use of Endorsements and Testimonials in Advertising*. This rule was updated in 2009 to apply to social media.
[12] 18 USC §2252 explicitly prohibits all forms of child pornography. This applies to production, distribution, reception and possession.
[13] RESTATEMENT (SECOND) OF TORTS § 652 C describes the right of publicity. "One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy."
[14] Cal. Lab. Code. §§1171-1206 (inclusive). California labor code defines standards for hours, wages, and working conditions for "apply to and include men, women and minors employed in any occupation, trade, or industry."
[15] Human subjects research is governed by 45 CFR 46, which requires detailed procedures, including consent and disclosures, for all subjects. The regulation gives heightened protection to subjects who are pregnant, fetuses, prisoners, and children.
[16] Adam Thierer, *Privacy, Security, and Human Dignity in the Digital Age: The Pursuit of Privacy in a World Where information Control is Failing*, 36 HARV. J.L. & PUB. POL'Y 429-431 (2013).
[17] Thomas Hemnes, *The Ownership and Exploitation of Personal Identity in the New Media Age*, 12 J. MARSHALL REV. INTELL. PROP. L. 1 (2012). (*see* section I.B.1)
[18] Stephanie Kuhlmann, *Do Not Track Me Online: The Logistical Struggles Over the Right "To Be Let Alone" Online*, 22 DEPAUL J. ART TECH. & INTELL. PROP. L. 229, 235 (2011).
[19] *See* Peter K. Yu, *The Political Economy of Data Protection*, 84 CHI. -K. L. REV. 777, 778 (2010) ("Although data have always been valuable, their value was not as greatly appreciated as it is today.").
[20] Jonathan Zittrain, *Privacy 2.0*, 65 U. CHI. LEGAL F. 65, 73 (2008).
[21] Stephanie Armour, *Data Brokers Come Under Fresh Scrutiny*, WALL ST. J., Feb. 12, 2014, *available at* http://online.wsj.com/news/articles/SB10001424052702303874504579377164099831516.
[22] Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES, June 16, 2012 at BU1, *available at* http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?_r=1&pagewanted=all.
[23] Jonathan Shaw, *Why "Big Data" is a Big Deal*, HARVARD MAGAZINE (March-April 2014).
[24] Dennis Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation or Co-Regulation?* 34 SEATTLE UNIV. L. R. 439, 448 (2011)
[25] ERIC SCHMIDT & JARED COHEN, THE NEW DIGITAL AGE: RESHAPING THE FUTURE OF PEOPLE, NATIONS AND BUSINESS 38 (2013).
[26] Patrick Copeland, et. al., *Google Disease Trends: An Update*, http://static.googleusercontent.com/external_content/untrusted_dlcp/research.google.com/en/us/pubs/archive/41763.pdf.
[27] Wai-Ming Yu, *Big Data Analytics Helps Protect Communities*, INFORMATION WEEK, http://www.informationweek.com/government/big-data-analytics/big-data-analytics-helps-protect-communities/d/d-id/1113720.
[28] CODE 2.0, *supra* note 6, at 202.
[29] Schmidt & Cohen, *supra* note 25.
[30] Once something is uploaded to the Web, an individual or a third party cannot remove it without help from the administrator of the website where it appears. On most websites, administrator-facilitated takedowns are elusive, if not impossible. The Internet Archive's Wayback Machine archives web pages dating back to 1996. *See* http://archive.org/web/web.php.
[31] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG., Feb. 16, 2012, *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=3&hp.
[32] Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES, Feb. 16, 2012, *available at* http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.
[33] Reputation also has implications for health as well as emotional and physical security. Some studies have shown a correlation between reputation damage and risk of suicide. Saxby Pridmore, *Suicide and Reputation Damage*, 16 AUSTRALASIAN PSYCHIATRY. 312 (2008). Press accounts about physical harm and suicide following viral disgrace are not infrequent. *See, e.g.*, Melissa Jeltsen, *Girl Cyber-Bullied, Hospitalized After Oral Sex Photos Go Viral*, THE HUFFINGTON POST, *available at* http://www.huffingtonpost.com/2013/08/20/slanegirl-photo-goes-viral_n_3785741.html.; HUFFINGTON POST, *Emma Jones, British Teacher, Killed Herself After Naked Photos Posted*

on Facebook, available at http://www.huffingtonpost.com/2010/02/26/emma-jones-british-teache_n_477337.html (October 8, 2013).
[34] *See* Patricia Sanchez Abril, Avner Levin & Alissa del Riego, *Blurred Boundaries: Social Media Privacy and the 21st Century Employee*, 49 AMER. BUS. L. J. 63 (2012).
[35] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999) ("this right to keep data isolated quickly proves illusory because of the demands of the Information Age.")
[36] Kashmir Hill, *Beware, Tech Abandoners. People Without Facebook Accounts Are 'Suspicious,'* FORBES, August 6, 2012, *available at* http://www.forbes.com/sites/kashmirhill/2012/08/06/beware-tech-abandoners-people-without-facebook-accounts-are-suspicious/.
[37] Neil M. Richards & Jonathon H. King, *Three Paradoxes of Big Data*, 66 STAN. L. REV. 41, 45 (2013).
[38] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1395 (2000).
[39] Paul Schwartz has argued that "[i]nformation asymmetries are likely to exist between data collectors and the individual whose personal information is collected. Indeed, data collectors have an incentive to engage in smokescreen tactics to make it difficult for individuals to obtain understandable information about data collection and use." Schwartz, *supra* note 2, at 2080; Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1894 (2012), ("either people have choices that are not meaningful or people are denied choices altogether.").
[40] Schwartz, *supra* note 2, at 2081.
[41] *Id.* at 2079 (discussing the critical mass problem, information costs, and detection costs that consumers face when trying to protect their privacy).
[42] Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1132–33 (2000).
[43] U. S. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress*, May 2000, *Text available at*: http://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission. Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1
[44] Pub. L. No. 99-508, Title I, 100 Stat. 1851, 1859 (codified at 18 U.S.C. §§ 2510–22 (2006)); Title II, 100 Stat. 1860 (codified at 18 U.S.C. §§ 2701–11 (2006)); Title III, 100 Stat. 1868 (codified at 18 U.S.C. §§ 3121–27 (2006)); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002) ("The ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication like Konop's secure website.").
[45] Because there is no federal or uniform privacy law applicable to online transactions, the states have adopted a smorgasbord of narrowly-targeted privacy laws. In 2013 alone, more than 10 states passed over two dozen privacy laws. Somini Sengupta, *No U.S. Action, So States Move on Privacy Law*, N.Y. TIMES, Oct. 30, 2013, A1. For example, Oklahoma moved to protect the privacy of its student's data. 70 OK § 3-168. California began requiring that companies disclose their consumer software tracking policies. CAL. BPC. CODE § 22575.
[46] *See* Guido Calabresi & A. Doug Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972).
[47] RESTATEMENT (THIRD) OF UNFAIR COMPETITION §46.
[48] Copyright law protects expressive works, but not ideas. 18 U.S.C. §102(b).
[49] *See supra* notes 6-9.
[50] Viktor Mayer-Schonberger, *Beyond Privacy, Beyond Rights-Toward a "Systems" Theory of Information Governance*, 98 CAL. L. REV. 1853, 1861 (2011).
[51] CODE, *supra* note 6, at 160-163.
[52] Tom Simonite, *If Facebook Can Profit from Your Data, Why Can't You?*, TECHNOLOGY REVIEW, *available at* http://www.technologyreview.com/news/517356/if-facebook-can-profit-from-your-data-why-cant-you/ (Feb. 24, 2014); *See* Julia Angwin & Emily Steel, *Web's New Commodity: Privacy*, WALL ST. J. (Feb. 28, 2011, 12:01 AM), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html.
[53] Tom Simonite, *Sell Your Personal Data for $8 a Month*, TECHNOLOGY REVIEW, *available at* http://www.technologyreview.com/news/524621/sell-your-personal-data-for-8-a-month/ (Feb. 24, 2014).
[54] Nicolas Rauline, *Take Back Control of Your Personal Data, Then Sell It*, WORLDCRUNCH, *available at* http://www.worldcrunch.com/tech-science/take-back-control-of-your-personal-data-then-sell-it-to-highest-bidder/start-up-yes-profile-advertising-profile-internet/c4s11754/#.Uxh--z9dWrR
[55] PERSONAL, https://www.personal.com/our-story (last visited Dec. 1, 2013).
[56] Schmidt & Cohen, *supra* note 25, at 38.

[57] *Id*. at 39.
[58] In the interest of focus, this article will not canvass every area of privacy. Decisional privacy is one such example. Griswold v. Connecticut 381 U.S. 479 (1965).
[59] U.S. Const., art. I, § 8 gives Congress the power to "promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."
[60] MARGARET JANE RADIN, PROPERTY AND PERSONHOOD, 966, 1001 (1982).
[61] WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW (2009) at 453 ("Intellectual property is notably diverse.").
[62] *See, e.g.,* ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (Antheneum 1967) ("the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."); Professor Richard Parker described privacy as "control over when and by whom the various parts of us can be sensed by others." Richard Parker, *A Definition of Privacy*, 27 RUTGERS L. REV. 275, 281 (1974); *See* Charles Fried, *Privacy, 77* YALE L.J. *475 (1968)* at 482. ("Privacy is . . . the control we have over information about ourselves.");
[63] *See, e.g.*, Daniel J. Solove, *A Taxonomy of Privacy,* 154 U. PA. L. REV. 477, 482 (2006) ("Privacy problems are frequently misconstrued or inconsistently recognized in the law. The concept of 'privacy' is far too vague to guide adjudication and lawmaking.").
[64] AMITAI ETZIONI, THE LIMITS OF PRIVACY 189 (Basic Books 1999).
[65] *Id.*
[66] See Edward Shils, *Privacy: Its Constitution and Vicissitudes*, 31 LAW AND CONTEMP. PROBS. 281 (1966). Some have attributed the increased attention on privacy laws during this time to the closing of the West, which made Americans feel that opportunities for seclusion were becoming limited. Robert Copple, *Privacy and the Frontier Thesis: An American Intersection of Self and Society*, 34 AM. J. OF JURIS. 87-104 (1989).
[67] Etzioni, *supra* note 64, at 205
[68] *Id.* at 205-07.
[69] Samuel Warren & Louis Brandeis, *The Right to Privacy,* 4 HARV. L. R. 193 (1890). ("The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.")
[70] Warren & Brandeis, *supra* note 69.
[71] *Id.*
[72] *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE L.J. 1151 (2004); Avner Levin & Patricia Sanchez Abril, *Two Notions of Privacy: Assessing Expectations of Privacy on Social Networking Websites*, 11 VANDERBILT JOURNAL OF ENTERTAINMENT & TECHNOLOGY LAW 1001 (2009).
[73] Kenneth Bamberger & Deirdre K.Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 254 (2011).
[74] See Radin, *supra* note 60.
[75] 227 U.S. 438 (1928).
[76] *Id*. at 478.
[77] 389 U.S. 347 (1967). Katz famously stated that the Fourth Amendment "protects people, not places."
[78] City of Ontario v. Quon, 130 S. Ct. 2619 (2010)(examining the privacy of text-messages on an employer-provided mobile device); see also Shlomit Yanisky-Ravid, *Privacy within the Virtual Workplace: The Entitlement of Employees to a Virtual 'Private Zone' and the 'Balloon' Theory*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2231694 (proposing a "virtual" sphere of privacy).[Shlomit - please let me know if this is OK to cite].
[79] Patricia Sanchez Abril, Avner Levin & Alissa del Riego, *Blurred Boundaries: Social Media Privacy and the 21st Century Employee*, 49 AMER. BUS. L. J. 63 (2012).
[80] Katz v. United States, 389 U.S. 347 (1967). In the context of private employers, the analysis is the same, involving the balance of the employer's property rights with the employee's dignitary rights. *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (finding that there is no "reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system."); Dir. of Office of Thrift Supervision v. Ernst & Young, 795 F. Supp. 7, 10 (D.D.C. 1992) (examining privacy of diaries containing personal and company data).

[81] *Id.* In other countries, such as the European Union Member States, employees have a right to dignity and to a private life that does not stop at the boundary of the workplace. While this right is not absolute and must be balanced with the employer's property rights, it does contain an inalienable core that protects the dignity of the employee as a human being.
[82] RESTATEMENT (SECOND) OF TORTS § 652B (1977).
[83] *See* Haelan Laboratories v. Topps Chewing Gum, 202 F.2d 866, 868 (2d Cir.), cert. denied, 346 U.S. 816 (1953)("A man has a right in the publicity value of his photograph, i.e., the right to grant the exclusive privilege of publishing his picture.")
[84]RESTATEMENT (THIRD) OF TORTS: § 45 (1995). ("Monetary Relief: Appropriation of Trade Secrets").
[85] Landes & Posner, *supra* note 61, at 355.
[86] *Id.*, at 141.
[87] Gary Stanley Becker, THE ECONOMIC APPROACH TO HUMAN BEHAVIOR (1978).
[88] RICHARD POSNER, THE ECONOMICS OF JUSTICE 243 (1981).
[89] *Id*. at 244.
[90] Code, *supra* note 6, at 160.
[91] *Id*. at 160.
[92] Acquisti, John & Loewenstein, *supra* note **Error! Bookmark not defined.**, at 258
[93] Ian Ayres & Matthew Funk, *Marketing Privacy*, 20 YALE J, ON REG. 77, 133-134 (2003).
[94] *Id.* at 96, 111.
[95] Simonite, *supra* note 52; s*ee also* Julia Angwin & Emily Steel, *Web's New Commodity: Privacy*, WALL ST. J. (Feb. 28, 2011, 12:01 AM), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html.
[96] *See* Lanier, *supra* note 9.
[97] Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 658, 659 (2012).
[98] Samuelson, *supra* note 42, at 1133
[99] Lanier, *supra* note 9, at 20.
[100] *Id.* at 246.
[101] *Id. See also*, Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 658, 704 (2012).
[102] Lanier, *supra* note 9, at 246.
[103] Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 26-41 (1996).
[104] Ian Ayres & Matthew Funk, *Marketing Privacy*, 20 YALE J. ON REG. 77, 133-134 (2003)(" the switch from government-imposed worthlessness (under a statute) to market valuation should cause people to value it more highly.").
[105] Code, *supra* note 6, at 160.
[106] Code 2.0, *supra* note 6, at 229.
[107] Anita Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 750 (1999). Julie E. Cohen, *supra* note 38, at 1377; Pamela Samuelson, *supra* note 42, at 1170–73; Simon G. Davies, *Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity*, in TECHNOLOGY & PRIVACY: THE NEW LANDSCAPE 143, 160 (Philip E. Agre & Marc Rotenberg, eds., 1997); Marc A. Lemley, *Private Property: A Comment on Professor Samuelson's Contribution*, 52 STAN. L. REV. 1545, 1551 (2000); Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1 (2001).
[108] Etzioni, *supra* note 64, at 190. Professor Etzioni noted this was true even by those who "otherwise draw on no religious images, terminologies or beliefs."
[109] *Id.* at 190.
[110] Edward Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. Rev. 962, 1003 (1964). ("The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity.")
[111] Margaret Jane Radin, *Property Evolving in Cyberspace*, 15 J. L. & COMM. 524-26 (1996); MARGARET JANE RADIN, CONTESTED COMMODITIES (1996).
[112] MICHAEL J. SANDEL, WHAT MONEY CAN'T BUY: THE MORAL LIMITS OF MARKETS 9 (2012).
[113] Schwartz, *supra* note 2, at 2086.
[114] *See* Radin *supra* note 111, at 2-15.

[115] *See also* Sonia M. Suter, *Disentangling Privacy from Property: Toward a Deeper Understanding of Genetic Privacy*, 72 GEO. WASH. L. REV. 737, 814 2003 (804).
[116] Samuelson, *supra* note 42, at 1141.
[117] *See* Radin, supra note 60.
[118] *Id.* at 957.
[119] Sandel, *supra* note 112, at 123.
[120] Joseph W. Jerome, *Buying And Selling Privacy: Big Data's Different Burdens and Benefits*, 66 STAN. L. REV. 47, 51 (2013) ("the poor are not in a position to pay for their privacy or to value it over a pricing discount, even if this places them into an ill-favored category").
[121] Reputation.com (formerly Reputation Defender) is the most widely known reputation-oriented service and charges between $3,000 and $15,000 to monitor the online reputation of businesses. Individual service plans start at $9.95 per month *See* http://www.reputation.com/reputationdefender (last accessed October 8, 2013).
[122] Cohen, *supra* note 38, at 1438. Professor Cohen suggests that "recognizing property rights in personally-identifiable data risks enabling more, not less, trade and producing less, not more, privacy."
[123]*See* Janet Dean Gertz, *The Purloined Personality: Consumer Profiling in Financial Services*, 39 SAN DIEGO L. REV. 906, 943 (2002).
[124] Schwartz, *supra* note 2, at 2078 ("The asymmetry of information available to various players in the market– as well as the systematic disadvantage and relative vulnerability of consumers in the market – underscores concerns about commodification of personal data.")
[125] Gertz, *supra* note 123, at 965. ("a property rights regime would set in motion a significant transfer of economic and market power to the data collectors."); Jared Livingston, *Invasion Contracts: The Privacy Implications of Terms and Use Agreements in the Online Social Media Setting*, 21 ALB. L.K. SCI. & TECH., 591, 625 (2011).
[126] Sonia M. Suter, *Disentangling Privacy from Property: Toward a Deeper Understanding of Genetic Privacy*, 72 GEO. WASH. L. REV. 737, 814 2003 (804).
[127]Gertz, *supra* note 123, at 965.
[128] Cohen, *supra* note 38, at 1397; Marc A. Lemley, *Cyberspace and Privacy: A New Legal Paradigm? Private Property*, 52 STAN. L. REV. 1545, 1557 (2000).
[129] Schwartz, *supra* note 2, at 2076.
[130] Cohen, *supra* note 38, at 1397.
[131] Schwartz, *supra* note 2, at 2077.
[132] "An intellectual property law governing personal data would result in the creation of literally billions of new intellectual property rights every day." Marc A. Lemley, *Cyberspace and Privacy: A New Legal Paradigm? Private Property*, 52 STAN. L. REV. 1545, 1557 (2000).
[133] Schwartz, *supra* note 2, at 2072.
[134] *Id.* at 252-3.
[135] Posner, *supra* note 88, at 231.
[136] One notable exception is the U.S.'s Visual Artists Rights Act of 1990 (VARA), which provides visual artists non-transferrable positive rights to claim their authorship and prevent the association of their name with work that he or she did not create. The law also gives artists right to prevent use of their name in association with a work of visual art that distorts, manipulates, or modifies their work in a prejudicial or dishonorable way. 17 USC §106A.
[137] 424 U.S. 693 (1976).
[138] *Id*. at 1160. ("The words 'liberty' and 'property' as used in the Fourteenth Amendment do not in terms single out reputation as a candidate for special protection over and above other interests that may be protected by state law.")
[139] *See also*, Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. 88 (2012).
[140] Neil M. Richards, *Reconciling Privacy Data and the First Amendment*, 52 UCLA L. REV. 1149, 1222 (2005) ("because the First Amendment protects at its core the dissemination of truthful information, any right of "data privacy" is in direct conflict with the First Amendment.").
[141] Schmidt & Cohen, *supra* note 25, at 58.
[142] *Id*.
[143] Landes & Posner, *supra* note 61, at 141. *See also* Richard A. Posner, *Our Domestic Intelligence Crisis*, WASH. POST, December 21, 2005, at A31.
[144] Sandel, *supra* note 112, at 114.
[145] DAN ARIELY, PREDICTABLY IRRATIONAL 75-102 (Harper, 2010). Professor Dan Ariely's studies suggest that in certain situations paying people to do something may elicit less effort and less favorable responses from them than asking them to do it for free.

[146] Sandel, *supra* note 112, example of lawyers being less likely to do pro bono work.
[147] See Fried, *supra* note 62. Fried writes, "To be friends or lovers persons must be intimate to some degree with each other. Intimacy is the sharing of information about one's actions, beliefs or emotions which one does not share with all, and which one has the right not to share with anyone. By conferring this right, privacy creates the moral capital which we spend in friendship and love." *Id.* ; Robert S. Gerstein, *Intimacy and Privacy*, PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 265, 265 (Ferdinand David Schoeman ed., 1984).
[148] Thomas E. Runge & Richard L. Archer, *Reactions to the Disclosure of Public and Private Self-Information*, 44 SOC. PSYCHOL.. Q. 357, 361 (1981) (discussing experimental findings in which subjects claim to like their stranger-partner more if the stranger-partner shares information that she claims she has not previously revealed).
[149] *See* CARL D. SCHNEIDER, SHAME, EXPOSURE, AND PRIVACY 42 (1977) ("Privacy creates the moral capital that is spent in friendship and intimate relations.").
[150] Zittrain, *supra* note 20, at 85.
[151] Bloustein, *supra* note 110, at 1003.
[152] U.S. v. White, 401 U.S. 745, 762 (1971) (Douglas, J., dissenting).
[153] *See* Cohen, *supra* note 38, at 1377.
[154] *See, e.g.*, Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957 (1989).
[155] Eric A. Posner & Cass Sunstein, *The Law of Other States*, 59 STAN. L. REV. 131 (2006).
[156] Stephanie Pell, *Jonesing for a Privacy Mandate, Getting a Technology Fix – Doctrine to Follow*, 14 N.C. J.L. & TECH. 489, 525 (2013).
[157] Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 STAN.L. REV. 1201 (2000).
[158] Zittrain, *supra* note 20, at 81.
[159] Landes & Posner, *supra* note 61, at 1.
[160] Code 2.0, *supra* note 6, at 231.
[161] *See, e.g.*, Warren & Brandeis, *supra* note 69.
[162] Social scientists have long described this as an intrinsic human need. *See, e.g.*, ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (Doubleday 1959); Bloustein, *supra* note 110, at 971.
[163] Radin, *supra* note 60 at 986.
[164] Moral rights are incorporated into the Berne Convention for the Protection of Literary and Artistic Work, Article 6bis, *available at*: http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html#P123_20726.
[165]*See* Whitman, *supra* note 72; Paul Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1971 (2013).
[166] Charter of Fundamental Rights of the European Union, 2000/C 364/01, *available at* http://www.europarl.europa.eu/charter/pdf/text_en.pdf.
[167] *Id.* These principles are derived from what is commonly known as the "EU Data Directive." 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). [Hereafter: EU Directive]. The EU Directive establishes data protection for Europeans in all their commercial transactions worldwide.
[168] For example, one European court allowed model Naomi Campbell to recover for the disclosure of a picture showing her exiting a Narcotics Anonymous meeting. Although the image was taken in public, the court, interpreting EU law, recognized it as an affront to her honor. *See* Stuart Goldberg, *The Contest for a New Law of Privacy: A Battle Won, a War Lost? Campbell v. Mirror Group Newspapers Limited*, 9 COMM. L. 122 (2004).
[169] French courts have held that employees have a bounded private space, even at work. *See* Arret 4164, Cour de Cassation – Chambre Sociale, 2001, *available at* http://www.courdecassation.fr/agenda/arrets/arrets/99-42942arr.htm.
[170] ROBERTA KWALL, THE SOUL OF CREATIVITY (2010)(arguing that U.S. law is deficient in protecting moral rights, especially as compared to European law).
[171] *See* Anita M. Allen, *Privacy-as-Data Control: Conceptual, Practical and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 861-62 (2000) (stating that "[t]he popularity of the privacy-control paradigm is problematic because there are a number of conceptual, practical, and moral limits to its plausibility).
[172] The problem, of course, is that the law often cannot anticipate what the foreseeable implications of any disclosure will be. We can all conjure scenarios in which information that is fungible, or low on a personhood scale, would be

damaging to an individual if disclosed and judged upon in certain contexts. This underscores the need for contract and tort law to supplement in those instances where the individual has a particular preference or injury.
[173] Zittrain, *supra* note 20, at 215.
[174] Zittrain, *supra* note 157, at 1240.
[175] NIVA ELIKIN-KOREN & ELI M. SALZBERGER, LAW, ECONOMICS AND CYBERSPACE: THE EFFECTS OF CYBERSPACE ON THE ECONOMIC ANALYSIS OF LAW 95 (2004). ("transaction costs might also decrease in the future…take, for example, the Platform for Privacy Preferences Project"). For a description of P3P, *see* Technology and Society Domain, *The Platform for Privacy Preferences Initiative*, (November 20, 2007) http://www.w3.org/P3P/.
[176] Examining technological solutions is beyond the scope of this chapter.
[177] *See supra* note 164.
[178] Organization for Economic Cooperation and Development. *APEC Privacy Framework 2005.* APEC Secretariat, Signapore, 2005.
[179] EU Directive *supra* note 167. (Relating to the Adequacy aspect).
[180] EU Data Directive; the Supplementary Act on Personal Data Protection within the Economic Community of West African States; The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), E.T.S. 108 was the first binding international treaty addressing the collection and processing of personal data. With the exception of Uruguay (which ratified the treaty in late 2013), all of the member nations are members of the Council of Europe, giving it the flavor of a regional rather than international instrument. *Available at* http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG.
[181] Code 2.0, *supra* note 6, at 231.
[182] *Id.*
[183] Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 Stan. L. Rev. 1049 (2000). Not even intellectual property rights, he argues, "give the intellectual property owners the power to suppress facts."
[184] *Id.* at 1057 (arguing that the only constitutionally permissible means for enforcing personal information privacy is contract law); Diane Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291 (1983).
[185] Volokh, *supra* note 183, at 1063
[186] *Id.* at 1076.
[187] Richards *supra* note 140, at 1160. Richards slices the problem thinner than Volokh, suggesting a two-pronged approach to reconcile free speech rights with privacy. First, he asks whether the activity in question is protectable speech under the First Amendment; then, if so, courts must determine the level of obligation or strength of First Amendment "protection."
[188] Acquisti, *supra* note 1.
[189] *See, e.g.*, Samuelson, *supra* note 42; Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POL'Y 591, 592 (1994) (claiming that a contractual solution most effectively protects privacy rights); Craig Martin, *Mailing Lists, Mailboxes, and the Invasion of Privacy: Finding a Contractual Solution to a Transnational Problem*, 35 HOUS. L. REV. 801, 850 (1998) (proposing an expansion of existing legislation coupled with industry contracting); Cohen, *supra* note 38; Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283 (2000). Economists argue that when transaction costs are low, enforceable contract rights are all that society needs, beyond some underlying set of entitlements so that the parties have something to contract about, to attain optimal use and investment. Landes & Posner, *supra* note 61 at 14, citing R.H. Coase, *The Problem of Social Cost*, 3 J. L.& ECON. 1 (1960).
[190] Code 2.0, *supra* note 6, at 200-1.
[191] PAUL H. RUBIN & THOMAS M. LENARD, PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION (2002).
[192] Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, THE GUARDIAN, *available at* http://www.theguardian.com/technology/2010/jan/11/facebook-privacy (last visited Dec. 6, 2013).
[193] Westin, *supra* note 62, quoting S.P. Wagner, *Records and the Invasions of Privacy*, 40 SOCIAL SCIENCE 38 (1965).
[194] *Id*. at 312-313.